STRATEGIC LATENCY UNLEASHED

THE ROLE OF TECHNOLOGY IN A REVISIONIST GLOBAL ORDER AND THE IMPLICATIONS FOR SPECIAL OPERATIONS FORCES

EDITED BY ZACHARY S. DAVIS, FRANK GAC, CHRISTOPHER RAGER, PHILIP REINER, AND JENNIFER SNOW

CENTER FOR GLOBAL
SECURITY RESEARCH

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory in part under Contract W-7405-Eng-48 and in part under Contract DE-AC52-07NA27344. The views and opinions of the author expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC.
ISBN-978-1-952565-07-6 LCCN-2021901137 LLNL-BOOK-818513 TID-59693

To download the ebook: See cgsr.llnl.gov

STRATEGIC LATENCY UNLEASHED

THE ROLE OF TECHNOLOGY IN A REVISIONIST GLOBAL ORDER AND THE IMPLICATIONS FOR SPECIAL OPERATIONS FORCES

EDITED BY ZACHARY S. DAVIS, FRANK GAC, CHRISTOPHER RAGER, PHILIP REINER, AND JENNIFER SNOW

Center for Global Security Research
Lawrence Livermore National Laboratory
January 2021

Table of Contents

EDITOR'S NOTE 1

FOREWORD 2

DEDICATION 4

ACKNOWLEDGEMENTS 5

INTRODUCTION

Latency Unleashed: What It Means for Special Operations Forces
Zachary S. Davis, *Lawrence Livermore National Laboratory (LLNL), Research Professor, Naval Postgraduate School (NPS)* 8

SECTION 1
GEOPOLITICS OF STRATEGIC LATENCY FOR SOF: CONTEXT IS EVERYTHING

Winning and Losing in Counterproliferation
Zachary Davis, *LLNL/NPS*, and Michael Greene, *Naval Special Warfare Command (ret.)* 15

The Role of Special Operations Forces in Countering Weapons of Mass Destruction
Brendan Melley, *Center for the Study of Weapons of Mass Destruction, National Defense University (NDU)* 22

Identity and Virtual Nations: Implications of Digital Citizenship and Developing Global Autonomous Communities for Special Operations Forces
Jennifer J. Snow, AFWERX/CTO 34

Special Forces and Strategic Deterrence
Brad Roberts, LLNL, Center for Global Security Research (CGSR) 51

Quantum Corps: Consequence and Superiority in the Theater of Applied Imagination
Marshall M. Monroe, Marshall Monroe MAGIC 61

Russia's Special Purpose Forces: A Strategic Weapon
Glenn Chafetz, *Ridgeline*; Michael Nacht, *University of California, Berkeley*; and Jonathan Fagins, *US Army Special Operations Command (USASOC)* 82

Sharp Swords of the Future Battlefield:
The Chinese Military's Special Forces and Psychological Operations
Elsa Kania, *Center for a New American Security*, and Peter Wood, *Bluepath Labs* 94

SECTION 2
BIOLOGY AND THE BODY POLITIC: MESSING WITH MOTHER NATURE

What COVID-19 and China's Grand Strategy May Teach about a History of the Future
James Giordano, *Georgetown University*, and L. R. Bremseth *USN SEAL (ret.)* 109

Cyborg Soldier 2050: Human-Machine Fusion and Its Implications
Peter Emanuel, *Army Futures Command*, and
Diane DiEullius, *Center for the Study of Weapons of Mass Destruction, NDU* 121

Contemporary Global Food Systems as Contested Space:
Implications for Special Operations Forces
Molly Jahn, *University of Wisconsin–Madison*;
David A. Bray, *Atlantic Council GeoTech Center and GeoTech Commission*;
Joseph Byrum, *Principal Financial Group*; LTG (ret.) Edward Cardon;
Tom Creely, *US Naval War College*;
Colonel Michael S. Gremillion, *US Air Force*; Aaron M. Kelly, *Jahn Research Group*;
Budhikka "Jay" Jayamaha, *United States Air Force Academy*;
Megan Konar, *University of Illinois at Urbana-Champaign*;
Seth C. Murray, *Texas A&M University*;
Tony Nguy-Robertson, *National Geospatial-Intelligence Agency*;
William L. Oemichen, *Jahn Research Group and University of Wisconsin–Madison*;
Michael J. Puma, *Center for Climate Systems Research, Columbia University*;
Jean-Paul Rodrigue, *Hofstra University*;
Matthew A. Rose, *General Services Administration's Centers of Excellence*;
Gregory F. Treverton, *Center for Strategic and International Studies and*
University of Southern California 148

As the Helix Turns:
How New Biology, Biometrics, and DNA Analysis May Forever Prevent Anonymity
Brad Hart and Brian Souza, *LLNL* 159

Table of Contents

SECTION 3
THE MATERIALS WORLD: POSSIBLE SOF APPLICATIONS

Additive Adversaries:
Enabling and Supporting the Warfighter with Additive Manufacturing
Lawrence E. Bronisz and Dominic S. Peterson, *Los Alamos National Laboratory (LANL)* 167

Nanotechnology and SOF: Is Smaller Really Better?
P. Randall Schunk, *Sandia National Laboratories (SNL)* 182

The Disruptive Potential of Advanced Energetics
Bryce C. Tappan and Patrick R. Bowden, *LANL* 193

Metamaterials: How Close Are We to a Klingon Cloaking Device
or Harry Potter Invisibility Cloak?
Michael T. Valley, *SNL* 209

Armor of the Future: Spider Webs, Buckyballs, Nanotubes, and Beyond
S. Robert Skaggs and Frank D. Gac (ret.), *LANL* 225

Emerging Trends in Flexible Electronics:
Opportunities and Challenges for a Clandestine Community
Brian T. Holmes and Michael W. David, *National Intelligence University* 241

Adapting SOCOM to an Electrified World
Karen Swider-Lyons, *US Naval Research Laboratory*; Joshua Lamb, *SNL*; and
Yet-Ming Chiang, *Massachussetts Institute of Technology* 253

SECTION 4
GLOBAL BUSINESS AND THE ROLE OF THE PRIVATE SECTOR
IN NATIONAL SECURITY: IMPLICATIONS FOR SOF

Cryptocurrency: Will the Digitization of Currency Allow Malign Actors
to Achieve Strategic Effects?
Sara Dudley, *USASOC* 269

Blockchain and the Battlefield
Girish Nandakumar, *Old Dominion University*, and Jon Cederquist, *Clearspeed* 283

The Significance of 5G for Special Operations of the Future
Toby Redshaw, *Verizon*. 293

On Being Stretch Armstrong:
Innovating Successfully inside Bureaucratic Organizations
Brad Chedister and Tambrein Bates, *SOFWERX*, and Jennifer J. Snow, *AFWERX/CTO* 305

Special Operations Forces as a Rapid Prototyping Laboratory
Leo Blanken, *NPS*, and Phillip Swintek, *USASOC* 322

SECTION 5
DIGITAL DOMAINS: THE SOF ROLE

Special Operations Forces and Cyber-Enabled Influence Operations
Herb Lin, *Stanford University,* and Trisha Wyman, *USASOC*. 333

The New COIN of the Realm: The Future of Technology and Insurgency
Peter Singer, *New America Foundation* 352

"Cyber FID": The Role of Cyber in Foreign Internal Defense
Philip Reiner, *Institute for Security and Technology*, and Whitney Kassel, *Morgan Stanley* 370

Open Minds, Open Societies, and Hybrid Conflict
David Bray and Vint Cerf, *People-Centered Internet Coalition*. 384

Artificial Intelligence: Risks and Opportunities for SOF
Paul Scharre, *Center for a New American Security*. 398

Weaponized Information: Influence and Deception in the Age of Social Media
Pablo Breuer, *Donovan Group*; David Perlman, *Copsycon*; and
Sara-Jayne Terp, *Bodacea Light Industries* 410

Table of Contents

SECTION 6

OPERATIONAL CONSIDERATIONS FOR MULTIDOMAIN WARFARE

Irregular as the New Normal: How Technology Will Change the Prevalence and Character of Irregular Warfare
Richard A. K. Lum, *Future Vision*, and Edwin Churchill, *Joint Special Operations Command (JSOC)* . . 447

Intelligence for Special Operations Forces
John Tullius, *NPS* 457

Systems of Systems: Coping with Pervasive Technology in Operating Areas
Mark W. Maier, *Aerospace Corporation*, and Edwin Churchill, *JSOC*. 465

The Whole World Is Watching: Special Operations in a Ubiquitous Surveillance Environment
George duMais, *FTS International*. 479

The Growing Importance of Subterranean Warfare and the Integration of General Purpose Forces in Subterranean Operations
Michael Alexander, *USASOC*. 486

Chaos and Constraint: Special Operations and "The Convergence"
Dan Leaf, *USASOC* 492

Few Weapons Are as Deadly as a Good Clock: Military Implications of 1:10^19 PNT
Robert G. Kennedy III, *Tetra Tech* 501

Megacities and Special Operations Forces
Margarita Konaev, *Center for Security and Emerging Technology, Georgetown University* 522

FINAL THOUGHTS ON LATENCY UNLEASHED

What Have We Learned?
Strategic Latency and the Future of Special Operations Forces
Zachary Davis, *LLNL/NPS* 536

Editor's Note

Zachary S. Davis

The Timing of This Manuscript

We started this project in 2018. It took two years to write and publish the chapters. Now it's 2021, and things have changed. The irony is not lost on us that while we were writing, the world kept spinning, and many of the things we predicted have since come to pass. Cyberattacks and disinformation campaigns have occurred as predicted, with devastating results. The global pandemic unfolded as some predicted. The global order is in further disarray. The scholars in this volume picked up on issues that were fresh and new when we started, and new issues have emerged since. It seems that, in some cases, the pace of events has compromised our ability to develop careful, reasoned, and thoughtful insights, at least in traditional forms of scholarship. These days, two years is a long time.

With this in mind, we created a digital multimedia version of the book in a format called a Mixonium, which includes additional materials for each chapter and can be updated by the authors. You can find the Mixonium for this book here: https://www.mixonium.com/#/public_clubs/599 (password: Beyond;20).

Technology channels people's motives and intentions at whatever pace of innovation they desire. The good news is that US SOF are also built for rapid adaptation, as noted by Hondo Geurts in his Foreword. And we take some comfort in the solutions we have proposed to accompany our warnings. But we need to take action on multiple fronts to ensure that we understand the threats and implement creative strategies that put us ahead of the curve instead of lagging behind it. Let's move out, before it's too late.

January 2021

Foreword

The Honorable James "Hondo" Geurts

> *"The ability to learn faster than competitors may be the only sustainable competitive advantage."*
>
> ***—Arie de Geus[12]***

Many saw it coming—the technology revolution, and its disruptive effects. Visionaries like Alvin Toffler, H. G. Wells, and Arthur C. Clarke gave the world decades of strategic warning, as they each, in their own ways, predicted how a new technological age would disrupt traditional thinking about national security. Private-sector innovators, not constrained by status quo or traditional bureaucracies, are now accelerating innovation at scale and in a way most previously believed possible only through government-funded megaprojects. Technologies, and the means with which they are being developed, are transforming both societies and the everyday activities of individuals at a dizzying pace. While there is consensus in the national security community that these vectors provide both new threats and new opportunities, the means and principles to adapt to them at the speed of relevance are far less clear.

Nowhere is the need for rapid adaptation more urgent than in our special operations forces (SOF), which serve as the touchpoint for so many of the nation's efforts to sense and cope with emerging threats and opportunities. Since their inception, special operations forces have been the nation's early adopters, leveraging curiosity, an unrelenting drive to experiment and improve, and tightly integrated teams of operators, acquirers, and technologists to lead the Department of Defense's transformation. From the early days of the Office of Strategic Services to the rapid adaptations of special operations forces in the post-9/11 conflicts around the globe, America's SOF have proven their ability to pivot, invent and adapt, and, where it makes sense, accelerate transition of these capabilities to other organizations to amplify innovations with scale and depth.

The success of special operations forces over the last several decades does not ensure future victory, however. Past success naturally leads to overvaluing the status quo and underappreciating the means and pace in which new thinking, driven by technological opportunities, can erode previous competitive advantages. Left unchallenged from within, the very things that have made the nation's special operations forces successful will likely become inhibitors to crucial transformation needed for future victories. Global competitors have seized the chance to enhance their competitiveness by exploiting technological opportunities others do not yet understand. If an organization's only sustainable competitive advantage is the ability to learn faster than its competitors, then it is imperative US SOF understand both

the future operational environment and the opportunities to blend new technologies, new thinking, and potential new relationships into winning strategies. That is why this book is so important.

In the chapters that follow, thought experts and experienced operators offer their insights into how special operation forces can exploit strategic latency to fight and win the conflicts of tomorrow as emerging technologies redefine operational environments, from the deep seabed to deep space. Through a wide variety of perspectives, the authors illuminate the opportunities to harness the latent potential of an expansive innovation ecosystem, from private start-ups to legacy providers, traditional lab organizations, and emerging nodes such as SOFWERX, AFWERX, NavalX, Defense Innovation Unit, and In-Q-Tel. The authors make the case that SOF must also similarly adapt from transactional and stovepiped approaches to highly integrated processes that close the distance between technologist, acquirer, and operator. Most important, these chapters reinforce the enduring power of teams and highlight SOF's proven ability to build and connect teams of highly capable people spanning traditional boundaries—now more than ever, this ability will enable SOF to lead the transformation to new systems, technologies, and thought processes.

The ability of US SOF to adapt and thrive in the age of technology is a harbinger of the larger challenges we face, in the military, the government, and society. Our special operations forces are uniquely positioned to lead the way in addressing these challenges and, in doing so, enable the United States to continue to be free, secure, and prosperous. This book—and all the contributers who have worked so hard on its content—will help guide special operations forces on its most critical missions for our nation.

Dedication

Lisa A. Owens Davis, 1966-2020
Wife, Mother, Daughter, Friend,
and National Security Expert

This book, *Strategic Latency Unleashed: The Role of Technology in a Global Revisionist Order and the Implications for Special Operations Forces*, is dedicated to Lisa Owens Davis, wife of Zachary (Zack) S. Davis, mother to Max and Sam Davis, daughter of Bill and Wendy Owens, friend to many, a national security expert, and a "special forces operator" in her own right.

Lisa succumbed to pancreatic cancer on February 26, 2020, after fighting valiantly for her life for seven months. Her story is inspiring for all. Lisa was born on the first day of spring in 1966, in Santa Barbara, California. She graduated from University of California, Santa Barbara with a degree in Spanish literature and a love for languages. She lived in Spain and worked at the Spanish consulate in Los Angeles, which sparked her interest in diplomacy. She taught English in the Czech Republic soon after the fall of the Berlin Wall and traveled extensively throughout eastern Europe and Russia in the days immediately following the collapse of the Soviet Union. Her adventures shaped her career, are indicative of her "special forces operator" skills, and made for long conversations during security-clearance reviews.

Lisa pursued he master's degree at the Monterey Institute of International Studies (now Middlebury Institute of International Studies at Monterey) and was one of William Potter's early graduates from the Center for Nonproliferation Studies, which he founded. She was an intern at the International Atomic Energy Agency (IAEA) and later returned to the US Embassy in Vienna, Austria to work on nuclear safeguards policy. Lisa was selected to the Presidential Management Program, which enabled her to serve in the Department of Defense and the Department of Energy (DOE), where she accepted a position managing nuclear safeguards support to the IAEA. At DOE, Lisa led delegations to numerous countries, funded research at national laboratories, served as lead DOE representative to the negotiations on the Additional Protocol, and chaired the interagency committee on safeguards technology. It was during the latter that she met Zack. In 1995, Lisa moved to the State Department and served as the chief of staff to Ambassador Norman Wulf, the US representative to the Treaty on the Non-Proliferation of Nuclear Weapons.

Lisa and Zack returned to their native California to work at Lawrence Livermore National Laboratory's Z Division, where Lisa quickly rose through the ranks to manage a wide range of analytic and operational intelligence support program. Throughout her professional career, she earned high praise for building bridges among diplomatic, military, intelligence, and technical agencies. Lisa also took delight in many hobbies and activities and will be missed by all.

Acknowledgments

Zachary S. Davis

This project was a massive cluster, if you know what I mean. With close to 40 chapters, almost 60 authors, five editors, multiple sponsors, a mix of technical, geopolitical, and operational information, security reviews, and management questions about the project, *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces* (SOF) required extreme collaboration. Fortunately, we assembled an extraordinary band of brothers and sisters who were motivated by the mission and not sidetracked by the usual bureaucratic distractions—or the pandemic, or social unrest, or crazy politics, or deployments, or any of the things that get in the way of good intentions. The contributors to this volume deserve all the credit and none of the blame!

Those of us who work for the government depend on managers and leaders who support our ideas and give us the freedom to pursue them. For us, the key was Joe Miller at Special Operations Command (SOCOM) J5. With his top cover, we were able to do things normally frowned upon, like spending weeks and months writing about our favorite topics. Also, a visit to Lawrence Livermore National Laboratory (LLNL) by former SOCOM commander Tony Thomas validated our ideas about bringing technology to the warfighter. The folks at SOFWERX and the Donovan Group are part of a sea change giving life to new ideas and unconventional thinking. As he did for previous Strategic Latency projects, Jim Stokes at the Pentagon funded key research projects at the Naval Postgraduate School (NPS) that form the basis of several chapters. The common thread was the future of SOF.

LLNL has consistently given me the freedom to develop the Strategic Latency program. Brad Hart at Z Program, Brian Souza (my cochair of the SOCOM working group), Chuck Lutes and Nalu Kaahaaina in the Office of Defense Coordination, Center for Global Security Research (CGSR) director Brad Roberts, CGSR deputy director Mona Dreicer, fellow cynic Wes Spain, Lara Telle, and the indefatigable Sandra Maldonado and Katie Thomas made it possible to do a project like this. The sharp wit and intellectual depth of Ben Bahney, Mike Markey, Harry Flashman, Jonathan Pearl, and Bruce Goodwin kept me honest, especially regarding issues of military history and multidomain conflict. No Strategic Latency publication would be complete without acknowledging the founding role of Ron Lehman.

At NPS, John Arquilla, Brian Greenshields, Leo Blanken, John Tullius, Tristan Volpe, and Brian Rose of the Department of Defense Analysis championed research on emerging technology and supported student interest in writing about technology and the warfighter, especially the SOF community. My students at NPS are the driving purpose behind this book and the inspiration for our devotion to the mission. They are the best of us.

My long suffering A-Team of coeditors—Christopher Rager, Frank Gac, Jen Snow, and Philip Reiner—deserve special recognition for their inspired leadership, keen-eyed editorial skills, and devotion to the mission. They were indispensable.

Finally, I lost my beloved wife Lisa Owens Davis in February 2020. She was a highly respected national security expert in her own right and contributed to previous Strategic Latency volumes. She is with us in spirit.

COEDITORS ACKNOWLEDGMENTS

Generally, coeditors do not provide acknowledgments—only the lead editor is endowed with that opportunity. However, in this case, we—Frank Gac, Chris Rager, Phil Reiner, and Jen Snow—would be remiss if we did not acknowledge the incredible contributions of Zachary S. Davis, whom we affectionately call Zack, to the success of this book.

Zack is the "brains behind the brawn." For starters, Zack pioneered the Strategic Latency concept, as it pertains to technology, with Ron Lehman in 2009. Basically, Ron is the "Father of Strategic Latency," Zack is the "Son of Strategic Latency," and we other editors are "kissin' cousins." This is the third book in the series, which also includes:

- *Strategic Latency and World Power: How Technology Is Changing Our Concepts of Security*, Zachary Davis, Ronald Lehman, and Michael Nacht, eds., 2014.
- *Strategic Latency: Red, White, and Blue—Managing the National and International Security Consequences of Disruptive Technologies*, Zachary S. Davis and Michael Nacht, eds., 2018.

Each publication has addressed specific issues and grown in complexity, which are testimonies to Zack.

Frank Gac

I have enjoyed being involved in this journey with Zack since the beginning and have seen Zack's inspiration, creativity, and doggedness firsthand. The latter has been particularly important for this third book, given the loss of Zack's dear wife, Lisa, to pancreatic cancer, and the "black swan event" of COVID-19. How Zack has continued in this endeavor has been nothing short of a miracle. Zack and Lisa have two sons: Max and Sam. We applaud them also in this endeavor and encourage them to be steadfast as they move forward.

Christopher Rager

First and foremost, I want to thank Zack for persuading me to lend my editorial skills to this project. It's been an honor to be part of a unique, forward-leaning endeavor that has gathered some seriously deep thinkers. I'm indebted to Zack for this opportunity. I'd also like to thank two of my colleagues from LLNL's Nonproliferation and Arms Control group, Paige Gasser and Cynthia Herrmann, who helped edit some of the enclosed chapters. Further, I'd like to express my gratitude to Jon Essner, Sean Monogue, and

Chris Herrington for permitting me to work on a book-length project given the many time constraints and commitments of our program. Finally, Zack's wife Lisa was a mentor to me and, in fact, recommended me for this project. She is missed by all of us who knew her.

A note about style. In general, I've tried to adhere to the *Chicago Manual of Style* 17th edition (online) and the Merriam-Webster online dictionary. Regarding endnotes, I mostly let author's determine the style of and format for endnotes in their respective chapters, though I often made slight adjustments for clarity and consistency. As you may notice, there is not a uniform bibliographic style to which I've asked authors to adhere.

Philip Reiner

There are requests for your time, then there are requests from Zack Davis for your time. Without pause, when asked to contribute to this effort, I could only be excited at the opportunity. Knowing Zack, and the Ron Lehman tradition he carries forward, has been both a personal and a professional gift for me, so I was more than honored to help lend a hand. What is at stake with this iteration of the Strategic Latency series is no less than the future success of our nations' special operations forces. There was a time when our men and women of the special operations community were always the first to receive the most cutting-edge tools and capabilities—this, unfortunately, is no longer the case. This book is in part an attempt to remedy that situation and to empower those who fight in the darkness on our behalf with tools they deserve, as adversaries move quickly to take advantage of our distracted and nearsighted current reality.

None of this would come together without the sheer unbridled force of will that Zack brings to all he does—nor would it have been possible without the deep love and affection that his wife Lisa gave to him and to all who knew her. Her loss hurt deeply. We all miss her immensely and dedicate this work to her commitment to serving her nation and ensuring its men and women had the tools they needed for the fight. To Zack, you have my steadfast loyalty, trust, and admiration—as a friend, father, husband, and patriot. Thank you for letting me be a part of this effort.

Lt. Col. Jennifer "JJ" Snow

When I approached Zack about taking this project on, I was aware of how much time and effort would be involved. I also knew Zack has zero quit in him, and he always turns out projects that exceed expectations. This latest edition of the Strategic Latency series is, by far, his best yet. Within these pages are the lessons that will guide and shape the next generation of technology influence operations for special operations forces, conventional forces, and our allies. I am exceptionally grateful for Zack's mentorship, friendship, and guidance on this project and the ones that came before and those yet to come. I miss Lisa greatly. She was a bright, vibrant, and strong innovator and leader. Her legacy will inspire many young women who chose to follow her path in national security. I am so glad I had the opportunity to know her. Thank you, Zack, for always standing strong for our special operations community even in the middle of your own battles and loss. You are someone who always inspires me to bring my best self to the fight.

Latency Unleashed: What It Means for Special Operations Forces

Zachary S. Davis

"Is it me, or is it getting crazier out there?"

—The Joker (2019)

It didn't have to be like this. The world could have evolved in different ways—toward a tranquil state marked by peace and cooperation, or on a trajectory of expanding chaos and violence. The current geopolitical situation is somewhere in the middle. While scholars analyze global politics and policy makers set the course of action, US special operations forces (SOF) adapt to both the peaceful and chaotic aspects of the operational environment to achieve mission objectives. This book contemplates the changing conditions under which SOF must operate and the role technology plays in making their jobs harder in some ways and easier in others.

"Strategic latency" refers to the potential for technologies to shift the balance of power among nation-states.[i1] "Strategic" effects have major, long-term consequences (in contrast to tactical effects that may be important but not game-changing). Latent power—expressed in the full range of military, economic, and political forms—can be *unleashed* to enable tools that people use to achieve their objectives. From the Stone Age to the Information Age, humans have wavered between peaceful and violent goals. Technology magnifies humanity's dual nature, predisposed to perform both good and evil deeds. Peering into the future, nothing suggests this fundamental truth will change. Thus, we should expect both conflict and warfare to endure and for SOF to play a leading role in future conflict. If war is an expression of "politics by other means," then technology will provide the soft- and hard-power tools with which wars will be fought. Therefore, SOF will have to employ appropriate technologies to ensure success in the evolving operational environment.

While human nature stays the same, other things are changing. The operating environment of world politics is undergoing a historic transformation. Nation-states remain the primary actors on the world stage, but the global balance of power is in flux. The "Long Peace" of the Cold War yielded to an interlude of American supremacy, followed by the current period of shuffling and realignment in which state and nonstate actors are challenging the norms, institutions, and alliances favored by the United States. The rules established to support the post–World War II global order are showing signs of weakness and decay. Countries and nonstate actors have violated

i We normally associate this shift in power with nation-states. However, we have learned that it can also be associated with regions and nonstate actors or entities like organized crime or business competitors.

international norms and treaties such as those prohibiting chemical weapons use, nuclear testing, and nuclear proliferation.

How much longer will the postwar norms hold, especially without verification or enforcement? Increasingly, key US allies question the security guarantees provided to address their fears of hostile neighbors, raising concerns they may break ranks to acquire nuclear, chemical, or biological capabilities. Rising powers, such as China, and revanchist states such as Russia and Iran welcome the demise of the aging American-led order, while nationalist movements around the world reject the core values of freedom and democracy that defined the American century. Tectonic geopolitical shifts are underway in Asia, Europe, and the Middle East, spilling into Africa and the Americas. Multicontinent mass migrations from poverty and violence have sparked fear and resentment from those who see refugees and immigrants as threats. Climate change is producing extreme weather, causing natural disasters and resource scarcity that directly affects the operational environment.[2] This is the new world that SOF encounters.

Further complicating the situation, a new generation of nonstate actors populate the landscape. Global corporations, many with no allegiances beyond their bottom line, pursue interests largely beyond the reach of nation-states. Activist groups advocate on behalf of people, animals, and myriad social causes, forming identities more tied to particular ideology than to national allegiance. Violent extremist organizations continue to thrive in the chaotic and ungoverned corners of the world, yet their messages of hate reach millions through social media, sometimes inspiring terrorism and rebellion. A common theme running throughout this changing ecosystem of states, groups, and individuals is the role of technology in giving force to their actions. How can US SOF find advantage amidst these conditions?

In contrast to the constancy of human nature, technology is changing at breakneck speed. Scientific discovery is accelerating, aided by the input of massive resources from governments and industries aimed at winning global competition for markets and influence, be it in communications, artificial intelligence, manufacturing, or health care. While US government–sponsored research and development has declined,[3] rising powers such as China pour human and financial resources into science and technology intending to reap the military and economic benefits.[4] Progress in the biological sciences, artificial intelligence, robotics, computation, and basic research fuels innovation in medicine, transportation, manufacturing, communications, and even entertainment. As the futurist Alvin Toffler predicted, a third wave of technology-inspired revolutions is remaking societies on a global scale.[5] The highly structured, brick-and-mortor industrial age is giving way to an era of nonhierarchical, individualized, instantaneous, global connectedness.

Often, technological changes reflect “the better angels of our nature” and bring improvements to the human condition. Sometimes, they serve the dark side of human nature and find expression as weapons of war. For example, fire, atomic energy, and computers have all fueled both peaceful and warfighting innovations. Gene editing and artificial intelligence may possess similar latent power.

Interconnectivity ensures the latest scientific discoveries will be available to all and puts the commercial applications of those discoveries in the hands of anyone with a credit card. Facebook, Google, Amazon, and their competitors have often forgone notions of privacy to create new levels of association among people, places, and things. Such witting and unwitting connectedness empowers all-encompassing surveillance systems used simultaneously for communication, commerce, and repression. How will SOF navigate this shifting landscape?

The Internet of Things promises even more connectivity. On the battlefield, a military version of the Internet of Things spans multiple domains, from subterranean and undersea, across the earth's surface, and into the atmosphere and outer space. The latent potential of drones and robots has already caused rapid innovation from both nations and nonstate actors. Interconnectedness begets data, which may soon challenge oil for its value as a strategic game changer. Echoing the words of the famous maritime strategist Alfred Mahan, "Whoever rules the waves rules the world,"[6] Russian president Vladimir Putin proclaimed "Whoever rules in artificial intelligence will rule the world."[7] Control of data may indeed be a strategic asset, but its value lies in the insights it provides into human behavior. New tools may not change humanity's fundamental nature, but they are changing how we live, govern, communicate, and fight.

Some scholars argue the risks associated with these global trends pale in comparison to the prosperity that defines our age.[8] Others view the risks as indicators of a gathering storm. One thing is certain: large-scale changes in geopolitics, spurred by technology, are changing the operational environment and, with it, the nature of warfare. For starters, the beginning and end of conflicts are getting harder to define, with gray-zone tactics becoming commonplace even in peacetime. Borders provide little protection from agressors, and the distinction between friends and enemies, be they nation-states or otherwise, is similarly blurred. Relatedly, the distinction between combatants and noncombatants has grown increasingly unclear. Even the rules of war are blurring, raising ethical questions about the uses of force, especially as the battlefield becomes less defined by physical or temporal boundaries and new weapons open uncharted paths of conflict and competition. To further confuse the situation, social media distorts perceptions of reality, exacerbating political differences.

US SOF must be prepared to meet a broad and growing array of challenges. When shadow wars are a constant background to international relations, and the spectrum of conflict extends from great power and peer competition through regional conflicts and proxy wars, calibrating effective SOF capabilities is more complex than ever. With more parties using an expanding toolbox of measures short of war to shape the environment, understanding the evolving threats to US security requires new insights. We must think differently. The purpose of this book is to open pathways for those new insights as they apply to the mission of US SOF. Fortunately, adapting to new threats is a notable strength of American SOF. Innovation is a defining

trait. SOCOM's experience fighting terrorism in the post-9/11 world provides many examples of the type of adaptation that is required for the new environment. Countering terrorism requires constant innovation in tactics and tools, in part because the practicioners of terror are themselves motivated innovators. Similarly, SOCOM's evolving role in countering weapons of mass destruction has spurred new approaches. This book is part of the effort to understand the threats, mobilize a response, and prepare US commandos with the tools they need to win.

To cope with these changes, however, it is not enough to perfect the "hyper-enabled operator"[9] or simply increase the range and lethality of the warfighter. Fortunately, the enduring SOF Truths[10] provide sturdy concepts for dealing with today's chaos and complexity. The five SOF Truths are listed below in quotations, followed by the authors comments as to how they apply to this chapter and book.

- "Humans are more important than hardware."

  Technology tools simply enable people to achieve their objectives. Understanding the constants of human nature provides insight into the intentions of our allies and adversaries. Tools are never more important than people. Technology must serve strategy.

- "Quality is better than quantity."

  What makes SOF special is the ability to understand and exploit the operational environment. Knowing which tools/technologies to use in specific circumstances and how to apply them requires uncommon knowledge of multiple disciplines. Such knowledge is rare but essential for SOF to deal with complexity and chaos. Knowledge is power.

- "Special operations forces cannot be mass produced."

  SOF are effective for certain missions but are not suited for all forms of conflict. Small teams of extraordinarily skilled, trained, equipped, and supported operators are tailored for speed, precision, stealth, and low visibility. This specialized capability augments general purpose forces and represents a small faction within the broader context of military, diplomatic, intelligence, and economic tools of statecraft. One objective of this project is to identify tools to maximize the reach, effectiveness, and resiliance of limited SOF resources.

- "Competent special operations forces cannot be created after emergencies occur."

  The Covid-19 pandemic of 2020 illustrated the problems that arise from trying to compensate for a lack of preparedness after the crisis has already struck. SOF cannot wait and react to the changes that are occurring in the world. We are preparing now for tomorrow's challenges. This book takes stock of the emerging operational environment and offers possible solutions to prepare SOF for future exigencies.

- "Most special operations require non-SOF assistance."

  To cope with complexity, SOF must deepen its relationships with a broad swath of society that is knowledgeable about the technologies and social movements behind the changes taking place in the world. This includes the private sector, academia, and people associated with unconventional points of view who can provide insights into the current situation. Beyond relying on general purpose forces, foreign partners, and the full range of capabilities available in the US government, SOF must engage with an expanding range of diverse, multidisciplinary, global perspectives, such as those presented here.

Taking guidance from these SOF Truths, and with full appreciation for SOF's Core Activities,[ii11] we have gathered a group of top experts from multiple disciplines, along with current and former SOF operators, to view developments in geopolitics, technology, and business through the eyes of American SOF. The book provides a compendium of SOF-relevant topics to illuminate important trends for irregular and unconventional warfare. The accompanying Mixonium multimedia platform offers additional insights and resources to those interested in these topics. The project intends to spark conversation and debate about these issues, so we invite you to join the discussion. Our contact information is available in this volume and on the Mixonium pages.

ii SOF Core Activities include Direct Action, Special Reconnaissance, Unconventional Warfare, Foreign Internal Defense, Civil Affairs Operations, Counterterrorism, Military Information Support Operations, Counterproliferation of Weapons of Mass Destruction, Security Force Assistance, Counterinsurgency, Hostage Rescue and Recovery, Foreign Humanitarian Assistance.

Endnotes

1 Davis, Zachary, Ronald Lehman, and Michael Nacht, eds., *Strategic Latency and World Power: How Technology Is Changing Our Concepts of National Security*, Livermore, CA: Lawrence Livermore National Laboratory, 2014.

2 Implications for US National Security of Anticipated Climate Change, Director of National Intelligence, September 2016, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Implications_for_US_National_Security_of_Anticipated_Climate_Change.pdf; Bases under Climate Threat Ranked, Defense News, June 13, 2019, https://www.defenseone.com/threats/2019/06/these-are-us-military-bases-most-threatened-climate-change/157689/print.

3 Gac, Frank D., Timothy P. Grayson, and Joseph M. Keogh, "What Works? Public-Private Partnerships for Development of National Security Technology," In *Strategic Latency: Red, White, and Blue—Managing the National and International Security Consequences of Disruptive Technologies*, Zachary S. Davis and Michael Nacht, eds., Livermore, CA: Lawrence Livermore National Laboratory, 2018.

4 Kania, Elsa, "In Civil-Military Fusion, China Is Learning Lessons from the United States and Starting to Innovate," *The Strategy Bridge*, August 27, 2019. https://thestrategybridge.org/the-bridge/2019/8/27/in-military-civil-fusion-china-is-learning-lessons-from-the-united-states-and-starting-to-innovate.

5 Toffler, Alvin, *The Third Wave*, Bantam Books, 1980. ISBN (hardcopy) 0-517-32719-8. ISBN (paperback) 0-553-24698-4.

6 Mahan, Alfred T., *The Influence of Sea Power Upon History*, 1660-1783, Boston: Little, Brown, 1890.

7 "Whoever Leads in AI Will Rule the World: Putin to Russian Children on Knowledge Day," September 1, 2017, RT News, https://www.rt.com/news/401731-ai-rule-world-putin, accessed June 26, 2019.

8 Pinker, Steven, *Enlightenment Now: The Case for Reason, Science, Humanism and Progress*, New York: Penguin Books, 2018; Peter Diamandis and Steven Kotler, *Abundance: The Future Is Better than You Think*, New York: Free Press, 2014.

9 "The Hyper Enabled Operator," Small Wars Journal, at https://smallwarsjournal.com/jrnl/art/hyper-enabled-operator.

10 SOF Truths, United States Special Operations Command, https://www.socom.mil/about/sof-truths, accessed 30 September 2019.

11 Core Activities, United States Special Operations Command, https://www.socom.mil/about/core-activities, accessed 30 September 2019.

12 de Geus, Arie. "Planning as Learning," *Harvard Business Review*, March 1988, https://hbr.org/1988/03/planning-as-learning.

SECTION 1

GEOPOLITICS OF STRATEGIC LATENCY FOR SPECIAL OPERATIONS FORCES

CHAPTER 1

Winning and Losing in Counterproliferation

Zachary Davis and Michael Greene

What does "winning" look like in the current counterproliferation (CP) mission space? This book is rich with insights into the geopolitical context within which special operations forces (SOF) must operate. How is "winning" defined in this megacomplex, hyperdynamic operational environment, when SOF are finding their place in the broad context of US national security and defense policy? What metrics and measures of performance are even appropriate? How do we distinguish between success and failure in an endless gray zone where wars are unacknowledged? One SOCOM mission that provides a useful case study in winning and losing is countering weapons of mass destruction (CWMD). We examine what it means for SOF to "win" in the effort to prevent more countries (or groups) from acquiring nuclear, chemical, or biological weapons and to mitigate the consequences if they do.

Nonproliferation (NP) refers to the mainly diplomatic efforts to persuade countries not to acquire weapons of mass destruction (WMD). The primary nonproliferation tools are security guarantees, alliances, multilateral agreements, international organizations, treaties, and global norms. Superficially, nonproliferation appears easy to measure: either a country gets WMD or it doesn't. In practice, however, countries may either acquire the capabilities needed to produce WMD covertly or develop latent production infrastructure that enables them to produce the necessary materials without violating any rules. Traditionally, preventing countries from crossing the boundary between civilian and military applications is considered a win for those trying to maintain global nonproliferation standards.

For SOCOM's CWMD mission, illicit acquisition of WMD production capabilities falls under the upstream defeat category. Wins and losses are measured in terms of a particular country or group's progress toward having WMD options. For example, persuading Japan or South Korea not to use their civilian nuclear infrastructure to produce nuclear weapons is a nonproliferation win. Failure to prevent them, or North Korea, or Iraq, from using their civilian nuclear capabilities to advance their covert weapons programs rank as NP failures. Iran hangs in the balance. But SOCOM would not have played much role in these failed nonproliferation efforts because SOF would not normally play a leading role in blocking illicit transfers of dual-use equipment, and no policy directive authorized attacks on their facilities. Where does SOF come into the picture?

Counterproliferation is oriented toward countries or groups that evade NP efforts and acquire WMD capabilities. "Winning" or "losing" in this context is harder to measure but focuses on limiting adversary abilities to deploy or use WMD in ways that threaten US interests. This is often a losing battle against a determined proliferator who is willing to resist NP pressures and pay the price required to get

WMD technologies. For example, Pakistan, India, North Korea, and Iran defied international pressure to advance their WMD aspirations. Counterproliferation includes policies and actions to roll back, disrupt, contain, and cope with adversary WMD programs that are advancing toward possession and stockpiling of nuclear, chemical, and biological weapons and delivery systems. This includes upstream efforts against latent programs that give the possessor the option of rapidly transforming civilian infrastructure into military weapons. For nuclear weapons, this includes the ability to enrich uranium or reprocess plutonium from spent reactor fuel. For chemical and biological weapons, CP focusses on industrial production of chemicals and pharmaceuticals for a wide variety of civilian purposes. If CP starts after NP has failed, SOF contributions to CP might be doomed to fail unless decision-makers are willing to authorize direct action against industrial sites, as occurred in the case of Israel's bombing of a covert Syrian reactor in 2007, the Stuxnet episode that disrupted Iran's centrifuges at Natanz, and possibly the reported 2020 damage at that same facility.[1] However, short of direct action, a more circumspect definition would give credit to disruption, interdiction, and other measures designed to slow down and complicate the weaponization process.

Categorizing SOF Priorities

Importantly, CWMD is a Department of Defense (DOD) construct not shared throughout the US government (USG). Most agencies are organized around NP and CP terminology, so measuring CWMD differs from either of the more established concepts. Therefore, determining the success or failure of SOCOM's role in DOD CWMD starts with identifying what is included in the SOF mission space—and what is not. SOF priorities fall into three categories: crisis response, pathway defeat, and early detection.

Crisis Response

Crisis response refers to the quick-reaction, technically prepared, and highly trained units that would be deployed to assess and render safe WMD that are not under the control of a nation-state. SOCOM has long prepared for such "loose-nuke" scenarios. The United States possesses a robust domestic and overseas CWMD crisis-response capability comprising numerous teams from various departments across the USG. Significant communication and collaboration exists across the crisis-response enterprise, resulting in a formidable whole-of-government capability postured for success. Nevertheless, there is room for improvement in the policy and communication aspects of the crisis-response mission, which we address later in this chapter.

Pathway Defeat

While the crisis-response effort is mature, robust, and coordinated across the whole of government, pathway defeat is a relatively new addition to the SOCOM lexicon,

although the term originated within the Naval Special Warfare community. For pathway defeat, operators trace back the proliferation networks and technological pathways that support the development of WMD programs to target critical nodes. Key DOD strategy documents embody this approach.[2] As we shall see, this mission space is already crowded with interagency collaboration, and the SOF role remains largely a work in progress.

Early Detection

Winning in CWMD depends on early detection. CWMD is not only crisis-response and/or pathway-defeat capabilities but also a coalition of foreign partners who possess similar (if not exact) capabilities able to detect and counter these threats away from the homeland. Essential to this vision is the USG and DOD's ability to exchange technological capabilities, communicate openly, and share sensitive intelligence. Outdated policies and a lack of requisite authorities prevent the effective and timely exchange of technology and/or intelligence.

Defining SOF Priorities for Success in CWMD

NP and CP focus generally on countries attempting to acquire prohibited weapons illicitly. While much attention has been given to the idea of "moving to the left of boom" to prevent adversaries from acquiring WMD capabilities in the first place—the nonproliferation realm—early detection and interdiction of WMD production equipment is already covered by an existing whole-of-government approach.[3] SOCOM can contribute to these ongoing efforts but is not replacing or competing with them via its concept of upstream defeat. A win for SOCOM in this mission space comes from supporting the coordinated efforts of intelligence, diplomatic, financial, and law enforcement agencies.

SOCOM has a rich legacy of such support in counterterror and counterdrug missions and can play a critical but niche role in executing CP policy. However, CP policy priorities are set by policy decisions, so relevant resources and authorities are directed and coordinated according to White House policy directives. In practice, this means no agency or department, including SOCOM and its subelements, is entirely free to pursue disruptive upstream actions without policy guidance. By contrast, SOCOM elements play a preeminent role in most crisis-response actions, although those too are guided by White House oversight and direction. Crisis-response roles and responsibilities are more clearly defined for nuclear weapons and less stringent with respect to actions involving chemical weapons, especially with respect to contaminated operational environments such as in Syria, where force-protection considerations are a priority. Biological threats present increasingly complex problems for readiness, whether human-made or naturally occurring. The ability to execute missions successfully in a WMD battlefield would constitute a major win for SOF. Conversely, the inability to execute missions because of WMD use, or threatened use, must be considered a loss. Advancements in detection,

personnel protective equipment (PPE), vaccines, decontamination, and other force-protection technologies are needed to limit the impact on SOF mission execution, whether focused on CP objectives or other urgent priorities.

As SOCOM adjusts its focus from CT to major-power competition, the SOF role in countering the WMD systems of peer competitors remains unclear, but would present major challenges. For example, upstream defeat has not traditionally focused on the strategic systems of de jure nuclear-weapon states, as defined under the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). Interdiction of proliferation networks and materials is directed mainly at nations and groups attempting to acquire WMD beyond the scope of their treaty commitments. Similarly, no major power admits to possessing chemical weapons, and all but a few countries have forsworn them via obligations under the Chemical Weapons Convention. Similarly, the Biological Weapons Convention outlaws all *offensive* biological weapons, but it lacks verification and enforcement mechanisms. SOCOM CWMD efforts are naturally directed at such illicit nuclear, chemical, and biological programs as part of the broader NP/CP policy of the USG. Winning in that context generally means contributing to the overall success of interagency collaboration.

Two Levels of Threat: Tactical and Strategic

These CP, NP, and CWMD issues can usefully be divided into two categories: tactical and strategic. There is a significant gap between the tactical capability to protect against or defeat a limited chemical threat[i] and a strategic threat from a yield-producing nuclear device that can be delivered on a missile. When assessing wins and losses, priority must be given to strategic threats that carry potential to damage the homeland and the American way of life significantly. One can imagine a wide range of nuclear, chemical, or biological threats that could achieve strategic effects, including economic and political damage. These contrast with important tactical threats that merit a vigorous response but are less likely to cause irreparable harm to core American interests. Below we outline several strategic threats that merit high priority for CWMD policy and operations and give examples of tactical threats that fall below the threshold of vital interest.

A Sampler of Strategic Threats from WMD: A SOF Perspective

Loose Nukes from Anywhere

A key element of existing and ongoing SOCOM responsibility in CWMD is the threat of "loose nukes": nuclear weapons not under the control of the nation that produced them. Because of the harm that a single such weapon could do to US or allied/partner forces, locating and disarming these weapons must rank as a top priority and a "no fail" mission for SOF. As stockpiles of nuclear weapons grow, the risk also

i For example, ISIS chemical weapons use in Iraq and Syria.

increases that imperfect security measures will result in a weapon being removed from custody. Growing arsenals in Russia, India, China, Pakistan, North Korea, and perhaps elsewhere could present appealing targets for those seeking to acquire a nuclear weapon. The render-safe mission also includes improvised devises either based on a stolen state weapon or constructed from illicitly acquired weapons-usable nuclear materials. This mission has rightfully ranked as a top priority for many years, and American SOF are positioned to win. However, current capabilities are limited and could be overwhelmed if more than a few weapons were to escape from custody and require multiple, simultaneous render-safe operations.

North Korea

While any hostile state that possesses the ability to threaten the US homeland with nuclear weapons must be considered a strategic threat, North Korea combines a number of factors that puts it in a class of its own. Historical animosities, the US-South Korean alliance, regional allies and adversaries, the risk of conventional war, and Pyongyang's decades-long commitment to its WMD programs have all made NP, CP and CWMD largely ineffective against North Korea's continued advancement of its WMD and missile programs. Despite successful interdiction efforts, determined proliferators overcome CP obstacles. Moreover, coping with North Korea's WMD during a war poses daunting challenges. In our view, the USG, DOD, and SOF are not postured for success and could actually fail to prevent a catastrophe if North Korea is able to use its WMD against the United States, South Korea, or Japan.

Peer Competitors

As stated previously, NP, CP, and CWMD policy has not focused on disrupting the WMD systems of peer competitors *in peacetime*. The presumption that deterrence is essentially a defense posture suggests major power's WMD are not intended as first-strike weapons. Of course, in wartime, limiting damage on the US homeland, troops, and allies makes foreign WMD systems fair game. Blunting Warsaw Pact WMD use in Europe was a US priority during the Cold War, one that diminished as Soviet forces withdrew. A reevaluation of peer and near-peer[ii] competitor WMD threats could suggest reprioritization of the threats from existing stockpiles.

Biological Wildcards

Whether of natural or human-made origin, biological hazards can cause strategic effects. As such, preparedness should be a national priority, and SOF should take steps to remain effective in the event of a wide spectrum of biological threats. To do less is to accept failure.

ii At least in terms of WMD capabilities.

A Sampler of Tactical Challenges from WMD: A SOF Perspective

Loose Chemical Weapons: A Tactical Problem

The term WMD lumps together a wide variety of dissimilar problems. Because of the challenges associated with using chemical weapons successfully on the battlefield, national chemical weapons programs may not constitute a strategic threat to the United States. Terrorist use of chemical weapons against military or civilian targets also is likely to be limited in its destructive effects. We believe terrorist use of chemical weapons would not necessarily meet the standard of strategic effects. Therefore, loss of control over chemical weapons, as was the case in Syria, should be considered a tactical threat. In the case of Syrian, ISIS's, and other group's use of CW in Iraq and Syria, the USG and DOD, specifically, enjoy a significant competitive advantage, as PPE is able to protect operators and render the enemy's chemical weapons ineffective. This constitutes a tactical win.

Radiological Weapons Not Strategic

Radiological dispersal devices have little military value and are mainly effective in producing fear in civilian populations. Granted, widespread fear of radiological exposure could be disruptive, including significant potential for economic harm. However, these are considered manageable risks that do not constitute strategic threats to the United States and are unlikely to undermine the effectiveness of SOF operations. Moreover, multiagency investments in consequence-management methods are in place to limit the effects of radiological hazards. We consider this a win against a tactical threat.

Biological Risks Can Be Managed

Many lessons can be drawn from the Covid-19 pandemic. For SOF, longstanding focus on readiness contrasts with the preparations that could have greatly reduced the impact of COVID-19 on society at large. But for SOF, aggressive force-protection procedures, vaccines, monitoring, and other specialized equipment can greatly reduce the threat posed by biological hazards, rendering them more of a tactical than a strategic threat. This, too, constitutes and important win for SOF.

What It Takes for SOF to Win against WMD

Counterproliferation is a team sport. Success requires the full range of USG capabilities and authorities to cover the full WMD development cycle, from cradle to grave, inception to employment. The selection of targets—which countries and proliferation networks to counter—and the methods used against them are policy decisions. The toolbox available to policy makers includes both positive and negative economic incentives, diplomatic agreements (such as the Joint Comprehensive Plan of Action with Iran or the Agreed Framework with North Korea), multilateral treaties such as the NPT and CWC, positive and negative security

assurances, and cooperative measures (such as Cooperative Threat Reduction [CTR] programs and the Proliferation Security Initiative [PSI]). Specific actions can include interdiction, sanctions, export controls, diplomatic engagement, military show of force, alliance cooperation, and covert action. Each of these depends on the specific skills, authorities, and resources available to the appropriate agencies of the USG, usually from the State, Defense, Treasury, Energy, Justice, and Commerce Departments as well as the intelligence community. Where do the activities of DOD, SOCOM, and its SOF elements fit in this mix?

US SOF possess a number of specialized skill sets that can contribute to the overall CP policy effort. Some are well-known and longstanding within the CP/CWMD community, such as the render-safe mission, countering terrorist WMD, and the ability to interdict ships suspected of carrying illicit cargo. Other capabilities, however, have not been exploited fully for CP purposes. For example, SOF teams regularly access remote areas where intelligence about local WMD-related facilities, organizations, and people may be hard to collect. Also, SOF training, support, and collaboration with local military and law enforcement provides an ideal platform for sharing best practices for a wide range of CP skills, as is done via CTR, PSI, and other partnership-building activities. Foreign internal defense training and exercises could include CP-related training modules where appropriate. Psychological operations could influence local perspectives on WMD, portray proliferation network operatives as corrupt, and support cooperative efforts. Preparation of the operational environment could be instrumental in planning CP operations, especially in hard-to-reach areas. A win for SOF would be to fill additional niche roles in the overall USG CP policy. A win for DOD CWMD is to bolster interagency collaboration on NP and CP.[4]

Endnotes

1 "Ending Secrecy, Israel Says It Bombed Syrian Reactor in 2007," New York Times, May 21, 2018, https://www.nytimes.com/2018/03/21/world/middleeast/israel-syria-nuclear-reactor.html; "Basic Attack Strategy of Stuxnet," Institute for Science and International Security, February 28, 2013, https://isis-online.org/isis-reports/detail/basic-attack-strategy-of-stuxnet-0.5/; "Update on Assessing the Detonation at the Natanz Iran Centrifuge Assembly Center: New High Resolution Satellite Imagery Refines Details on the Explosion and Fire," Institute for Science and International Security, July 9, 2020, https://isis-online.org/isis-reports/detail/update-on-assessing-the-detonation-at-the-natanz-iran-centrifuge-assembly.

2 Joint Publication 3-40, Joint Countering Weapons of Mass Destruction, November 27, 2019, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_40.pdf?ver=2020-04-09-140128-347.

3 Davis, Zachary, "Bombs Away," *The American Interest*, January 1, 2009.

4 Rautio, Matthew, "Fostering Inter Agency Collaboration for Upstream Counterproliferation," *Journal of Inter Agency Studies*, August 17, 2017.

CHAPTER 2

The Role of Special Operations Forces in Countering Weapons of Mass Destruction

Brendan G. Melley

The use of nuclear, chemical, and/or biological weapons against the United States and our allies and partners continues to be perceived as a low-probability event in the national security community. Yet, at a time when international norms and other constraints on the use of these weapons have grown weaker, they are becoming more accessible and attractive to adversaries because of their potential utility against a range of vulnerable targets. Major US strategy documents—including the 2017 National Security Strategy (NSS), 2018 National Defense Strategy (NDS), 2018 Nuclear Posture Review (NPR), 2018 National Military Strategy (NMS), and 2018 National Strategy for Countering Weapons of Mass Destruction Terrorism—identify countering the threat or use of weapons of mass destruction (WMD) as a critical priority for the United States.[i]

Emerging technology with WMD applications will further complicate the ability of the United States to prevent the acquisition of WMD capabilities by state and nonstate actors, contain and reduce WMD threats, and respond to crises, which are the core objectives of the 2014 Department of Defense (DOD) Strategy for Countering Weapons of Mass Destruction (CWMD).[1] WMD threats will become more challenging to counter as technologies develop—from capabilities that enable rapid analysis of massive amounts of data, to advances in the life sciences and new delivery methods, to cite a few important areas of innovation. Technology development cuts both ways, however, as US efforts to keep pace or gain advantage over adversaries' capabilities can assist with detecting and responding to WMD threats that may arise.

The WMD-related objectives identified in the national and DOD strategies rely implicitly on the roles of US special operations forces (SOF), whose capabilities are critical for competing and winning in this WMD-infected security environment. Core SOF capabilities work to shape the operating environment in the current "steady-state" landscape in a manner that serves to deter, dissuade, and frustrate adversaries from pursuing or aquiring WMD. US SOF's close relationships with foreign forces enable stronger partnerships to complement broad DOD or US government efforts against adversaries who possess or seek WMD capabilities. Below the level of armed conflict, SOF can disrupt the efforts of state and nonstate actors, including terrorists, who pose a threat of acquiring, developing, and employing WMD capabilities. In a crisis, SOF can counter imminent WMD threats through direct action,

i The views expressed in this paper are those of the author and are not an official policy or position of the National Defense University, the Department of Defense, or the US government. The author is grateful for the advice of Mr. Paul Bernstein, Mr. John Caves, Dr. Diane DiEuliis, Senior Chief Petty Officer, USN (Ret.) Michael Greene, and Mr. Dain Hancock in crafting this paper.

sabotage, unconventional warfare, or counterterrorism operations. With their global presence and reach, SOF remain a critical capability for meeting the United States' priorities for countering WMD.

The Emerging Strategic Environment and WMD

As we enter the third decade of the twenty-first century, US national security is being challenged as never before. The federal government's "fundamental responsibility is to protect the Amercian people, the homeland, and the American way of life."[2] The 2018 NDS summary presents a significant change in focus from that of the post-Cold War period, stating that the "central challenge to US prosperity and security is the reemergence of long-term, strategic competition" with China and Russia, shifting from the emphasis on counterterrorism following 9/11.[3] Not only are competitors seeking to compete with the United States militarily, they and some other state actors seek to undermine what we take for granted—rule of law, freedom of speech, a robust economic foundation, domestic stability, accurate information, and fact-based reason.

WMD threats are transregional and global, without regard to borders, designated areas of responsibility, or bureaucratic authorities, and the global community cannot wish away or uninvent these weapons. Nuclear, chemical, and biological weapons often are attractive to actors who seek advantage over their rivals or protection from outside intervention. With few exceptions, history has shown that states in possession of WMD will not give them up unilaterally.[ii] The perceived and real advantages to a state's security often outweigh external sanctions and pressure because possession of WMD are believed to create demonstrable deterrence or other leverage against foreign influence or attack. Analysts have long argued that North Korea uses its nuclear program to advance its political, diplomatic, and security interests.[4]

The continued threat from terrorist or other violent extremist organizations (VEOs) obtaining WMD remains a significant concern. The 2018 National Strategy for Countering WMD Terrorism, complementing the 2018 National Strategy for Counterterrorism, emphasizes "the need for continuous pressure against WMD-capable terrorist groups."[5] The strategy includes reducing and securing the agents, precursors, and materials needed by terrorists to acquire WMD, deterring states from providing support to terrorists with WMD ambitions, and detecting and defeating terrorist WMD networks.[6]

Moreover, the proliferation behavior of bad actors is increasingly putting pressure on the international nonproliferation regimes. Syrian and Russian use of chemical weapons show a flagrant disregard for their commitments under the Chemical Weapons Convention (CWC). Since the 1990s, the testing and deployment of nuclear weapons in South Asia, and North Korea's aggressive nuclear weapons program, have

ii For example, Belarus, Ukraine, and Kazakhstan removed or dismantled Soviet nuclear weapons on their territory after the fall of the Soviet Union, and South Africa's President De Klerk ordered the dismantling of its nuclear weapons in 1990.

demonstrated that states can successfully develop these capabilities outside of the constraints of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT).

The increasing pace of technological developments across all sectors of society, from the information sphere to public health, creates a significant potential for surprise to US security interests.[7] The United States will face challenges identifying and countering the rapid development of new and innovative technology with WMD applications. States will continue to accord the highest security protection to prevent discovery and disruption of their most sensitive programs; advances in computing power, encryption, and manufacturing capabilities can serve to hide secret programs, leading to fewer detectable signatures. Even as the United States harnesses these advancements for its own security needs, federally funded technology developments to detect and counter adversary WMD programs may not be sufficient. Close and continuous collaboration with innovators in the private sector will be essential, as markets likely will drive the commercial breakthroughs that provide the possessor with a competitive edge.

Since the early 1990s, several US initiatives, programs, and strategies have been created, to include more explicit guidance to SOF and joint forces to address emerging WMD threats in a post–Cold War environment.[iii] Concerns ranged from the security of WMD, associated materials, and expertise in the former Soviet Union, to the rise of "rogue" states who already possessed or were seeking nuclear, chemical, or biological weapons programs that would present a threat to US forces. Although the risk of an existential nuclear war may have declined, the likelihood of the use of WMD, especially chemical and biological weapons, by rogue states in regional conflicts had increased.

United States' WMD-Related Priorities

The United States' priority efforts, as stated in the 2017 NSS, include detecting and disrupting WMD, enhancing counterproliferation measures, and targeting WMD terrorists.[8] The NDS includes as a DOD objective, "dissuading, preventing, or deterring state adversaries and nonstate actors from acquiring, proliferating, or using weapons of mass destruction."[9] DOD cannot meet this objective on its own, as other federal agencies and departments have specific authorities for their nonproliferation and counterproliferation responsibilities.

By integrating and coordinating with the range of national security organizations across the US government, DOD must prepare to counter WMD threats before they materialize, while also preparing to "fight and win"[10] conflicts with WMD-armed adversaries and develop response capabilities needed to mitigate and recover from WMD use.[11]

Because the five prioritized challengers identified in the NDS—China, Russia, North Korea, Iran, and VEOs—already possess or are seeking nuclear, chemical, or biological weapons capabilities, joint force strategies and plans must recognize the range of WMD-use challenges across all levels of competition and conflict.

iii See, for example, the Defense Counterproliferation Initiative of 1993, the 2002 National Strategy to Combat Weapons of Mass Destruction, and the 2010 Quadrennial Defense Review.

Nuclear Threats

Competition among nuclear-armed states can negatively affect important US security interests, including relations with allies receiving assurance of US extended deterrence. Without a common view on geopolitical stability, there is potential for lasting damage to the global nonproliferation regime as more states consider nuclear weapons programs to defend their interests or pursue their goals.

- The actions of China and Russia to erode US reach, influence, and alliances simultaneously occur as they increase resources to develop and deploy advanced nuclear weapons and delivery systems, as a means to both coerce at the political level and to counter US and coalition advantages at the military level.
- North Korea is already a nuclear-armed state (though not a "nuclear-weapon state" as defined in the NPT). North Korea has successfully weathered decades of international pressure to develop nuclear weapons that can hold the United States and its allies at risk and protect the Kim Jong-un regime. Pyongyang also is suspected of supporting the nuclear program of Syria (set back by Israel in 2007) and Iran.[12]
- Iran may still aspire to possess nuclear weapons.[13] Preventing Iran from developing such weapons and delivery means has been a leading preoccupation of international diplomacy and US alliance relationships for over two decades.
- The dangerous potential of VEOs developing or acquiring WMD capabilities will not diminish, and preventing this will remain one of the nation's highest priorities. As stated in the National Strategy for Countering WMD Terrorism, "The growth in terrorists' capabilities and aspirations and the spread of dual-use technology have made the threat of weapons of mass destruction (WMD) terrorism progressively more acute."[14]
- Allies under the US nuclear umbrella have raised questions about the credibility of US extended deterrence commitments. Some have mused openly about their potential need to acquire their own nuclear weapons, as have some other states who do not enjoy formal US security guarantees.[15]

The potential need for joint forces to operate in a nuclear environment should not be discounted. Adversaries may choose to employ nuclear weapons in a limited way to disrupt or defeat conventional military operations. The 2018 Nuclear Posture Review (NPR) directs that the joint force "will plan, train, and exercise to integrate US nuclear and nonnuclear forces and operate in the face of adversary nuclear threats and attacks."[16]

Biological Threats

The ability to understand, manipulate, and utilize living organisms is ever increasing in capacity, worldwide dissemination, and economic penetration.[17] The application of advances in biology are driven largely by commercial interests, rather than government investments or policy, and science will continue to provide regular surprises. Technologies than can enable an adversary's biological weapons program are more widely available and less expensive, can reduce technical hurdles, and are increasingly accessible to small states and nonstate actors.[18] For example, improved aerosolization techniques for medical purposes has direct application to weaponizing and delivering biological agents.

Detecting and attributing biological attacks will become even more difficult as novel or a combination of agents can be developed and employed with few signatures. The ability to develop medical countermeasures rapidly will be challenged. In the early phases of a new infectious disease, governments may not be able to distinguish between a natural outbreak, accidental release, or deliberate attack. While the COVID-19 pandemic is the result of a naturally occuring disease, it is easy to see how a biological attack could overwhelm the joint force's ability to protect itself and accomplish assigned missions.

Chemical Threats

The bold and deadly use of chemical weapons in the last decade—by Syria and the Islamic State (ISIS) against foes and innocent civilians and by North Korea and Russia for assassination—demonstrate blatant contempt for international prohibitions on chemical-weapon employment. Russia's use of the lethal, nontraditional chemical agent Novichok in the United Kingdom in 2018 was another indication of Moscow's belligerent and brazen willingness to ignore the CWC.[19] Moreover, the Kim regime is responsible for the use of the lethal nerve agent VX to assassinate Kim's half-brother in Malaysia in 2017.[20] Diplomatic pressure, sanctions, and other legal action, have been the primary responses, though the United States twice struck Syrian military targets in response to highly lethal sarin attacks by the Bashar al-Assad regime.

In 2002, Russia used aerosolized chemicals with apparent incapacitating intent but deadly results to end a hostage siege (approximately 130 hostages died from exposure). While Moscow has never confirmed the agent that was used, analysis of survivors points to a mixture of fentanyl analogs.[21] Although "law enforcement including domestic riot control purposes" is not a purpose prohibited by the CWC,[22] the Scientific Advisory Board to the Organization for the Prohibition of Chemical Weapons (OPCW) has found the aerosolized use of central nervous-system acting chemicals (CNSAC), like fentanyl and its analogs, cannot be done safely, with the clear implication they are inappropriate for law enforcement use.[23] CNSAC, a subset of pharmaceutical-based agents, fuel concern that the CWC's law enforcement exemption could be exploited in ways unforeseen when it was negotiated. (The United States, Australia, and Switzerland are leading a diplomatic effort to preclude this.[24])

These actors, and others carefully watching, may have concluded impactful responses to chemical and perhaps biological weapons use are unlikely without clearly attributable violations of the treaties leading to punitive United Nations Security Council Resolutions. They may come to judge the advantages of the use of such weapons outweigh international consequences.

In this WMD security environment, the United States cannot discount that state actors that do not possess WMD may seek to acquire them, and states already in possession could seek more advanced capabilities. It is conceivable that new chemical and biological threats could emerge rapidly and be used in ambiguous or nonattributable ways across the spectrum of competition and conflict. Advances in chemical technology, including nanotechnology and microreactors, could yield new and superior forms of chemical weapons that are more capable against existing defenses, more discriminate, and/or harder to attribute. Nonstate actors, adversary SOF, or pseudoprivate specialized units may also use chemical and biological weapons clandestinely to avoid direct engagement with US joint or partner forces.

The United States should not assume that great-power competitors and rogue states will wait until armed conflict has begun to employ chemical or biological weapons. Given that adversaries have seen the United States overwhelm opponents in regional conflicts, they may choose, in a crisis or prior to the onset of armed hostilities, early use of WMD to disrupt joint and partner forces. Limited, plausibly deniable asymmetric attacks have the potential to prevent the United States from gaining air supremacy, denying territory, assembling offensive capabilities, supplying forces, or maintaining freedom of maneuver.[25] Chemical or biological attacks on partner soil could induce panic, impede movement, and destabilize friendly populations.

How SOF Can Contribute

The 2014 DOD Strategy for Countering Weapons of Mass Destruction identifies pathway defeat, a concept that originated in the 1990s, as an important task for the department. It defines pathway defeat as "deliberate actions against actors of concern and their networks to delay, disrupt, destroy, or otherwise complicate the conceptualization, development, possession, and proliferation of WMD, related expertise, materials, technologies, and means of delivery." Pathway defeat activities are intended to "create layers of complex barriers to impose recurring, collectively reinforcing, and enduring costs and setbacks on those seeking to acquire or proliferate WMD or related capabilities."[26]

Several core SOF activities can contribute to WMD pathway defeat objectives. The analysis and appreciation of the operational environment assists the joint force in planning and executing a range of military operations within a joint or multinational task force.

Their ability to understand regional dynamics through foreign internal defense and civil affairs activities, such as understanding the language and culture of

friendly nations, enable long-term relationships that engender trust in US forces. These efforts not only can prepare partners to counter insurgencies, defend against external attacks, and engage in coalition operations, but also provide the tools to help identify and respond to regional WMD risks before they materialize into threats. Additionally, it has been recognized that SOF missions are "almost always coalition in nature," which points to the strength that SOF bring to combined operations.[27]

Maintaining local and regional relationships enables SOF to influence adversary perceptions and behavior regarding WMD through activities such as military information support operations (MISO). These tactical and operational capabilities support overall strategic efforts to dissuade and deter competitors and adversaries' "conceptualization" of WMD intent,[28] and from developing, acquiring, or attacking with WMD. Influencing an adversary's cognitive end-state—that is, the perception of the costs and benefits of a WMD capability—is intended to reduce an adversaries' incentives to pursue, possess, and employ these weapons.

These global capabilities can quickly lead to the effective employment of military resources to "delay, disrupt, destroy, or otherwise complicate" WMD threats. When directed, SOF can respond rapidly around the globe to disrupt the early development and acquisition of WMD capabilities, and deliver kinetic and nonkinetic (e.g., cyber) effects on the WMD programs of hostile actors. SOF can employ long-range reconnaissance assets, conduct direct action and sabotage against WMD delivery and supporting systems (including command and control and logistics nodes), and disrupt adversary maneuver and logistics—all of which could be critical capabilities early in a crisis or prior to an imminent attack.

Moreover, US SOF are uniquely postured to counter adversary SOF activities, including the staging and use of WMD against targeted populations or joint and partner forces. SOF's rapid response to imminent WMD threats could reduce incentives for actors to employ WMD against US forces and interests. Adversaries also may hesitate to escalate with WMD if they understand that their weapons and delivery systems may be held at continuous risk of disruption or destruction. SOF's relationships with allies and partners built and maintained throughout its historic counterterrorism responsibilities are key to understanding and responding to today's VEO efforts to acquire WMD. As the commander of US Specical Operations Command (USSOCOM), General Richard D. Clarke, USA, stated, severing the "financial, messaging, and foreign terrorist fighter networks that enable and sustain VEOs" will "degrade and disrupt VEO attacks,"[29] including those with WMD. Importantly, continuous and aggressive US-led counterterrorist actions deny VEOs the time, space, and resources to develop or plan effective use of WMD.

In 2016, President Barack Obama authorized the transfer of responsibility for coordinating countering WMD activities in DOD from US Strategic Command (STRATCOM)to USSOCOM. According to the Joint Staff, a coordinating authority is the "designated lead for representing a problem set including topics such as planning, risk, prioritization, resourcing, synchronization of activities in plans, and

transition to contingencies."[30] In this capacity, SOCOM produced the DOD Functional Campaign Plan to Counter Weapons of Mass Destruction in 2018, which "nests under, cross-cuts, and complements the NDS, the NMS, and global and other functional campaigns."[31] This responsibility, along with the SOCOM commander's other coordinating authority roles for countering violent extremist organizations and MISO/WebOps, provide SOF the ability to understand and influence the planning for a range of DOD activities for addressing WMD threats.

In his April 2019 congressional testimony, General Clarke stated:

> *Our worldwide access and placement, our networks and partnerships, and our flexible global posture enable the department to understand adversary actions and intent and to respond across the spectrum of competition, especially below the threshold of armed conflict.*[32]

Since the end of the Cold War, SOF have maintained a high degree of focus on WMD contingencies and circumstances where their unique strengths can be applied. Alongside joint and partner forces, and other federal organizations, SOF provide robust, mature, and adaptive capabilities against WMD threats.

DOD's efforts to prevent and respond to WMD threats can take advantage of unique SOF capabilities to assist the joint force in planning and executing a range of military operations. Specific notional SOF roles,[iv] if directed, can consist of:

- Foreign internal defense and civil affairs activities, to include understanding the language and culture of friendly nations, enable long-term relationships that engender trust in US forces and provide the tools to help identify and respond to regional WMD risks before they materialize into threats.
- Cyber and military information support operations (MISO) that support overall strategic efforts to dissuade and deter adversaries' intentions for a WMD capability, shape the perspectives of leadership and the population on WMD activities, and reduce the incentives to pursue or employ these weapons.[33]
- Rapid responses to imminent WMD threats, including direct action and sabotage, can influence adversary perceptions of the costs and benefits of a WMD capability, demonstrating that their systems may be held at continuous risk from disruption or destruction.
- Countering adversary SOF activities can disrupt operational plans to stage or use WMD against targeted populations or US joint and partner forces.
- Continuous and aggressive counterterrorist actions can deny VEOs the time, space, and resources to develop or plan effective use of WMD.

iv Author's notional application of USSOCOM "Core Activities" (USSOCOM, https://www.socom.mil/about/core-activities) to NDS priorities.

SOF, Great Power Competition, and WMD

SOF's role in countering WMD threats from great powers likely will be more evident during an emerging crisis or actual conflict than in peacetime. While SOF can support US efforts to influence Russian and Chinese perceptions of the utility of developing, proliferating, or using WMD, direct action against the internal WMD activities of Russia or China may be limited because of the risk of escalation, absent a significant crisis leading to a presidential directive. Under precrisis conditions, diplomatic and economic activities likely would remain the preferred courses of action. A caveat to this judgment is warranted if chemical or biological attacks, traced to great powers, occur against allies or partners in situations short of armed conflict. Evidence of responsibility may negate efforts at deniability, and the president may desire SOF options for a response, which could involve asymmetric or direct actions.

Moreover, Russia and China play an important role with regard to achieving the US goals of denying North Korea and Iran's WMD ambitions. As permanent members of the United Nations Security Council, their veto power—and growing regional influence—complicates efforts to dissuade Iran from restarting its nuclear program, and to achieve the denuclearization of North Korea.[34]

There is unfortunately a wide generational gap between today's military professionals and those who experienced the Cold War standoff between the United States and Soviet Union. During the Cold War, US and NATO forces prepared for operations involving tactical nuclear, biological, and chemical weapons in an effort to disrupt and destroy a rapid advance of Warsaw Pact forces in a crisis.[35] Today, as joint force leaders with active service prior to the dissolution of the Soviet Union retire, DOD is undertaking the process of refining, adapting, and planning for both SOF options and DOD efforts against WMD capabilities during a crisis, a skillset new to many active-duty service members.

Conclusion

In the evolving security landscape, global tensions can increase as a result of miscommunication, mistrust, miscalculation, and the weakening of the rules-based international order. The breadth of SOF capabilities must be coordinated and integrated with all instruments of state power, and with allies and partners, to counter WMD threats effectively. Adversaries are not likely to risk major, force-on-force confrontation with the United States, in the near future, moving them to pursue asymmetric actions in the "gray zone."[36] In this environment, SOF likely will play a larger role for DOD. As potential adversaries sidestep US military superiority by competing below the level of high intensity armed conflict, and potentially employ ambiguous and targeted chemical and biological attacks to disrupt US military operations and weaken US resolve, SOF will be necessary to support early warning through partner relationships, and conduct SOF-unique asymmetric actions.

As Clint Eastwood's character famously said in the 1986 movie *Heartbreak Ridge*, "You improvise. You adapt. You overcome."[37] Reportedly an unofficial US Marine Corps

slogan, Eastwood's famous quote also aptly describes the capabilities SOF bring to deter and counter adversary WMD use. As the 2018 NDS reminds us, the security environment demands adaptation to "develop a lethal, agile, and resilient force posture and employment."[38]

Uncertainty demands being agile and flexible, and, as the NDS states, "strategically predictable but operationally unpredictable," and to "out-think . . . out-innovate" potential adversaries.[39] Confronting WMD threats before they fully materialize always will be preferable to responding to actual use. Once again, SOF activities make an important contribution to this task.

Although adversary use of nuclear, chemical, and/or biological weapons is often perceived as a low-probability event, there is a need for increased attention to the dramatic, potentially massively disruptive or even existential consequences of such use. Normative reluctance to use these weapons is eroding, and technological developments with WMD applications are advancing at breathtaking speeds.

The global COVID-19 pandemic, marked by surprise, speed, and mass disruption, demonstrates that both individual and unit preparedness for biological threats—whether naturally occuring or weaponized agents—requires the ability to rapidly detect, mitigate, and attribute biological agents. A reduction in force readiness caused by any biological release will negatively affect SOF and other forces deployed globally. This is perhaps a requirement that has not received necessary attention among junior and senior leaders, but the need is urgent—especially if SOF is to maintain its effectiveness against WMD threats in all levels of competition and conflict described above.

This outbreak highlights that education and leader development on WMD issues must keep pace with the demands of this new security environment. The NDS states unequivocally that professional military education (PME) has "stagnated, focused more on the accomplishment of mandatory credit at the expense of lethality and ingenuity."[40] Military officers (commissioned, noncommissioned, and warrant) and DOD civilians require a broad understanding of deterrence and countering WMD concepts, techniques, and strategies throughout their careers. Without this, the nation's leaders may not receive the best risk-informed military advice, and strategic and operational risk will be higher.

Because the United States may not be able to predict how the convergence of scientific and technological innovations may produce dangerous new WMD applications that terrorists may choose, "we must remain vigilant in identifying and responding to technological trends with nefarious applications."[41] SOF must pursue relentless innovation to prevent and disrupt proliferation and prepare for offensive actions to defeat WMD threats.

SOF has long recognized that "humans are more important than hardware,"[42] which naturally extends to the development of trained professionals who are prepared to develop and execute operations to counter adversaries' WMD capabilities. With its increased attention on the demands of the new security environment, SOF will remain one of the most effective weapons in the US arsenal to counter WMD threats.

Endnotes

1 "Department of Defense Strategy for Countering Weapons of Mass Destruction," US Department of Defense, June 2014, 9, https://archive.defense.gov/pubs/DOD_Strategy_for_Countering_Weapons_of_Mass_Destruction_dated_June_2014.pdf.

2 "National Security Strategy of the United States of America," The White House, December 2017, 4, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

3 "Summary of the 2018 National Defense Strategy of the United States of America," US Department of Defense, 2018, 2, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

4 Shane Smith, "Nuclear Weapons and North Korean Foreign Policy," in Adrian Buzzo (ed.), North Korea Handbook (New York: Routledge, forthcoming). See also Jonathan D. Pollock, "No Exit: North Korea, Nuclear Weapons and International Security," London: The International Institute for Strategic Studies, 2011; Michael Auslin, "How North Korea is Ensuring a Nuclear Arms Race in Asia," The National Interest, September 15, 2017, https://nationalinterest.org/feature/how-north-korea-ensuring-nuclear-arms-race-asia-22315, "Military and Security Developments Involving the People's Republic of Korea," Department of Defense, Report to Congress Washington, DC: 2019, https://media.defense.gov/2018/May/22/2001920587/-1/-1/1/REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-DEMOCRATIC-PEOPLES-REPUBLIC-OF-KOREA-2017.PDF.; Jonathan D. Pollock, "No Exit: North Korea, Nuclear Weapons and International Security," London: The International Institute for Strategic Studies, 2011; and Michael Auslin, "How North Korea is Ensuring a Nuclear Arms Race in Asia," The National Interest, September 15, 2017, https://nationalinterest.org/feature/how-north-korea-ensuring-nuclear-arms-race-asia-22315. The Council on Foreign Relations provides a helpful timeline of North Korean nuclear negotiations since 1985, at https://www.cfr.org/timeline/north-korean-nuclear-negotiations.

5 "National Strategy for Countering Weapons of Mass Destruction Terrorism," The White House, December 2018, i, https://www.whitehouse.gov/wp-content/uploads/2018/12/20181210_National-Strategy-for-Countering-WMD-Terrorism.pdf.

6 "National Strategy for Countering Weapons of Mass Destruction Terrorism," 1.

7 James Kadtke and John Wharton, "Technology and National Security: The United States at a Critical Crossroads," Institute for National Security Studies, National Defense University, Defense Horizons, March 2018, 7, https://inss.ndu.edu/Portals/68/Documents/defensehorizon/DH-84.pdf.

"Department of Defense Strategy for Countering Weapons of Mass Destruction," US Department of Defense, June 2014, 8, https://archive.defense.gov/pubs/DOD_Strategy_for_Countering_Weapons_of_Mass_Destruction_dated_June_2014.pdf.

8 "National Security Strategy of the United States of America," 8-11.

9 "Summary of the 2018 National Defense Strategy of the United States of America," 4.

10 "Summary of the 2018 National Defense Strategy of the United States of America," 3.

11 "National Strategy for Countering Weapons of Mass Destruction Terrorism," 10; and "Department of Defense Strategy for Countering Weapons of Mass Destruction," 11.

12 Bruce E. Bechtol, Jr, "North Korea's Illegal Weapons Trade: The Proliferation Threat From Pyongyang," Foreign Affairs, June 6, 2018, https://www.foreignaffairs.com/articles/north-korea/2018-06-06/north-koreas-illegal-weapons-trade.

13 "Iran's Nuclear Program: Status," Congressional Research Service, December 20, 2019, 2, https://fas.org/sgp/crs/nuke/RL34544.pdf.

14 "National Strategy for Countering Weapons of Mass Destruction Terrorism," I.

15 See Richard N. Haass, "The Coming Nuclear Crises," Council on Foreign Relations, November 19, 2019, https://www.cfr.org/article/coming-nuclear-crises; "Erdogan says it's unacceptable that Turkey can't have nuclear weapons," Reuters, September 4, 2019, https://www.reuters.com/article/us-turkey-nuclear-erdogan/erdogan-says-its-unacceptable-that-turkey-cant-have-nuclear-weapons-idUSKCN1VP2QN;
Henry Sokolski, "In the Middle East, Soon Everyone Will Want the Bomb,
Foreign Policy, May 21, 2018, https://foreignpolicy.com/2018/05/21/in-the-middle-east-soon-everyone-will-want-the-bomb/; and https://www.washingtonpost.com/news/worldviews/wp/2017/09/13/most-south-koreans-dont-think-the-north-will-start-a-war-but-they-still-want-their-own-nuclear-weapons.

16 "Nuclear Posture Review," Office of the Secretary of Defense, February 2018, 21, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

17 Diane DiEuliis, "Key National Security Questions for the Future of Synthetic Biology. Global Transformations: A Century Since the Great War," in The Fletcher Forum of World Affairs, Winter 2019, 43:1. https://www.fletcherforum.org/archives/2019/2/4/431-winter-2019.

18 Natasha Bajema, et al., "The Digitization of Biology: Understanding the New Risks and Implications for Governance," https://wmdcenter.ndu.edu/Publications/Publication-View/Article/1569559/the-digitization-of-biology-understanding-the-new-risks-and-implications-for-go/.

19 "Joint Statement on the Salisbury Attack," Office of the Spokesperson, US Department of State, September 6, 2018, https://www.state.gov/joint-statement-on-the-salisbury-attack/.

20 "Imposition of Chemical and Biological Weapons Control and Warfare Elimination Act Sanctions on North Korea," Press Statement, US State Department, Washington, DC, March 6, 2018, https://www.state.gov/imposition-of-chemical-and-biological-weapons-control-and-warfare-elimination-act-sanctions-on-north-korea/.

21 "ECBC Researches Metabolic Carfentanil Reactions, The R&T Connection, Edgewood Chemical Biological Center, 7, July 2017, https://www.cbc.ccdc.army.mil/wp-content/uploads/2018/04/RTconnection_toxEdition_26July17.pdf.

22 Chemical Weapons Convention, April 29, 1997, Article II, 9(d), https://www.opcw.org/chemical-weapons-convention/articles/article-ii-definitions-and-criteria.

23 Christopher M. Timperley, Chairman, Scientific Advisory Board, Organization for the Prohibition of Chemical Weapons, "Central Nervous System Acting Chemicals – The Scientific Perspective," presented to the Conference of States Parties 22, The Hague, Netherlands, November 27, 2017, https://www.opcw.org/sites/default/files/documents/SAB/en/SAB_Chair_Presentation_at_CSP22_Side_Event_on_CNS-Acting_Chemicals.PDF.

24 Statement by H.E. Ambassador Heinz Walker-Nederkoorn, Permanent Representative of Switzerland to the OPCW, at the Ninety-Second Session of the Executive Council, EC-92/NAT.17, October 11, 2019, https://www.opcw.org/sites/default/files/documents/2019/10/ec92nat17%28e%29.pdf.

25 "Summary of the 2018 National Defense Strategy of the United States of America," 3.

26 "Department of Defense Strategy for Countering Weapons of Mass Destruction," 10.

27 "JTF C2 and Organization," Second Edition, Joint Staff J-7, January 2020, 5, https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/jtfc2_fp2nd_ed.pdf?ver=2020-01-13-083433-550.

28 "Department of Defense Strategy for Countering Weapons of Mass Destruction," 1.

29 Clarke, General Richard D. "Statement before the House Appropriations Committee, Defense Subcommittee," 5.

30 "Management and Review of Campaign and Contingency Plans," Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3141.01F, January 1, 2019, A-3, https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%203141.01F.pdf?ver=2019-03-18-121700-283.

31 General Raymond A. Thomas III, USA, "Statement before the Senate Armed Services Committee, Washington DC, February 14, 2019, 5, https://www.armed-services.senate.gov/imo/media/doc/Thomas_02-14-19.pdf.

32 General Richard D. Clarke, USA, "Statement before the House Appropriations Committee, Defense Subcommittee," Washington, DC, April 9, 2019, 5, https://docs.house.gov/meetings/AP/AP02/20190409/109281/HHRG-116-AP02-Wstate-ClarkeR-20190409.pdf

33 "Department of Defense Strategy for Countering Weapons of Mass Destruction," 1.

34 "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for US National Security," Minority Staff Report, Committee on Foreign Relations, US Senate, 115th Congress, 2nd Session, S. Prt. 115-21, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

35 For example, see "Basic Nuclear/Chemical Offensive Considerations," Nuclear, Chemical and Defensive Biological Operations, United States Marine Corps, FMFM-11-1, 20 May 1975, Ch. 9; US Embassy Paris Telegram 4422 to State Department, "NATO Nuclear Planning Group: What Happened at Ankara," Secret (declassified), September 30, 1967, the George Washington University, National Security Archive, https://nsarchive2.gwu.edu//dc.html?doc=6532129-National-Security-Archive-Doc-15-U-S-Embassy; Adam Rawnsley and David Brown, "The Littlest Boy," Foreign Policy, January 30, 2014, https://foreignpolicy.com/2014/01/30/the-littlest-boy/; and Bill Wilson, "The Fulda Gap," Military History Online, May 31, 2014, https://www.militaryhistoryonline.com/Modern/FuldaGap.

36 "Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission," v, United States Institute of Peace, November 13, 2018, https://www.usip.org/publications/2018/11/providing-common-defense.

37 Heartbreak Ridge, Directed by Clint Eastwood. Distributed by Warner Bros. Pictures. 1986.

38 "Summary of the 2018 National Defense Strategy of the United States of America," 7.

39 "Summary of the 2018 National Defense Strategy of the United States of America," 5.

40 "Summary of the 2018 National Defense Strategy of the United States of America," 8.

41 "National Strategy for Countering Weapons of Mass Destruction Terrorism," 12.

42 General Richard D. Clarke, USA, "Statement before the House Appropriations Committee, Defense Subcommittee," 2.

CHAPTER 3

Identity and Virtual Nations: Implications of Digital Citizenship and Developing Global Autonomous Communities for Special Operations Forces

Lt Col Jennifer "J. J." Snow

Introduction

Virtual nations are the latest in a series of unusual emerging global actors. An addition to the well-known nation-state, aspiring nation-state, and more recent rise of violent extremist organizations (VEOs), virtual nations pose unique challenges to the future of governance and the role of the nation as the sole grantor of identity and citizenship. In the context of this chapter, I define a virtual nation as an individual, group, or corporate entity that derives power from high capital resources or high data resources, allowing for the influence and successful massing of decentralized digital power to achieve physical effects at the state, national, or regional level.

Virtual nations may be self-, state, or nonstate sponsored or self-assembling entities. Examples may include high-net-worth individuals like Mark Zuckerberg; alternative governance entities like Bitnation, eCitizens of Estonia, and Cyprus and United Arab Emirates (UAE) real-estate-for-citizenship schemes; corporate entities, including Facebook, Google, Amazon, or Apple; and certain self-assembling groups with specific shared goals, such as the hacker collective Anonymous. These entities are focused on the pursuit of specific individual or group goals to influence or shape key events, drive change, or, in a worst-case scenario, seek to cause chaos or decision paralysis to limit the effectiveness of traditional governance structures and tools. This chapter examines the latest radical developments in identity and governance and the challenges these pose for special operations forces (SOF), the U.S. military, and U.S. allies.

Drivers of Change: How Exclusion Birthed the Rise of Global Citizenship

> *"I believe the nation-state oligopoly is being phased out naturally, due to the forces of globalization, and we're obviously trying to help fast-forward that process."*
>
> ***—Susanne Tarkowski Tempelhof, Bitnation founder[1]***

Susanne Tarkowski Tempelhof grew up in a family considered *stateless*—people living at the margins without the identification, benefits, or the security that comes with being a national citizen. According to the United Nations, at least 10 million people globally live in this condition. Stateless populations continue to grow as policies designed to secure countries against terrorism block immigration, ethnicity restrictions

limit options to obtain citizenship, and regional conflict and crises zones contribute to massive displacement events, leaving many with no place to go.[2]

In Tempelhof's case, growing up stateless led her on a quest to fix these issues for others suffering the same challenges. She began a career in advertising, seeking opportunities to learn how to gain support and influence for ideas by smart branding. After a time, Tempelhof earned a position in government hoping to be able to drive policy change on immigration from within the system. Her work for the US government landed her a lucrative opportunity that she turned into a highly successful strategic communications company that conducted specialty projects across the Middle East.[3] Her involvement in various conflict zones, where she undertook nation-building tasks, taught her not only how states operate but also how they can be successfully deconstructed and rebuilt anew. This experience gave Tempelhof the expertise and know-how necessary to navigate international law using information operations and unconventional warfare, especially gray-zone operations, to create new governments on the fly.

While her company was successful at reshaping governments in conflict, Tempelhof still could not create the changes for immigration policy she so desparately hoped to achive. Frustrated by her lack of progress and determined to find a solution that would make citizenship an open option for those without, Tempelhof sold her company. Next. she announced she would begin an experiment, the goal of which would be to create a government that was a viable alternative to the existing nation-state system, one in which anyone who wanted citizenship could have it. Her goal was to establish nonterritorial, corporate-like governance models as a successor to the nation-state model. Her believe that this could be done was driven by the emerging models founded on recent sweeping technological advances seen in the internet, blockchain, and cloud computing communities. Tempelhof's initiative, Bitnation, provides digital identity solutions, notary services, and birth, marriage, and death certificates on the blockchain. It also provides smart contracts for businesses and various nonstate actors and stateless populations.[4] Of the many communities that convinced her to change her tactics, the most influential was the Facebook community and founder Zuckerberg.[5]

Facebook provides an example of how communities can assemble at a local, national, or regional level using digital space around shared areas of interest to influence and drive change—for better or worse. The internet has long been a home to the displaced, the isolated, those seeking acceptance, and tribes built around shared values, ethics, and beliefs. These groups create transnational digital communities capable of driving tangible change across national and regional boundaries. Some are organized based on refugee migration patterns and keep immigrants connected to family and cultural or religious belief systems they left behind. Others organize around specific goals, ideologies, or politics. All have the population to mass decentralized power and project influence rapidly if appropriately incentivized to do so. With the right leadership, these populations have the potential to change the world.

Simple examples of the effects of individuals marshalling *new power*—the ability to harness the energy of digitally connected populations to drive change in the real world—include the #MeToo movement; the Ice Bucket Challenge; Movements.org, a site that connects human-rights activists with supporters around the globe to establish partisan networks; and the Global Climate Strike, the latter of which was inspired by social media postings of 16-year-old Swedish environmental activist Greta Thunberg, leading to 2,500 events worldwide and attended by almost four million people.[6] New power is transparent, available, and easily accessible to everyone who knows how to use it. And it just might be the next factor to change what government looks like and how identity works in the future.[7]

In a model that looks strikingly similar to Bitnation, Zuckerberg announced his plan to establish an alternate financial infrastructure that will be interoperable with most global currencies and will enable the execution of smart contracts between parties. In essence this effort building off of existing Facebook communities constitutes the first true attempt at a nonterritorial corporate state. Zuckerberg's Libra cryptocurrency—which has financial backing from Visa, Spotify, PayPal, and others—will be the first true global digital currency. There are multiple opportunities here: Facebook could establish new forms of governance, new digital economies, and alternative financial options for the unbanked; it could create an entirely novel global financial system. If Libra is launched successfully, these combined actions could allow Facebook to maintain primacy by leapfrogging ahead of traditional financial services to capture businesses seeking greater fiscal agility in emerging markets and resulting in an overmatch situation.

The use of nongovernment-influenced banking options are expected to be in high demand from massive unbanked populations in Africa and Southeast Asia.[8] The joined populations of these regions constitute 2 billion people and growing, a massive untapped market.[9] If Zuckerberg choses to move forward with this plan, will existing nations even be able to stop it? His ability to mass decentralized digital new power from online populations, scale it, and build the first global sovereign virtual nation is entirely outside *old power* nation-state control. There are no rules for these kinds of actions because this kind of power didn't even exist before 2000.[10]

Many argue that such an initiative will never succeed, that there are no grounds to support the creation of a virtual nation or alternative forms of identification, that Templehof and Zuckerberg are just two extreme dreamers. And they would be wrong. Multiple examples already exist of virtual nations and alternative identities that are not just surviving but thriving, backed by both nations and nonstate actors aiming to capitalize on these new technological opportunities to boost growth, access, and power on the world stage.[11]

Estonia was the original adopter of digital identification and the construct of the "nation as a service" (NAAS), starting with its e-residency program and then their establishment of digital embassies to back up blockchain-based services securely. The Estonian government successfully moved a majority of services to the blockchain,

including benefits and tax filing; marriage, birth, death, and divorce certificates; smart contracts for business interactions; and even voting. Services are more or less transparent and work in the background, automatically providing the appropriate benefits and forms, while also allowing citizens to have full access to all their records, all the time, in a secure environment.

Eventually, NAAS models may drive competition between virtual nations and actual nations as they compete to provide the best services, drawing the best and brightest to their countries to benefit them economically, militarily, and diplomatically. Early adopters and some fast followers will have the advantage, making them ever more competitive as they fine-tune their campaigns to citizen needs and wants. These efforts will be further advanced by leveraging the growing sea of data available on every individual as they interact with the internet, their phones, and other peripherals during daily life. Identity controlled by the nation-state, exemplified by the the Social Credit System popularized in China to "improve security," will benefit closed societies in maintaining control, while liberal democratic states may choose to advocate for individual control of one's personal data. In the latter case, having control of one's personal data is a plus and may also function as a mechanism for monetizing specific aspects of that data for nations, researchers, or companies to lease or buy from the owner. It may also allow the owner to see where their data resides, who is interested in it, and potentially for what purpose.

As of 2020, all of Estonia's citizens (1.3 million), 6,000 new companies, and 50,000 digital citizens from its e-residency program are using their identification to access the Estonia digital services environment globally. Azerbaijan has also implemented an e-residency program after seeing the economic advantages experienced by Estonia, including the savings gleaned from reducing the amount of government administration by lessening the process and paperwork required. Bitnation has slowly grown and now has 15,000 digital citizens using its infrastructure for vital records, smart contracts, identification, and other licensing. Bermuda started a citizen authentication program in 2019 to test an e-ID system. As of 2019, Catalonia was building a decentralized identity platform with online government services called IdentiCAT. Thirty-three other nations, including Belgium, Finland, Germany, Israel, Nigeria, Poland,and Malta all have e-ID systems in place. These systems allow citizens to access government benefits, banking, and personal records, and they allow citizens to sign digital documents electronically for business contracts. These e-ID cards have varying applications within each nation, some strictly for banking, others covering a wider area of government applications as well as business and banking. As these kinds of identification become more prevalent globally, the ability to travel discreetly or under an alternate name that is accurate to an individual's biometrics will become much more difficult, limiting criminal and blackmarket operators but also impacting clandestine intelligence operations.[12]

This is not the only new development in the rise of digital identity and virtual nations. The real-estate citizenship market is a growing sector. Cyprus, Greece, the

UAE, and Estonia offer citizenship options through real-estate purchases. In Cyprus, newly constructed or yet-to-be-constructed apartments and condominiums come with something called a "golden visa." This concept was originally set up in the Caribbean and has been adopted in parts of Europe, allowing foreigners to buy their way to citizenship through the purchase of property. For example, an investor in real or *virtual real estate* (properties not yet built) in Cyprus also conveys citizenship to the buyer in not just one country but also in the European Union. In this version of virtual identity or virtual nation, the citizens derive their rights and benefits from investment and legal charters without having to ever step foot in the country or do business there.

Greece, Portugal, and the UAE all have various fees for their golden visa programs; some are legitimate and some are black-market scams. This space is not well regulated. China also has invested heavily in this space and provides a sliding payment scale of options depending on the kind of citizenship one is looking for, their ability to travel, and their Social Credit score if they are a Chinese citizen. These types of virtual citizenships are recognized and may grant tax advantages and other benefits; however, they can also provide a mechanism to evade national or international law for those engaged in illicit activities, especially if the state of alternate citizenship lacks an extradition policy. While in some cases identification may make it easier to track individuals globally, in others, it may make them equally untouchable under existing legal frameworks.[13]

Beyond these nation-states attempting to create hybrid systems that leverage old and new structures of governance or those growing digital states that extend far beyond their physical borders exists one more category of virtual nation: the corporation. These are global companies that are changing roles, moving from participant status under existing nation-state rules to *market maker* status, where they begin to set and establish their own rules outside of state influence and control. Data is king, and companies like Facebook, Google, Apple, and Amazon are pushing the boundaries of governance. In many instances they seek opportunities to remove government in favor of their own *functional sovereignty*.[14]

As a nation cannot or will not fulfill specific regulatory or policy obligations, private-sector powerhouses are stepping in to create their own form of legal jurisdiction. These controls are designed to address a problem, but unlike a nation, the primary consideration is always to protect and advance the corporation's agenda in the digital political economy. This is a perfect mechanism by which an entity can accumulate decentralized power, via the customer or end user, and apply it globally to achieve tangible results. For example, Amazon is a global corporation, an international marketplace, a logistics provider, a cloud-service solution, a creditor, an electronic-payment provider, a data collector, a crowdsourced workforce (Mechanical Turk), and more. It is such a distributed, transnational actor that no one government can claim control over it. In essence, Amazon has replaced the government as the primary broker of law because no single entity can provide the same level of service or control. As Frank Pasquale, University of Maryland law professor notes in one of his articles:

> *Rory van Loo has described the status of the "corporation as courthouse"—that is, when platforms like Amazon run dispute resolution schemes to settle conflicts between buyers and sellers. Van Loo describes both the efficiency gains that an Amazon settlement process might have over small claims court, and the potential pitfalls for consumers (such as opaque standards for deciding cases). I believe that, on top of such economic considerations, we may want to consider the political economic origins of e-commerce feudalism . . . .The evisceration of class actions, the rise of arbitration, boilerplate contracts—all these make the judicial system an increasingly vestigial organ in consumer disputes. Individuals rationally turn to online giants for powers to impose order that libertarian legal doctrine stripped from the state. And in so doing, they reinforce the very dynamics that led to the state's etiolation in the first place."*[15]

Entities like Amazon are enjoying a rapid transfer of power from government because government is limited in ways that make its ability to operate successfully at speed in a technology-influenced environment an impossibility. So instead of reducing barriers inside the bureaucracy, government organizations slowly start to give away power to contracted corporations to execute on its behalf. This began at the end of World War II and is a legitimate threat to national security. Examples include Amazon Cloud for Department of Defense (DOD) or Google's Project Maven. What happens when critical DOD processes, logistics, acquisitions, and equipping functions are completely taken over by Amazon in the future? Does Amazon have the ability to leverage this power as control? The more power given to these actors the less power and control the government has to operate independently. What happens if a certain division decides to strike because they do not believe in supporting a specific mission set? What if another nation-state pays for them to strike to cripple the capability or another state? What recourse will a commander have if a company decides to turn off or withhold a capability? How much of the DOD intelligence and operational capability is currently reliant on outside entities that they do not control?

Pasquale concludes his observations of this transfer of power from government to the private sector with the following cautionary note:

> *Understanding the bigger picture here is a first step. Political economy clarifies the stakes of Amazon's increasing power over commerce. We are not simply addressing dyadic transactions of individual consumers and merchants. Data access asymmetries will disadvantage each of them (and advantage Amazon as the middleman) for years to come. Nor can we consider that power imbalance in isolation from the way Amazon pits cities against one another. Mastery of political dynamics is just as important to the firm's success as any technical or business*

acumen. And only political organization can stop its functional sovereignties from further undermining the territorial governance at the heart of democracy.[16]

Is Amazon a potential threat to national security? Probably not. Could it become one in the future? Yes, it could, especially if governments continue to give away their power and allow external entities to decide legal and governance procedures based on company policy. These kinds of revolutionary changes will require entirely new ways of thinking, new laws, and policy to deal with transnational, borderless sovereigns who may also seek to engage in novel forms of warfare to further erode traditional nation-state systems to their advantage.[17] One of the ways such entities may attempt to do this could be through the control and employment of emerging disruptive technologies.[18]

Leveraging Technology-Influenced Environments for Competitive Advantage

"After weeks of speculation, megacorporation Google is claiming to have achieved 'Quantum Supremacy' in a paper published in the prestigious journal Nature*."*

—Victor Tangermann[19]

"The possession of great power necessarily implies great responsibility."

—William Lamb,
2nd Viscount Melbourne, prime minister under Queen Victoria, 1817[20]

Whoever controls the technology, information, and access will control economies, governments, industry, and warfare. As more and more powerful technologies come online, those who find themselves as creators or owners of such capabilities will be confronted with the age-old question of how to employ them ethically, for society and to improve the human condition, or for self-gain, power, and control and subjugation of others. These narratives are playing out on the global stage between nations like the United States and China. What most nations have yet to realize is that the stage is about to get more crowded, and not with additional nation-states but with virtual nations.

A recent example of a technological advantage is Google's breakthrough in quantum computing. This solution will enable users to solve extremely complex problems that mathematically would have taken thousands of years but now can be done in minutes to seconds.[21] A second example, also from Google, is the employment of the DeepMind AI to successfully beat 98.8 percent of all human players in a complex video game called Starcraft II.[22] Such technologies pose an overmatch advantage that, when combined, could easily outcompete existing nations in a variety of strategies and consistently lengthen the gap between technology

owner and potential rivals. Imagine the advantage DeepMind would have if combined with quantum computing and then applied to international financial markets or multidomain operations on the battlefield. The owner of this capability would have an unbeatable solution, because it would constantly feed new data about competitors into the system, learn and adapt faster than competitors, and essentially anticipate and defeat moves *before they are even tried*. If that owner is a corporation, a high-dollar individual, or a nonstate group, the Westphalian rules that have governed the nation-state system since 1648[23] do not apply. A revolution in capability that impacts multiple sectors, rapidly dethrones current incumbents, and leads to a consolidation of power in the hands of a few regional or global leaders could dramatically alter the diplomatic, information, military, economic, and political landscape.

Using the quantum-computing example, it is expected that entities will race to be the first to employ these new technologies to gain and keep an advantage. Those that succeed will not be burdened with extensive rules and regulations and may not be concerned with morals or ethics, either. Bureaucratic, slow-moving, and highly regulated entities will fall by the wayside to be subsumed by the winners. Quantum computing owners will have the advantage in creating new processes, tactics, materials, and drugs. This advantage will enable them to corner key markets by anticipating trends and individual and group behaviors to out-maneuvering others with ease. The early adopters get the win and are able to maintain their position because the technology keeps them multiple steps ahead of their rivals.

In this scenario, quantum prescience becomes the norm, moving from science fiction into science fact. Early versions of these technologies already exist and are being used successfully by hedge-fund managers and private-sector strategists. Quantum computing will serve to amplify those effects and grant the owners the power to dominate in multiple sectors, especially if their competition is late to the game or lacks similar access and capability. In game theory (even in a sequential game), with an overmatch technology like Quantum that gives a transparent, proactive, predictive view of all other player moves, a first-mover advantage is the only advantage, and everyone else comes in last.[24]

These are just a few examples of how identity and governance are radically changing without government input and in ways that could pose significant risks to international security and special operations. So how did we arrive at this place? And where do we go from here?

Traditional Governance versus Virtual Governance

> *"There is only one global superpower these days: the public opinion of 7 billion people. The question is how to marshal that power."*
>
> ***—Simon Adholt,***
> ***founder of the Good Country Party Virtual Nation***[25]

Simon Adholt is another marketing expert who sees the potential of new power and believes it can be harnessed in ways that can drive both positive and negative changes globally. In a 2014 interview, Adholt argued public opinion has become a force for driving change in and external to existing systems.[26] When large groups of people come together as they did in Arab Spring, there is not much that can stop them. Science-fiction novels initially postulated the existence of a *global citizen*, but until recently, the technology did not exist to make this a reality. Today, virtual nations and digital identity are becoming fact and moving from thought experiment into viable foundations for future forms of governance that are not dependent on a nation-state system. More than ever, the internet is bringing us closer together, uniting millions in cyberspace. Social media platforms host billions of users who can connect with each other on shared interests across the world. Over four billion people were using the internet as of 2018; 67 percent of the world has access to a mobile phone, and over half of those are smartphone devices; and over three billion people are using social media on their mobile devices every month.[27]

Public space is no longer just a physical place, it is digital as well. This means enhanced interconnectivity is making physical boundaries less relevant. Emergent technologies necessary to establish digital identities are creating the basis for the adoption of a legally recognized international identification. For the first time, individuals could be connected to each other voluntarily, choosing their form of governance and freeing themselves from traditional governance structures. Previously, nations were the basis for this shared sense of community, but today people are more likely to see themselves as *global citizens* than *national citizens*, joining together on complex issues involving the environment or human rights.[28] Following recent economic and political challenges, there is a growing belief that online transnational communities present viable options to replace what many perceive to be outdated, failing, and corrupt national governance and identity models.[29] As Liav Orgad noted in his work, "By showing global responsibility, even if limited and with a weak sense of agency, individuals are participating in activities whose scope and target audience go beyond national boundaries. The changing public opinion thus goes hand in hand with changes in individual actions motivated by a sense of global political responsibilities."[30]

Citizens have traditionally derived their identity and their legal status from where they are born. Their state provided them with certain guarantees, benefits, and legal protections. In exchange, each citizen may be required to provide a service or pay

taxes to support the state. With citizenship also comes a certain amount of power. A US citizenship will convey more rights, freedoms, and soft power than some other citizenships might. This is because countries like the United States or the United Kingdom also have diplomatic and military tools to protect their sovereignty and their citizens. The powers granted to citizens also extend to their ability to travel freely around the world. But what if power was no longer tied to traditional forms? Jeremy Heimans and Henry Timms explore this topic in their book, *New Power: How Power Works in Our Hyperconnected World and How to Make it Work for You* (2018). While traditional forms of power are held by state actors, new power is available to everyone; it is distributed and decentralized. Most important, it can be massed rapidly in the digital realm by nonstate actors and used to achieve physical effects at the state, national, and regional levels. The Ice Bucket Challenge, #MeToo, Black Lives Matter, Facebook, AirBnB, Cambridge Analytica, Occupy Movement,and the Parkland Students for Gun Control initiative are all recent example of new power in action.[31] As Decca Aitkenhead notes in an interview with Heimans:

> *"The future . . . will be won by those who can spread their ideas better, faster, and more durably. . . . It's really hard not to make the argument that the forces of misinformation and extremism and nativism are in the lead."*
>
> *He invites us to contrast the success of the new power recruitment strategy of ISIS with the failure of the US State Department's old power effort to thwart it; ISIS recruits through a peer-to-peer network of youngsters sharing seductive intimacies on social media, which the State Department sought to defeat with a calamitously ill-judged Twitter account bearing an image of its official seal and the instruction: 'Think Again, Turn Away!"*[32]

The key is to navigate when it is appropriate to stay with traditional power structures and when new power tools should be employed. Governments tend to be inexperienced at this, while the private sector and virtual nations excel. Those entities that understand new power will have a vast advantage when working to spread their message, building loyalty across communities and turning these groups into a movement to force change. And that includes establishing borderless nations and a global citizenry. Understanding these new entities and how they will play into military operations is also crucial, especially for special operations.[33]

Virtual Nations, Digital Identity, and the Implications for Special Operations Forces

As these new actors begin to play larger roles on the world stage, it will be important to understand their impact on military strategy and plans. Special operations teams will be the first forces likely to encounter and be forced to deal with the effects of virtual nations and digital identity. New technology,training, and access to the right experts and information are crucial to the future success of SOF. Some of the expected features of this new landscape include the following challenges:

- Impaired ability to conduct covert operations because of restricted freedom of movement as digital identity and biometrics facilitate tracking through social media, adware, digital fingerprinting, cell-phone and computer usage, global transportation trackers, and open-source space and intelligence resources.
- Compromised ability to surprise a near peer or peer competitor or to mass forces rapidly for an operation without being detected.
- Increased risk of warfare on the home front with individual leaders or teams and their families targeted through cyber or other means.
- Non-nation-state actors that emerge from corporations or individuals and small groups entering conflict zones, as ease of access to new technologies and new power grant capability to successfully compete with nation-state modern militaries.
- Increased military use of cyber tactics, partisan forces, proxy wars, and "new frontier" wars (i.e., conflicts in the polar regions, conflict through misinformation, conflict in emerging zones such as space, and satellite-based warfare and subterranean warfare).
- Increased use of nonkinetic combat (economic, legal, and social methods) to cripple enemies from within.[34]

The way of warfare as we know it is changing permanently. But there are measures that can be taken to remain competitive and transition to a more agile force for the future. Tactics and methods to consider include:

- Incorporate nontraditional experts into strategy, planning, and futures discussions to understand state of art and what is to come.
- Ramp up cyber foreign internal defense and build global partisan networks with friendly hackers and makers to maintain forward posts for intelligence and information purposes.
- Build innovation and forecasting into special operations at the team level up through headquarters staff.

- Consider the implementation of *special teams* operating under Title 60 (Title 10 and 50) authorities for extreme crises events.
- Prioritize the biggest threat areas for SOF today, and implement targeted efforts to create teams that are empowered to move forward on radical solutions that will reclaim the lead, and if possible gain and maintain overmatch; this includes cyber, misinformation and psyops, targeted countering-weapons-of-mass-destruction efforts, artificial intelligence and autonomous systems, novel covert operations, interoperability, advanced communications, and avatar driven operations.[35]

Conclusion

While virtual nations and digital identity may become a positive for hybrid national governance structures in the future, ignorance of the dual nature of these developments is no excuse for dismissing them and ignoring their potential. Virtual nations could be tremendously beneficial in reducing global conflict and granting *stateless* populations the rights and benefits all humans deserve, saving lives, cutting costs, and streamlining government administration for the better. Or they could pose the next major threat to democracy, polarize populations, and lead to advanced forms of conflict that will scale similar to the digital spaces they derive from and cause massive disruption in ways previously not seen.

The digital space has quietly turned into a powerhouse, and it is hard for global leaders to realize the threat because the powers aligning against them don't wave a flag, wear a uniform, or even operate according to national and international law. And yet they exist, and they are growing stronger daily. Special operations forces will be the first to confront these challenges because of where they sit and the operations they execute. Policy, regulation, acquisitions, and authorities must catch up quickly, and only by radically changing the mindset of how we view the current and future battlespace will SOF continue to command the advantages they hold today and the ability to operate successfully.[36]

Bibliography

Adams, T. (2014, November 30). "Simon Anholt Interview: 'There Is Only One Global Superpower—Public Opinion.'" Retrieved from https://www.theguardian.com/politics/2014/nov/30/simon-anholt-good-country-party-global-superpower-public-opinion.

Allen, C. (2016, April 25). "The Path to Self-Sovereign Identity." Retrieved from http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

"**AlphaStar: Mastering the Real-Time Strategy Game StarCraft II.**" Deep Mind Blog. (2019, January 24). Retrieved from https://deepmind.com/blog/article/alphastar-mastering-real-time-strategy-game-starcraft-ii.

Berdah, B. (2019, June 14). "The Demise of Nation States: Introducing the Nation as a Service (NaaS)." Retrieved from https://medium.com/@BBerdah/the-demise-of-the-nation-states-introducing-the-nation-as-a-service-naas-ef3bf9f494e3.

Bhakuni, M. (2018, July 25). "Following Digital Breadcrumbs: Delivering Actionable Insights from Market Intelligence. Retrieved from https:yourstory.com/2018/07/market-intelligence-digital-breadcrumbs.

Bridle, J. (2018, February 22). "The Rise of Virtual Citizenship." Retrieved from https://www.theatlantic.com/technology/archive/2018/02/virtual-citizenship-for-sale/553733/.

Coats, Daniel R. (2019, January 29). "Statement for the Record: World Wide Threat Assessment of the US Intelligence Community." Retrieved from https://www.odni.gov/files/ODNI/documents/2019-ATA-SFR—SSCI.pdf.

Davis, Z., and Nacht M. (2018) *Strategic Latency Red White and Blue: Managing the National and International Security Consequences of Disruptive Technologies*. Lawrence Livermore Press. Retrieved from https://cgsr.llnl.gov/content/assets/docs/STATEGIC_LATENCY_Book-WEB.pdf.
"**Digital Breadcrumbs: The Data Trail We Leave Behind Us.**" (2016, May 3). Pod Academy. Retrieved from https://podacademy.org/podcasts/digital-breadcrumbs-our-data-trail/.

Ehrsam, F. (2017, November 29). "Blockchain Governance: Programming Our Future." Retrieved from https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74.

Felsenthal, Mark. (2019, April 19). "Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows." World Bank. Retrieved from https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows.

Ferrara, C. (2018, April 21). "Disrupting Governments: #Blockchain Is Changing the Meaning of #Citizenship." Retrieved from https://medium.com/@caterinaferrara/disrupting-governments-blockchain-is-changing-the-meaning-of-citizenship-a7a96a72d1d1.

Fowler, Geoffrey A. (2019, October 31). "Think You're Anonymous Online? A Third of Popular Websites Are 'Fingerprinting' You." Retrieved from https://www.washingtonpost.com/technology/2019/10/31/think-youre-anonymous-online-third-popular-websites-are-fingerprinting-you/.

Foxley, William. (2019, October 16). "Bermuda Starts Development of a Blockchain-Based National ID System." Coindesk. Retrieved from https://www.coindesk.com/bermuda-starts-development-of-a-blockchain-based-national-identity-system.

Gallego, J. (2016, March 11). "Bitnation Launches the First Virtual Constitution." Retrieved from https://futurism.com/bitnation-launches-worlds-first-virtual-constitution-virtual-nation.

Giordano, J., Bremseth, R. (2019, March 4). "The Importance of Integrative Science/Technology Intelligence (InS/TINT) to the Prediction of Future Vistas of Emerging Threats." TRADOC Mad Scientist Blog. Retrieved from https://madsciblog.tradoc.army.mil/125-the-importance-of-integrative-science-technology-intelligence-ins-tint-to-the-prediction-of-future-vistas-of-emerging-threats/.

Giordano, J., Bremseth, R. (2018, December 13). "Emerging Technologies as Threats in Non-Kinetic Engagements." TRADOC Mad Scientist Blog. Retrieved from https://madsciblog.tradoc.army.mil/105-emerging-technologies-as-threats-in-non-kinetic-engagements.

"The Good Country Is an Entirely New Global/Virtual Nation, Aiming 'to Make the World Work Better.'" (2018, September 21). Retrieved from https://www.thealternative.org.uk/dailyalternative/2018/9/22/thegoodcountry-launches-virtually.

Griffin, M. (2019, June 27). Estonia Becomes the World's First Virtual Nation Capable of Rebooting Itself," Retrieved from https://www.311institute.com/estonia-virtual-nation-capable-of-rebooting-itself-in-war/.

Griffin, M. (2019, April 24). "US military Identifies Virtual Nations as a Potential Security Threat to US Sovereignty." Retrieved from https://www.fanaticalfuturist.com/2018/12/us-military-identifies-virtual-nations-as-a-potential-security-threat-to-us-sovereignty/.

Heller, N. (2017, December 11). "Estonia, the Digital Republic," *New Yorker*. Retrieved from https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.

Heimans, Jeremy. (2018, April 20). "Like It or Not, the Old World Isn't Coming Back." The Guardian. Retrieved from https://www.theguardian.com/politics/2018/apr/20/new-power-jeremy-heimans-social-media.

Heimans, J., Timms, H. (2014, December 1). "Understanding 'New Power." Harvard Business Review. Retrieved from https://hbr.org/2014/12/understanding-new-power.
Humenansky, J. (2019, August 16). "The Impact of Digital Identity." Retrieved from https://medium.com/blockchain-at-berkeley/the-impact-of-digital-identity-9eed5b0c3016.

Kania, E. (2018, September 20). "Quantum Surprise on the Battlefield." TRADOC Mad Scientist Blog. Retrieved from https://madsciblog.tradoc.army.mil/84-quantum-surprise-on-the-battlefield.

Kemp, Simon. (2019, January 30). "Digital 2019: Global Internet Use Accelerates." We Are Social Global Digital Reports 2019. Retrieved from https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates.

Keys, A. (2019, August 12). "Welcome to the Fourth Industrial Revolution—19 Blockchain Predictions for 2019." Retrieved from https://media.consensys.net/welcome-to-the-fourth-industrial-revolution-19-blockchain-predictions-for-2019-8b2e542bf86a.

Koens, T., & Meijer, S. (2018, May 1). "Matching Identity Management Solutions to Self-Sovereign Identity Principles." Retrieved from https://www.linkedin.com/pulse/matching-identity-management-solutions-self-sovereign-tommy-koens.

Loo, Rory Van. (2016) "The Corporation as Courthouse." Yale Journal, 33 (2), 547-601. Retrieved from http://digitalcommons.law.yale.edu/yjreg/vol33/iss2/5.

Maack, M. M. (2019, May 10). "Nation as a Service Is the Ultimate Goal for Digitized Governments." Retrieved from https://thenextweb.com/tnw2019/2019/05/09/nation-as-a-service-is-the-ultimate-goal-of-for-digitized-governments/.

Marr, Bernard. (2019, October 7). "Facebook's Blockchain-Based Cryptocurrency Libra: Everything You Need to Know." Retrieved from https://www.forbes.com/sites/bernardmarr/2019/10/07/facebooks-blockchain-based-cryptocurrency-libra-everything-you-need-to-know/#3bdb00d24d7a.

McKinney, Phil. (2019, November 18). "James 'Hondo' Geurts on Taking the Navy into the Next Wave of Innovation. Killer Innovations." Retrieved from https://killerinnovations.com/james-hondo-geurts-on-taking-the-navy-into-the-next-wave-of-innovation.

McQuinn, A., and Castro, D. (2019, April 30). "A Policymaker's Guide to Blockchain." Retrieved from https://itif.org/publications/2019/04/30/policymakers-guide-blockchain.

Miller, S. (2018, February 16). "Global Citizenship in a Post-Nation State World." Retrieved from https://words.democracy.earth/global-citizenship-in-a-post-nation-state-world-d5bf21ac9bb1.

Murphy, M. (2018, July 3). "66. Virtual Nations: An Emerging Supranational Cyber Trend." Retrieved from https://madsciblog.tradoc.army.mil/66-virtual-nations-an-emerging-supranational-cyber-trend/.

Noguchi, Yuki. (2011, November 29). "Following Digital Breadcrumbs to 'Big Data' Gold." National Public Radio Morning Edition. Retrieved from https://www.npr.org/2011/11/29/142521910/the-digital-breadcrumbs-that-lead-to-big-data.

Orgad, L., & Baubock, R. (Eds.). (2018). "Cloud Communities: The Dawn of Global Citizenship." European University Institute. Retrieved from http://globalcit.eu/cloud-communities-the-dawn-of-global-citizenship/.

Palmer, Daniel. (2019, September 9). "Catalonia to Build DLT-Based Identity Platform for Citizens." Coindesk. Retrieved from https://www.coindesk.com/catalonia-government-to-build-dlt-based-identity-platform-for-citizens.

Pasquale, Frank. (2017, December 6). "From Territorial to Functional Sovereignty: The Case of Amazon." Law and Political Economy Blog. Retrieved from https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon.
Pasquale, Frank. (2017, July 20). "Will Amazon Take Over the World?" Boston Review. Retrieved from http://bostonreview.net/class-inequality/frank-pasquale-will-amazon-take-over-world.

Peck, Morgan. (2015, December 9). "The Radical Politics of the Blockchain." Wired Magazine. Retrieved from https://www.wired.com/2015/12/the-radical-politics-of-the-blockchain/.

Prisco, G. (2014, December 8). "Governance 2.0—Evolution of the System or Revolution Against the System?" Retrieved from http://www.ccn.com/governance-2-0-evolution-system-revolution-system.

Rothman, P. (2015, February 18). "Interview: Bitcoin Pioneer Susanne Tarkowski Tempelhof on Bitnation and M+." H Plus Magazine. Retrieved from https://hplusmagazine.com/2015/02/18/interview-bitcoin-pioneer-susanne-tarkowski-tempelhof-on-bitnation-and-m/.

Sclavounis, O. (2017, November 17). "Understanding Public Blockchain Governance." Retrieved from https://www.oii.ox.ac.uk/blog/understanding-public-blockchain-governance/.

Shen, C., & Pena-Mora, F. (2018). "Blockchain for Cities—A Systematic Literature Review." IEEE Access, 6, 76787–76819. doi: 10.1109/access.2018.2880744.

Shier, C., Mehar, et al. (2017). "Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack." SSRN Electronic Journal. doi: 10.2139/ssrn.3014782.

Stalnaker, S. (2019, February 18). "Crafting Virtual Nations." Retrieved from https://www.maize.io/en/content/crafting-virtual-nations.

Statt, N. (2019, October 30). "DeepMind's StarCraft 2 AI is now better than 99.8 percent of all human players." The Verge. Retrieved from https://www.theverge.com/2019/10/30/20939147/deepmind-google-alphastar-starcraft-2-research-grandmaster-level.

Symons, T. (2018, February 1). "The Nation State Goes Virtual: Why Citizenship Need No Longer Be Determined by Geography." Retrieved from https://tech.newstatesman.com/guest-opinion/virtual-nation-states.

Tangermann, V. (2019, October 24) "Here's Why Quantum Supremacy Matters: Google's Watershed Quantum Computing Achievement Explained." Futurism. Retrieved from https://futurism.com/why-quantum-supremacy-mattsers.

Tobin, A., Reed, D., & Windley, P. (2017). "The Inevitable Rise of Self-Sovereign Identity." Sovrin Foundation. Retrieved from https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

Toth, K. C., & Anderson-Priddy, A. (2019). "Self-Sovereign Digital Identity: A Paradigm Shift for Identity." IEEE Security & Privacy, 17(3), 17–27. doi: 10.1109/msec.2018.2888782.
US Army. "TRADOC Pamphlet 525-3-1: The US Army in Multi-Domain Operations 2028." (2018, December 6). Retrieved from https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

Vines, P., Roesner, F., Kohno, T. (2017, October 30) "Exploring ADINT: Using Ad Targeting for Surveillance on a Budget—or—How Alice Can Buy Ads to Track Bob. Retrieved from https://adint.cs.washington.edu/.

"World's Stateless." (2014, December). Institute for Statelessness and Inclusion. Retrieved from https://files.institutesi.org/worldsstateless.pdf.

Endnotes

1 Institute for Ethics and Emerging Technologies. 2016. "Susanne Tarkowski Tempelhof: The Diamond Lady of DIY Goverance 2.0." March, 2016. https://ieet.org/index.php/IEET2/more/prisco20160302.

2 "World's Stateless," 2014.

3 Rothman, "Interview: Bitcoin Pioneer Susanne Tarkowski Tempelhof on Bitnation and M+," 2015.

4 Rothman, "Interview: Bitcoin Pioneer Susanne Tarkowski Tempelhof on Bitnation and M+," 2015; Peck, "The Radical Politics of the Blockchain," 2015.

5 Rothman, "Interview: Bitcoin Pioneer Susanne Tarkowski Tempelhof on Bitnation and M+,"2015; Peck, "The Radical Politics of the Blockchain." 2015.

6 Barclay, Eliza and Brian Resnick; "How Big was the Global Climate Strike? Four Million People, Activists Estimate." *Vox*, September 22, 2019 Accessed 1 May 2020. online at https://www.vox.com/energy-and-environment/2019/9/20/20876143/climate-strike-2019-september-20-crowd-estimate.

7 Aitkenhead, Decca. 2018. "New Power Author Jeremy Heimans: 'Like It or Not, the Old World Isn't Coming Back,'" 2018; Heimans and Timms. "Understanding 'New Power,'" 2014.

8 Marr, "Facebook's Blockchain-Based Cryptocurrency Libra," 2019.

9 Felsenthal, "Financial Inclusion on the Rise," 2019.

10 Aitkenhead, Decca. 2018. "New Power Author Jeremy Heimans: 'Like It or Not, the Old World Isn't Coming Back,'" 2018; Heimans and Timms, "Understanding 'New Power,'" 2014.

11 Maack, "Nation as a Service Is the Ultimate Goal for Digitized Governments," 2019; Miller, "Global Citizenship in a Post-Nation State World," 2017; "66. Virtual Nations: An Emerging Supranational Cyber Trend." *Mad Scientist Laboratory*. July 3, 2018. https://madsciblog.tradoc.army.mil/66-virtual-nations-an-emerging-supranational-cyber-trend; Stainaker, S. 2019. "Crafting Virtual Nations." Maize. February 18, 2019. https://www.maize.io/en/content/crafting-virtual-nations.

12 Berdah, "The Demise of Nation States," 2018; Foxley, W. "Bermuda Starts Development of a Blockchain-Based National ID System," 2019; "Estonia Becomes the World's First Virtual Nation Capable Of Rebooting Itself." 311 Institute. September 20, 2018. https://www.311institute.com/estonia-virtual-nation-capable-of-rebooting-itself-in-war; Heller, "Estonia, the Digital Republic," 2017; Maack, "'Nation as a Service' Is the Ultimate Goal for Digitized Governments," 2019; Miller, "Global Citizenship in a Post-Nation State World," 2017; "66. Virtual Nations: An Emerging Supranational Cyber Trend." Mad Scientist Laboratory. July 3, 2018. https://madsciblog.tradoc.army.mil/66-virtual-nations-an-emerging-supranational-cyber-trend; Palmer, "Catalonia to Build DLT-Based Identity Platform for Citizens," 2019; Stainaker, S. 2019. "Crafting Virtual Nations." Maize. February 18, 2019. https://www.maize.io/en/content/crafting-virtual-nations.

13 Bridle, "The Rise of Virtual Citizenship," 2018; Miller, "Global Citizenship in a Post-Nation State World," 2017; Murphy, "66. Virtual Nations: An Emerging Supranational Cyber Trend." 2018; Stainaker, S. 2019. "Crafting Virtual Nations." *Maize*. February 18, 2019. https://www.maize.io/en/content/crafting-virtual-nations.

14 Pasquale, "From Territorial to Functional Sovereignty: The Case of Amazon," 2017; Pasquale, "Will Amazon Take Over the World?" 2017.

15 Pasquale, "From Territorial to Functional Sovereignty: The Case of Amazon," 2017; Pasquale, "Will Amazon Take Over the World?" 2017; Loo, "The Corporation as Courthouse," 2016.

16 Pasquale, "From Territorial to Functional Sovereignty: The Case of Amazon*,"* 2017.

17 Coats, "Statement for the Record," 2019; Griffin, M. 2018. "US Military Identifies Virtual Nations as a Potential Security Threat to US Sovereignty." *Fanatical Futurist*. December 14, 2018. https://www.fanaticalfuturist.com/2018/12/us-military-identifies-virtual-nations-as-a-potential-security-threat-to-us-sovereignty.

18 Coats, "Statement for the Record," 2019; Giordano and Bremseth, "Emerging Technologies as Threats in Non-Kinetic Engagements," 2018; Giordano and Bremseth, "The Importance of Integrative Science/Technology Intelligence (InS/TINT) to the Prediction of Future Vistas of Emerging Threats," 2019.

19 Tangermann, Victor, "Here's Why Quantum Supremacy Matters," *Futurism*, 2019, https://futurism.com/why-quantum-supremacy-matters.

20 Commons Sitting. 1817. "Habeas Corpus Suspension Bill." *Hansard*. June 27, 1817. https://api.parliament.uk/historic-hansard/commons/1817/jun/27/habeas-corpus-suspension-bill.

21 Tangermann, "Here's Why Quantum Supremacy Matters," 2019.

22 Statt, "DeepMind's StarCraft 2 AI is Now Better than 99.8 Percent of All Human Players," 2019; "AlphaStar," 2019.

23 Oxford Reference. "Westphalian State System." Oxford University Press. Accessed April 10, 2020. https://www.oxfordreference.com/view/10.1093/oi/authority.20110803121924198.

24 Kania, "Quantum Surprise on the Battlefield?" 2018; Tangermann, V. 2019. "Here's Why Quantum Supremacy Matters: Google's Watershed Quantum Computing Achievement Explained." *Futurism*. October 24, 2019. https://futurism.com/why-quantum-supremacy-matters.

25 Adams, T. "Simon Anholt Interview," 2014.

26 Adams, T. "Simon Anholt Interview," 2014.

27 Kemp, "Digital 2019: Global Internet Use Accelerates," 2019.

28 Adams, T. "Simon Anholt Interview," 2014.

29 Orgad, "Cloud Communities," 2018; Stainaker, S. 2019. "Crafting Virtual Nations." *Maize*. February 18, 2019. https://www.maize.io/en/content/crafting-virtual-nations; Symons, "The Nation State Goes Virtual," 2018.

30 Orgad, "Cloud Communities," 2018.

31 Aitkenhead, Decca. 2018. "New Power Author Jeremy Heimans: 'Like It or Not, the Old World Isn't Coming Back,'" 2018.

32 Heimans and Timms, "Understanding 'New Power,'" 2014.

33 Aitkenhead, Decca. 2018. "New Power Author Jeremy Heimans: 'Like It or Not, the Old World Isn't Coming Back,'" 2018; Heimans and Timms, "Understanding 'New Power,'" 2014.

34 Bhakuni, "Following Digital Breadcrumbs," 2018; Coats, "Statement for the Record World Wide Threat Assessment of the US Intelligence Community," 2019; Fowler, "Think You're Anonymous Online?" 2019; Giordano and Bremseth, "Emerging Technologies as Threats in Non-Kinetic Engagements," 2018; Giordano and Bremseth, "The Importance of Integrative Science/Technology Intelligence (InS/TINT) to the Prediction of Future Vistas of Emerging Threats," 2019; Noguchi, "Following Digital Breadcrumbs to 'Big Data' Gold," 2011; Vines, "Exploring ADINT," 2017.

35 US Army, "TRADOC Pamphlet 525-3-1," 2018; Davis and Nacht, *Strategic Latency Red White and Blue*, 2018; McKinney, " James 'Hondo' Geurts on Taking the Navy into the Next Wave of Innovation," 2019.

36 Coats, "Statement for the Record World Wide Threat Assessment of the US Intelligence Community," 2019; Davis and Nacht, *Strategic Latency Red White and Blue*, 2018; McKinney, "James 'Hondo' Geurts on Taking the Navy into the Next Wave of Innovation," 2019.

CHAPTER 4

Special Forces and Strategic Deterrence

Brad Roberts

What role, if any, do special forces play in underwriting strategic deterrence as practiced by the United States? What role should they play? In recent decades, most experts in the defense community would probably have answered both of these questions with "little, if any, role," given the close association of strategic deterrence with nuclear weapons and of special operations forces (SOF) with the war on terrorism. The Department of Defense's joint operating concept for deterrence, for example, makes no mention of a role for SOF.[1] Similarly, the joint publication setting out the roles of SOF makes just a single reference to the role of SOF in helping to "prevent and deter conflict or prevail in war" and no mention of strategic deterrence.[2] Analyses of the potential contributions of SOF to strategic deterrence are few and far between.[3] The major shift in national defense strategy from the war on terror to major-power rivalry has only reinforced a widespread perception that SOF's role is in decline.

But this answer is wrong. Special forces can, and should, play a significant role in meeting the strategic deterrence requirements of the United States in the emerging security environment. However, their precise role has not yet been defined, partly because the new challenges of strategic deterrence have not yet been defined with sufficient specificity to characterize the particular contributions of SOF. This lack of definition exists partly because US strategy toward conflict in the gray zone—that is, in conflict short of armed hostilities—remains underdeveloped. But a simple mental picture of the main challenges in the emerging security environment can help add some fidelity to the consideration of SOF roles.

This chapter begins with a review of developments in US defense strategy bearing on the question of SOF roles and provides a short list of the key roles for SOF in the new security environment. The chapter then turns to the problem of strategic deterrence in this new environment. This is a problem different from the Cold War problem. In the Cold War, strategic deterrence addressed the problem of preventing Armageddon-like massive nuclear exchanges. In the new security environment, strategic deterrence must address the problem of securing the interests of the United States and its allies in conventional regional conflicts against nuclear-armed adversaries. Next, the chapter turns to an exploration of the particular deterrence challenges of such conflicts. It then explores the potential contributions of SOF to the achievement of US objectives.

The Changing Place of SOF in US Defense Strategy

A casual reading of the Donald Trump administration's strategic documents leaves the impression that SOF will be of declining relevance in the years ahead. The 2018 National Defense Strategy (NDS) reflected the administration's assessment

that "inter-state strategic competition, not terrorism, is now the primary concern in US national security."[4] The reduced concern about the threat from radical violent extremists implies a reduced role for the forces at the center of the fight against them. The increased emphasis on interstate rivalry implies a resurgence of general purpose and strategic forces. Thus, the 2017 National Security Strategy (NSS) emphasizes "the growing political, economic, and military competitions we face around the world" and a "peace through strength" strategy aimed at military preeminence.[5]

A closer reading of these documents tells a different story, however. The NSS commits the United States to retain a full-spectrum force:

> *The Joint Force must remain capable of deterring and defeating the full range of threats to the United States. The Department of Defense must develop new operational concepts and capabilities to win without assured dominance in air, maritime, land, space, and cyberspace domains, including against those operating below the level of conventional military conflict. We must sustain our competence in irregular warfare, which requires planning for a long term, rather than an ad hoc, fight against terrorist networks and other irregular threats.*[6]

Similarly, the NDS argues, "the reemergence of long-term strategic competition, rapid dispersion of technologies, and new concepts of warfare and competition that span the entire spectrum of conflict require a Joint Force structured to match this reality."[7] This leaves open a basic question: What is the necessary and appropriate place of SOF in that structure?

Most obviously, SOF still has a central place in the fight against terrorist networks and other irregular threats. The precise level of effort cannot be anticipated, but excellence at this mission for the long term remains a key national priority. Less obviously, SOF has a place in the fight against rogue states—that is, regional powers controlled by regimes hostile to US interests, US allies, and US-backed regional orders. Currently, North Korea and Iran are two primary examples of rogue states. SOF has a central place in the effort to combat rogue-state ambitions for weapons of mass destruction (WMD) through an aggressive counterproliferation effort aimed at suppressing trade in sensitive materials, technologies, and expertise and collapsing existing WMD and missile-development programs.

Even less obviously, SOF has a place in meeting the challenges posed by rivalry and long-term strategic competition with Russia and China. To understand that place, we must understand the ways in which Russia and China have prepared for regional wars against the United States and its allies. They have prepared for conventional wars under the shadow of risk cast by their nuclear and other strategic capabilities. Rogue states have made similar preparations. This is the hardest new problem

brought to us by a changing security environment and the evolution of US defense strategy. What can SOF contribute to meeting this set of challenges?

Defining the New Challenge of Strategic Deterrence

Russia, China, and North Korea have strong motivation for a credible deterrence posture vis-à-vis the United States. In their common assessments, the end of the Cold War ended the counterbalancing of American power, and, since then, the United States has been on an ideologically driven campaign to remake the world in its image and to encircle and contain them as a prelude to attempts at regime change. Thus, for three decades these states have been seized with the question of how "to deter and defeat a conventionally superior nuclear-armed major power and its allies."[8]

Having started on this project in the 1990s, at a time when these three countries had little money or technology to throw at this problem, they focused first on putting their intellectual houses in order. The result is a set of concepts, hypotheses, and some wishful thinking about how to succeed in that effort. Think of these collections of theories of victory in the spirits of Carl von Clausewitz and Sun Tzu. Clausewitz defined victory as the "culminating" political point in a conflict when one state chooses to no longer run the costs and risks of continued war. Sun Tzu defined victory as subduing an enemy without fighting. A theory of victory in the spirit of Clausewitz is a set of ideas about how to bring the United States and its allies to a culminating point to accept war termination terms offered by its adversary. A theory of victory in the spirit of Sun Tzu is a set of ideas about how to remake regional and global orders without engaging in overt armed conflict.

Russia, China, North Korea, and Iran all have such theories to deter and defeat the United States and its allies. Despite important differences among them in orientation, interest, and capability, these states face a common problem and, therefore, have come to similar strategies. Boiled down to their essence, these strategies reflect the following core hypotheses.

- First, if war with the United States and its allies appears inevitable, or if some local prize can be won opportunistically, an adversary can accomplish a fait accompli at a reasonable cost and can prevent a decisive response by the United States and its allies by presenting them with a credible image of a terrible cost to be paid in the attempt.to reverse the fait accompli.
- Second, if the United States and its allies choose unreasonably to try to reverse the fait accompli, an adversary can break weak links in these alliances, thereby putting the United States in a position of having to decide to fight alone (or nearly so) or not at all.
- Third, if the United States chooses unreasonably to fight on, an adversary can compel it to stop short of doing grievous damage by inflicting high costs on its power-projection forces.

- Fourth, if the United States chooses to put the regime at risk or to significantly punish it for aggression, an adversary can persuade it to back down by illustrating the vulnerability of the American homeland to attack.
- Fifth, this entire pathway can be avoided by success in the gray zone—that is, through the use of a creative mix of hard and soft power tools to remake regional security orders in a manner that breaks encirclement and entanglement without running the costs and risks of war. If the United States and its allies resist militarily, and consider bringing to bear their full military potential, they must contemplate the credible counterescalation capabilities now in place to deter and defeat them.

Underpinning Russian, Chinese, and North Korean confidence in their escalatory threats is an assessment about asymmetries of stake and geography. In their assessment, regional conflicts would involve important interests for the United States, but not vital interests in the way they would be seen in Moscow, Beijing, or Pyongyang. The asymmetry of geography follows from the fact that the United States must attack their homelands to prevail in a regional conflict, which would lend credibility to their threats to respond with attacks on the American homeland. They imagine the use of force as a way to "sober" the United States to these asymmetries.

In short, these three potential US adversaries have developed strategies for nuclear blackmail and brinksmanship and multidomain escalation in time of crisis and war that they apparently believe would deter and, if necessary, defeat the United States. In time of crisis and war, the United States would find itself in a multidomain, multidimensional, and transregional conflict (to cite former chairman of the Joint Chiefs of Staff Joseph Dunford).[9] In the gray zone, Russia, China, and North Korea use the cover provided by these strategies to push up to the brink of war to try to remake political facts on the ground. Given their increased assertiveness regionally and, in the case of Russia and China, globally, the leaders of these three countries apparently have newfound confidence in their ability to accept the risks of confrontation with the United States.

The task for US strategy is to strip away this confidence. The United States and its allies must have the means to:

- Erode the conditions for success in the potential fait accompli, so that it looks like an unattractive quagmire instead;
- Reinforce the expectation of alliance solidarity in time of escalating conflict;
- Ensure the ability of the United States to surge forces into the theater in a timely manner, despite the contested environments and domains;
- Protect the American homeland from limited attack and ensure a credible threat of nuclear retaliation;
- Render unrewarding Red (defined below) efforts to alter regional security orders through gray zone tactics.

Put differently, the United States and its allies must have the means to affect the deterrence calculus of its potential adversaries in conventional regional conflicts under the nuclear shadow. The Deterrence Operations Joint Operating Concept describes this deterrence calculus as containing three primary variables:

- The adversary's perception of the benefits of a course of action.
- The adversary's perception of the costs of a course of action.
- The adversary's perception of the consequences of restraint or inaction (i.e., the benefits and costs of not taking the course of action in question).[10]

In meeting the new strategic deterrence challenge of conventional regional wars against nuclear-armed adversaries, these three factors should be understood as the adversary's *deterrence and escalation calculus.* Adversaries must be denied the confidence that the costs and risks of war against the United States and its allies, of escalating and counterescalating in war, and of pressing demands in the gray zone are acceptable, especially relative to the expected gain.

Defining SOF's Potential Contributions

What can SOF contribute to the achievement of these objectives? Little thinking appears to have been done on this question, not least because little thinking has been done about the character of these new challenges or of the needed response by the United States and its allies. New thinking is needed. For the time being, some old thinking has come into play.

In the period between 9/11 and Russia's annexation of Crimea in 2014, the United States focused its military innovation on the challenges of counterterrorism and counterinsurgency. As military planners have come back to the problem of state-to-state conflict in an era of major-power rivalry, they have fallen back on some thinking that began to take shape in the 1990s when a new problem took shape: rogue-state challengers and the possibility of major theater wars with a WMD dimension.[11]

The 1993 Bottom Up Review of US defense strategy, conducted after the collapse of the Soviet Union, both highlighted the new threat posed by leaders such as Saddam Hussein armed or arming with WMD and launched the Defense Counterproliferation Initiative to adjust deterrence strategies to this new problem. The first Quadrennial Defense Review in 1994 defined a new planning focus: major theater wars. Rogue-state acquisition of long-range missiles added urgency to this problem. As a matter of national policy, the United States rejected mutual vulnerability with rogue states and, in 1998, set out to develop a national missile defense posture sufficient for this purpose, motivated in large part by the assessment that nuclear deterrence might prove unreliable against a leader who fears defeat and ejection (or death) by a US-led coalition enjoying conventional supremacy. For such an adversary, no war with the

United States could be expected to remain limited in a meaningful way because it would automatically involve questions of regime survival.

In the period between 9/11 and 2014, the United States did not neglect this topic completely. The George W. Bush administration continued the focus on rogue states and the rejection of mutual vulnerability but also added the terrorist aspect. It emphasized "the nexus" of rogue states, terrorism, and WMD and embraced preventive and preemptive military action as necessary complements to deterrence and defense. Like its predecessor, it emphasized strategic cooperation with Russia and China, while also hedging against a turn for the worse. In contrast, the Barack Obama administration did not embrace the term "rogue state" or "the nexus." But it set out a comprehensive agenda for adapting and strengthening regional deterrence architectures to deal with the threats posed by regional challengers. It too rejected mutual vulnerability with such states while seeking cooperation with Russia and China to strengthen strategic stability.

After 2014, US defense planners began to return to the problem of major-power rivalry and conflict. In 2015, Secretary of Defense Ash Carter called for "a new playbook" for Russia, while also leading an effort for a "third offset" to restore conventional deterrence of major-power rivals. Since then, the ideas from the 1990s have enjoyed a resurgence in the defense community, including an emphasis on deterrence by denial (with missile defense and resilience in the new domains), with a reluctance to rely heavily on nuclear deterrence, and with the expectation that adversary WMD employment would likely come only in a last-resort effort to prevent regime removal. These ideas fit poorly with the new challenge.

The 2018 NDS proved helpful in shifting military thinking onto the new challenge of strategic deterrence. The congressionally mandated bipartisan National Defense Strategy Commission hailed the NDS as "a constructive first step" that "points the Department of Defense and the country in the right direction."[12] But the commission went on to deliver a sharp critique. The NDS may point us in the right direction, but "it does not adequately explain how we should get there." Its criticism is especially sharp on the absence of concepts for translating deterrence objectives into meaningful outcomes.[13] To cite further:

- The NDS "leaves unanswered critical questions regarding *how* the United States will meet the challenges of a more dangerous world."
- "Although the NDS states that deterring adversaries is a key objective, there was little consensus among DOD leaders with whom we interacted on what deterrence means in practice, how escalation dynamics might play out, and what it will cost to deter effectively."
- "DOD leaders had difficulty articulating how the US military would defeat major-power adversaries should deterrence fail."
- "There are numerous unmet operational challenges such as . . . deterring, and if necessary defeating, the use of nuclear or other strategic weapons in ways

that fall short of justifying a large-scale nuclear response."

- "The United States . . . urgently requires new operational concepts that expand US options and constrain those of China, Russia, and other actors."
- "Put bluntly, the US military could lose" the next state-to-state war.
- "The Department does not appear to have a plan for succeeding in gray zone operations . . . nor does the administration as a whole."
- "The NDS asserts that DOD will 'expand the competitive space' but offers little evidence of how it will do so."[14]

The NDS Commission's assessment has a clear implication for the exploration of SOF's contribution to the new challenge of strategic deterrence. Assuming the NDS Commission is correct, SOF cannot simply fit in to existing concepts, strategies, or approaches. It cannot "plug and play." It must help the Department of Defense, and national leadership more broadly, chart a new SOF course. The central question is, what can special operations core activities contribute to meeting these challenges? For the following analysis, "Red" and "Blue" are used to put in abstract terms the adversarial parties in these conflicts. Red refers to potential US adversaries. Blue refers to the United States and its allies.

SOF and the Fait Accompli

What can SOF contribute to the Blue objective of eroding the conditions for success in the potential fait accompli? Blue's deterrence objective should be to strip away Red's confidence it can achieve a quick and decisive victory and avoid a quagmire that gives Blue time to play to its strengths. To accomplish this objective, Blue must have robust and reliable means to impose early and crippling costs on Red and to rapidly reinforce its own forces.

SOF can contribute to both of these missions. With special reconnaissance, it can help provide timely warning to Blue. With foreign internal defense, it can disrupt and delay Red force flow and logistics support. With security force assistance, it can strengthen the capacity of allies and partners to support these tasks. Additionally, we should note the prominent role that Red (especially Russia and North Korea) attach to the role of their SOF in accomplishing the fait accompli; this suggests an additional preventative role for SOF direct action.

SOF and Alliance Solidarity

What can SOF contribute to the Blue objective of reinforcing Red's expectation of Blue solidarity in time of escalating conflict? Blue's deterrence objective should be to strip away Red's confidence that its efforts to impose costs and risks on US allies and alliances will not generate an unwelcome reply from Blue. In part, this requires steps to address the misperceptions that those alliances are weakly linked, that allies are weakly led, and that allied publics can be counted on to pressure governments not to

respond forcefully to Red actions (the most important tasks necessary to accomplish this objective are outside the military domain). This partly requires military means, first, to reduce Red's expected benefits from attacking US allies and alliances and, second, to increase Red's expected costs.

SOF can contribute to both of these tasks. To meet the fait accompli challenge, special reconnaissance, foreign internal defense, and security-force assistance can play significant roles.

SOF and "Surge"

What can SOF contribute to ensuring Blue's ability to "surge" its forces in a timely manner and despite contested environments and domains? Blue's deterrence objective should be to prevent attacks on US power-projection forces—as well as other forces (allied, coalition, or United Nations) that may be brought into play—that would compromise the military campaign they are executing. To accomplish this objective, Blue must be able to strip away Red confidence such attacks would cripple Blue capability to provide timely defense to US allies and result in costs Red considers bearable. This implies the ability to defend critical infrastructure in CONUS, supporting power projection, especially from cyberattack, to defend ports of debarkation and embarkation and to strike critical Red nodes and other assets across the theater and in a manner that keeps them out of operation.

SOF can contribute both defense and offense to these tasks. It can also help to counter Red SOF operating in support of this mission.

SOF and Homeland Defense

What can SOF contribute to the protection of the US homeland from limited attack and to ensuring a credible threat of nuclear retaliation? Blue's deterrence objective should be to prevent both limited strikes intended for coercive purposes through deterrence by denial and large-scale strikes intended for decisive military and political effect through deterrence by threat of retaliation, including nuclear. To accomplish this objective, Blue needs effective limited homeland missile defense as well as a nuclear deterrent that can retaliate at the major thresholds Red might perceive.

SOF's contributions to these tasks are more limited but not nil. SOF can play an essential role in "left of launch" defense against missile attacks (that is, preventive and preemptive attacks) and in eroding Red confidence in its ability to command and control its forces in time of war with the United States.

SOF and the Gray Zone

What can SOF contribute to the effort to render unrewarding Red efforts to alter regional-security orders through gray-zone tactics? Blue's deterrence objectives must be modest in this context, as the gray zone is, by definition, one in which military forces are not employed to impose costs on the enemy (therefore making threats to employ them not credible). But deterrence is not irrelevant. Red prosecutes its

interests in the gray zone in part by projecting confidence in its ability to manage the transition into overt hostilities and, thus, Blue preparations for such a transition can help to strip away Red confidence in safeguarding its interests if war erupts. Moreover, Blue may calculate that military action in the gray zone is necessary and warranted because it finds the cumulative effect of Red actions in the gray zone unacceptable. Thus, Blue's deterrence objective should be to strip away Red confidence that its gray zone actions will result in gains that are not reversible. To accomplish this objective, Blue must have the means to recover its regional position and/or to damage Red's regional position by other means.

SOF could make potentially numerous contributions in this realm. Special reconnaissance, foreign internal defense, direct action, and security-force assistance are all likely to play a role. Given the high priority Red attaches to information campaigns in its gray zone strategy, SOF's military information support operations may be especially critical, particularly if they can be knit into a whole-of-government approach.

Conclusions

In the new security environment, a new problem of strategic deterrence has emerged: conventional regional wars against nuclear-armed adversaries. The US military response to the present environment is still taking shape. A look at theories of victory of potential US adversaries reveals the specific new challenges of strategic deterrence. Meanwhile, a simple picture of the needed response from the United States and its allies reveals a broad range of potential contributions by special operations forces. Beyond this simple picture, greater fidelity is needed to tailor the further develop of SOF core activities to the new security environment.

The views expressed here are the personal views of the author and should not be attributed to the laboratory or its sponsors or any other US government agency.

Endnotes

1 *Deterrence Operations Joint Operating Concept, Version 2.0*, Department of Defense, 2006.

2 *Special Operations, Joint Publication 3-05*, Department of Defense, July 16, 2014, I-1.

3 See, for example, *Comprehensive Deterrence*, White Paper, United States Army Special Operations Command (USASOC), April 12, 2016; The Gray Zone, White Paper, USASOC, September 9, 2015; Redefining the Win, White Paper, USASOC, January 6, 2015; and Robert Haddick, How Do SOF Contribute to Comprehensive Deterrence?, Joint Special Operations University Report 17-11, JSOC, MacDill AFB, n.d.

4 Summary of the 2018 National Defense Strategy of the United States, Sharpening the American Military's Competitive Edge, US Department of Defense, December 2018.

5 *National Security Strategy of the United States of America (NSS), December 2017*, citations from the introduction.

6 *NSS*, 29

7 *National Defense Strategy (NDS)*, 1.

8 Roberts, Brad, *The Case for US Nuclear Weapons in the 21st Century* (Stanford, CA: Stanford University Press, 2015), chapters 2-5, 51-175; See also Brad Roberts, Theories of Victory, Red and Blue, Livermore Paper No. 7 (Livermore, CA: Center for Global Security Research, 2020).

9 Thornhill, Paula, and Mara Karlin, "The Chairman the Pentagon Needs," *War on the Rocks*, January 5, 2018.

10 Deterrence Operations Joint Operating Concept, 20.

11 "The Evolution of US Nuclear Policy and Posture since the End of the Cold War," in Roberts, *The Case for US Nuclear Weapons in the 21st Century*, 11-50.

12 "Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission," United States Institute of Peace, November 2018.

13 "Providing for the Common Defense," 2018.

14 "Providing for the Common Defense," 2018.

CHAPTER 5

Quantum Corps: Consequence and Superiority in the Theater of Applied Imagination[i]

Marshall M. Monroe

Introduction

There is a novel and multilevel initiative underway to unify successful real-world innovation models in a practical pattern language that can enhance and accelerate transformation management and performance. Merriam-Webster[1] defines science as "knowledge or a system of knowledge covering general truths or operation of general laws especially obtained and tested through the scientific method."[ii] Given this definition, one might describe this new focused inquiry of innovation success models as nothing short of the dawn of a new field of science. It is resulting in a unified practical framework and doctrine relevant to agile problem-solving, mission planning, product development, scientific discovery, personal performance, content creation, strategic planning, perception management, new concept operations, systems development, economic competitive advantage, and enterprise transformation.

All these topics are relevant to the planning, direct action, and optimal performance of special operations forces (SOF). This emerging science is of strategic value in high-delta environments such as the ones we face today resulting from globalism, advanced software, and digital information systems proliferation. Within the domain of national security, this doctrine is proving applicable in both kinetic (traditional military) and "soft-power"[iii] or "gray-zone"[iv] competition and conflict. Based on the nascent study and heuristics outlined herein, recommendations include advancing the new scientific domain in this space. Additionally, recommendations call for further development of new practical doctrine in this field, refinement of practical tools supporting "innovation velocity,"[v] and a coherent experiential training regimen for a new class of freedom defenders deployed in multiple theaters and contextual settings.

i The investigations, original concepts, and intellectual property disclosed herein are being commercialized under the trade name Quantum Leap Mechanics (QLMx), and this article is an excerpt from the upcoming M. Monroe book currently entitled *Making Magic.*

ii The steps of the scientific method are question, hypothesis, experiment, observation, analysis, and conclusion.

iii *Cambridge Dictionary* defines soft power as "the use of a country's cultural and economic influence to persuade other countries to do something, rather than the use of military power." Joseph Nye of Harvard University first coined the term in *Bound to Lead: The Changing Nature of American Power* (1990). https://dictionary.cambridge.org/dictionary/english/soft-power.

iv The *Cambridge Dictionary* defines the gray zone as "activities by a state that are harmful to another state and are sometimes considered to be acts of war, but are not legally acts of war." https://dictionary.cambridge.org/dictioinary/english/gray-zone.

v Innovation velocity is a widely accepted term in the business world and refers to the speed and direction of growth that an innovation creates.

We recommend creating a Quantum Corps, a new special force with specialized training for unconventional situational response and planning.[vi]

Background

The practice of conceiving new ideas and bringing them to fruition has a unique history. As a phenomenon, it has happened since recorded or known human existence, whether in the marshaling of fire as a heat source, in the forging and furnace of new types of tools (wrought from stone, iron, bronze, and titanium, or the semiconductor), or in the construction of great works, like the pyramids in Egypt and Central America, the Notre Dame cathedral in Paris, or the Burj Khalifa in Dubai. Defined in a realistic way, "applied imagination" includes a vast sweep of endeavor and consequence. From winning strategies for catching prey in the interest of survival, calculated war strikes, and in the growing of crops to social structures, political models of governance, great works of fine art, the discovery of the double helix, and the silly commercial success of the Pet Rock,[vii] "applied imagination" touches all areas of academia yet has not been declared a subject in itself. Today, the topic has been confined conceptually as a reference to dot-com-type digital-software-enabled start-up companies, but we endeavor to maintain the wider view. We reflect on how the 9/11 Commission labeled the terrorist attacks of September 11, 2001 a "failure of imagination"—leaders did not understand "the gravity of the threat."[2]

Upon simple observation, we can see the practice of applied imagination largely precedes any attempt to understand what it is that is actually going on, or any inquiry of how to get better at the practice of it. It is a fascinating phenomenon because it generally results in something new that never existed before. It is about not only "design thinking" but also conceptual breakthroughs that can take a multitude of forms—thus, it is a superset of "design." As a practice, applied imagination has left us countless expressions of itself at work, yet its ubiquity means it escapes our focused attention. We can begin to think of it like atmosphere, sunlight, procreation, consciousness, electrons orbiting a nucleus, or gravity. At once common and every day—ubiquitous—yet deeply miraculous if observed and studied at a deeper level.

The Invention of Creativity

In the mid-twentieth century, the topic of applied imagination, or innovation, or what has also been called "industrial problem-solving," took a significant leap forward with a set of observations and inquiries.[viii] Since then, a dynamic, scattered, and fragmented set of studies of the topic have taken shape.[3] Beginning with the landmark work of George Prince and William Gordon and their concept of "Synectics"

vi We expand on this concept in the Recommendations section.

vii The Pet Rock was a collectible toy made in 1975. It was marketed like live pets in a cardboard box equipped with straw and breathing holes.

viii We include a curated reading list in the bibliography. It offers a cross section of publications on the applied imagination or innovation topic.

in the 1950s, many authors and subject-matter experts have taken their pass at defining "creativity" and how to at least consider, if not master, it.[4] These inquiries exist in a broad cross section of fields of endeavor, in many cases focusing only on generating new ideas—some in the arts, some in the practice of writing, some in "start-up incubators," some in business schools, and some in engineering or science discovery. Sometimes the topic is treated on a small scale, as in the arranging of flowers, a new software service, or in works of literature or personal self-discovery. Other times it is large in scale, as in political history, industrial strategic planning, or mass social movements. Sometimes the domain is intensely technical, as in the SR-71 aircraft[ix]; other times it is more artistic or procedural. Each is of interest, but the most fascinating aspect of these studies is that none of them share a meaningful cross-reference or set of unifying and adaptive articulated themes.

Amid this backdrop, we began an effort in the 1980s to explore this topic, seeking to identify resonant themes that could begin to converge into a unifying framework. An analogy to this effort was the study of the physical laws of gravity, which began with a ubiquitous physical phenomenon, and, then, through structured observation and evaluation—such as documenting the motion of the planets—a set of equations could be derived to profile a new physical law.

High-Delta Environments

Over thousands of years of human history, the phenomenon of applied imagination can be seen at work in myriad domains. Because of the physical, molecular nature of the construction of new worlds, and in the physical or "oral tradition" forms of information distribution, the context for the actions could be described as a punctuated equilibrium. A seismic type of new concept like the Archimedes' screw[x]—or the printing press, or concrete, or live theater, or the flying buttress—would alter or impact a domain and would remain as a novel concept of operations for many years, if not decades or even centuries. But today, something new is happening. In the context of digital networks and information systems, ideas propagate faster. They come to fruition, especially in the case of software applications, at higher speed, condensing development times. Additionally, as the new concepts are absorbed and propagated, they are copied or built upon more quickly, resulting in a more fluid "theater" of operations for the innovator.

One way to illustrate this basic phenomenon is shown in the two diagrams in Figure 1, where "Q" represents quantum-type improvements and "t" is time. On the left we see what punctuated equilibrium looks like—with long periods of relative stasis in a domain, then specific, quantum-type improvements, followed by relatively

ix The CIA developed the secret A-12 OXCART in 1965. The SR-71 Blackbird was the Air Force's two-seat follow-on version. The OXCART program's innovations (there's that word again) both produced the two fastest, highest-flying, piloted jet aircraft and pioneered stealth technology.

x The Archimedes' screw is a helical surface wound around a cylindrical shaft (i.e., a screw) fitted inside a hollow pipe or trough. The unit is set up at an angle to the water. Turning the shaft raises the water up the helical structure to the top end.

long periods of relative stasis. An example of this might be in the travel domain, with the sequence being first walking barefoot, then walking in shoes, then riding a domesticated horse, then riding in a carriage, then in a car, in a plane, in a jet, and so on. On the right we see something more akin to the innovator's environment today, where new ideas are appearing more frequently, and the "half-life" of novelty, and any subsequent competitive advantage generated thereby, is much, much shorter. Examples of this might be the graphics processing unit (GPU), machine-learning algorithms, or multirotor drones, where improvements keep coming and seemingly not a week goes by that another innovation does not improve the performance, opportunity, and threat implications of these devices.

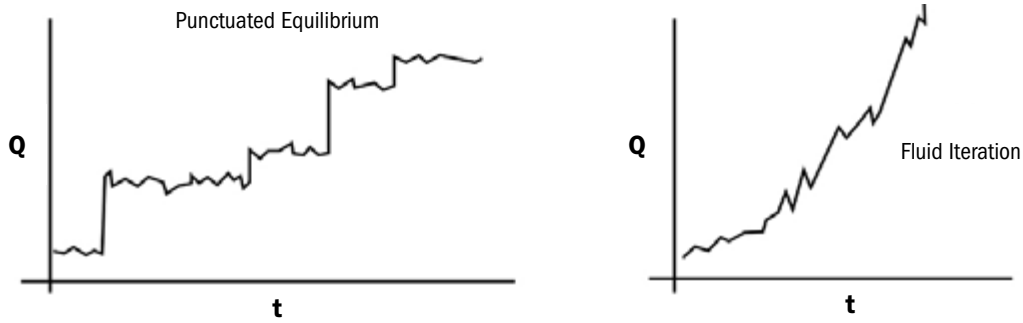


Figure 1. Punctuated equilibrium vs. fluid iteration, where Q represents quantum-type improvements and t is time.

We identified the modern high-delta environment context three decades ago, which formed the motivation to investigate this topic and build practical frameworks to help navigate the current and near-horizon world.

The Emerging Framework—Quantum Leap Mechanics (QLMx)

After three and a half decades of study as a practitioner in this innovation field, including consideration given to existing thought and resources on the broad topic, we have identified that the nature of optimal conceptual progress is best described as a pattern language. This means a number of concurrent critical "factors" are in play and at work as new concepts are formed, refined, developed, and deployed. This observation has come from an intentional investigation at the professional practitioner level in a multitude of application areas, including:

- Private-Sector Entertainment Content and Product Development
- Commercial Industry Resorts and Theme Parks (Innovation at Municipal Scale)
- National Security Intelligence Tradecraft
- Regional Economic Development—Generating multiple billions of dollars in public-sector impact

- Industry Transformation—Agriculture Technology Systems
- Nonprofit Advancement, Operations, and Communications
- eRetail and Mobile Application Development
- Illusioneering
- Venture Capital Investing—Start-up Acceleration
- Real Estate Development

Special Operations Strategic Planning across Multiple Domains

At the highest level, the concept of innovation can be compared to how an electron orbits a nucleus in an atom, as shown in Figure 3. The electrons seem—for reasons not entirely understood—to prefer certain levels (n) of sustainable motion pattern, or orbitals. Upon the injection of sufficient energy (E) an electron can be moved up in energy level, but this transition generally happens in an all-or-nothing shift. Similarly, when an electron drops in energy level, it moves to a lower orbital and a unit of energy is released in the form of light, or electromagnetic energy (hv; where h is Planck's constant and v is the frequency of the electromagnetic radiation). This is the origin of the concept of "quantum" transition.

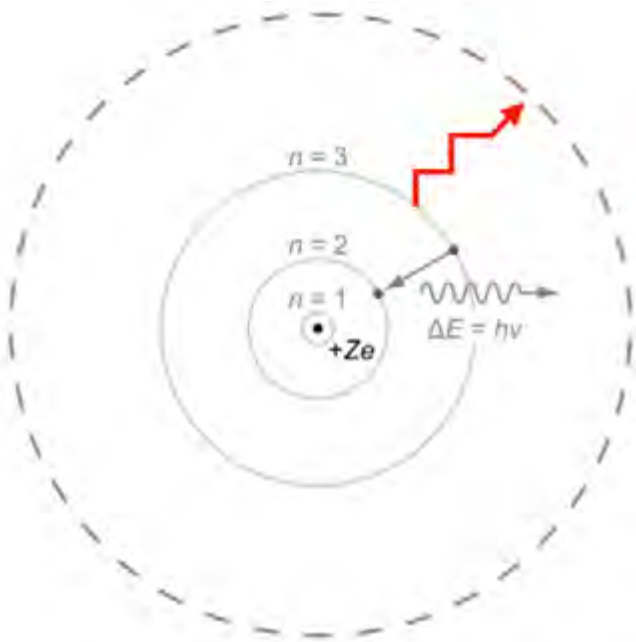


Figure 3. Illustration of electron orbitals around the nucleus of an atom.

Because of the symbolic value of this pattern found in nature, and because it is consistent with the nature of consequential innovation for purposes of this study, the quantum-physics model became a foundational element of our present investigation.

In the process of observing and working across these domains, and within this notion of Quantum Leap Mechanics, the resuting framework is communicated visually in Figure 4.

Figure 4. Mandala of Quantum Leap Mechanics framework.

This diagram, or mandala, represents the simultaneous workings of seven different core-quality patterns that together constitute what we have dubbed the Quantum Leap Mechanics model for innovation velocity. These concurrent core-quality patterns are given basic, familiar names, with each representing broad and deep compartments of endeavor. The core orbitals are summarized as follows:

SketchPad, S_P (circle)

- Ideation; including Beginner's Mind and Scribbles; Blue Sky, Concept Formation
- Includes Aesthetics, Multi-Modal Communication and Visualization—Design and Style
- Includes Tools for Seeing Problems in New Ways—Brainstorming, Art of the Possible
- Persona for this is an enthusiastic child, Charles Eames,[xi] crayons to the paper's edge

TextBook, T_B ("Diamond" tip)

- Science, Technology, Natural Laws, Mathematics—Height of Abstraction

xi Charles Eames (1907-1978) was an American designer, architect, and filmmaker.

- Can't fake this, requires education—Calculus, FFTs,[xii] Dif. EQs,[xiii] Physics
- Enables leaps in performance, transcending intuition; Experimentation Rigor
- Persona for this is J. Robert Oppenheimer, Albert Einstein, or Richard Feynman

Balance Sheet, B_S (little square in bigger square)

- Business, Profit Motive, Accounting, Law, Regulatory Context, Tax, Capital Formation
- Various models for reward, Risk Management, Project Delivery, Human Resource Management
- Persona for this is Warren Buffett, Michael Boskin, or Jim Cramer

WorkBench, W_B (rectangle)

- Prototyping, Tools, Testing, Crafts, Shop Space, Garage, and Scale Fluency
- Includes Fabrication Skills—Code, Shop, Machines, Materials, Attitude, Work Ethic
- Think of a construction foreperson or general contractor—a good one
- Persona for this Leslie Groves, director of the Manhattan Project

MarketPlace/COTS,[xiv] M_P ("line"/extended rectangle)

- Available Components, Expertise, Products, Services—Supply Chain
- Search Engines, Machine-Learning (ML) Tools, Trade Shows, Worldliness, Image and Video Libraries
- New Tools for Search and Reference Cataloging, Prior Art, Competitors
- Persona for this is Lily Tomlin as the switchboard operator Ernestine,[xv] Connectors

PlayBill—"ART", P_B (ring)

- Myth, Mystery, Primal Urges, Biological Drives, Emotion, Intuition, Subconscious
- Fear, Love, Addiction, Obsession, Desire, Lust, Tragedy, Greed, Glory
- Gender Affordances, Attractions, Life, Birth, Death, Procreation, Generational Lines
- Symbolic and Archetypal Elements—Hero, Mentor, Guardian, Villain, Siren, Muse
- Persona for this is Rafiki in *Lion King*, Yoda, and William Shakespeare

xii FFT is an acronym for fast Fourier transform, an efficient algorithm used widely in engineering, music, and science for signal processing.

xiii Dif. EQs stands for differential equations. This is a mathematical equation that relates one of more functions and their derivatives. The function typically represents physical quantities, the derivatives are the rate of change, and the differential equation defines the relationship between the two. Applications include modeling cancer growth, the transfer of electricity, and modeling investment returns.

xiv i.e., commercial off-the-shelf.

xv A recurring character on the television show *Rowan & Martin's Laugh-In* (1967-1973).

GoodLife, G_L (triangle)

- Values, Ethics, Trust, Community, Morality, the "Soul" of Motives
- The Inherently Social Aspects of Change and Transformation
- The benefits and risks of peer pressure, purpose, conformity
- Faith (rapidly becoming an undiscussable topic), Deep Significance, Spirit
- Critical Factor for High and Ultimate Risk Environments (Pilgrims)
- Persona for this is Stephen Covey, Billy Graham, Mother Teresa

Beyond the individual core-orbital qualities outlined above, the key is to train conceptual thinkers to shift among these various mindsets and consider any idea or initiative with each in mind. A key framework for this understanding is the "Monroe Muscle Theory of Mind," where multiple cognitive modalities work in concert with one another—and often in opposition to one another—to effect functional results. One will quickly notice that in our consciousness, these modalities do not appreciate, or even care to acknowledge, one another. Over time, and with structured training, the skills develop to enable quick and agile changes in perspective, for rapid triage and refinement of concepts. An omni-lateral awareness develops and serves the process. This framework also informs team design.

A Preliminary Mathematical Framework

The exploration of this topic begins with understanding the roles of time and "degrees of novelty," which form the basis for measurement and prediction. In this model, the basic form of a parabola is used to approximate the energy profile of an innovation initiative, as illustrated in Figure 5. As defined in Figure 1, "Q" represents quantum-type improvements, and "t" is time. This premise of a parabola is taken as a broad approximation only and is used to assist in the development of a model framework for early evaluation. In this approach, the time duration (t) of an innovative project is taken as "P," which, in the diagram, is P_1 for the slower, longer type of project and P_2 for an accelerated, high-speed implementation. The latter is a desired relative outcome of this project, with innovation delivered at a sustained high quality, but in a shorter amount of time.

The formula portrayed in the figure is the vertex form of a parabolic equation, where Q is the peak of the parabola, P/2 is the midpoint of the parabola, -Q/(P/2) is the vertex of the downward facing parabola, and $-Q/(P/2)^2$ is the factor, K_Q, that determines the width of the parabola, identified as the "Kink." The "x" in the formula is really "t," time. By further extension, the equation for calculating the concurrent investment, I, and resultant value derived by a full-spectrum innovation project would be:

General Form:

$$I_Q = \int_0^P K_Q \left(S_P + T_B + M_P + B_S + P_B + W_B + G_L \right)^2 dt$$

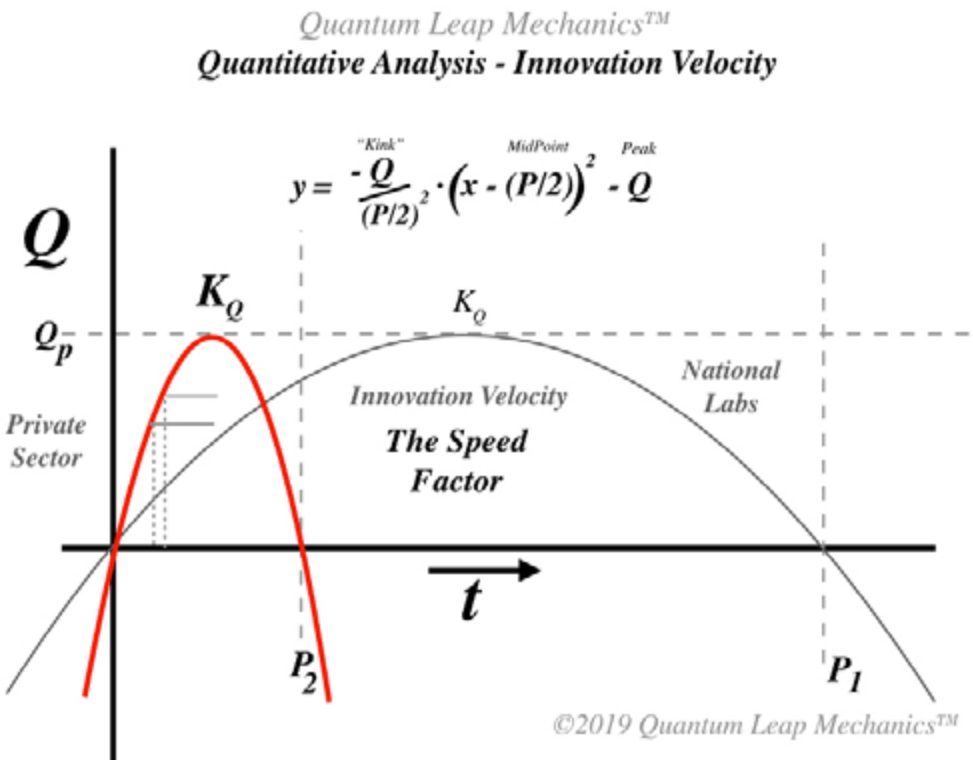


Figure 5. A normalized, parametric view of the journey from initiation to fruition in creative projects.

On first exposure, this type of mathematical treatment of a largely amorphous phenomenon, like "degrees of novelty," seems somewhat far-fetched. Yet when we compare it to the early concepts of measuring and deriving universal constants related to the force of gravity, it becomes less crazy. The key lies in the establishment of measures and units thereof. Furthermore, we begin to see that if we do grow this model and approach, we may find that new software-enabled tools may begin to take shape that can help us with this process.

An Innovation and Quantum Leap Archetype

Figure 6 represents a summary framework for discussing new concepts, their formation (the Vision), and the Journey to Fruition. This framework emphasizes representing all the elements of an instance of successfully expressed applied imagination. In this case, a sphere represents the preexisting reality, and a reticle and related new, if not focused, sphere identifies the new reality. The colors of the steps represent not only the need for a managed temporal sequence to fruition but also the concurrent core-quality factors that should be managed along the way. Importantly, this discourse is intentionally limited to the practice of applied imagination toward a beneficial or preferred outcome and does not give full consideration to raw "creativity," which can include random ideas with no intention or goal of fruition.

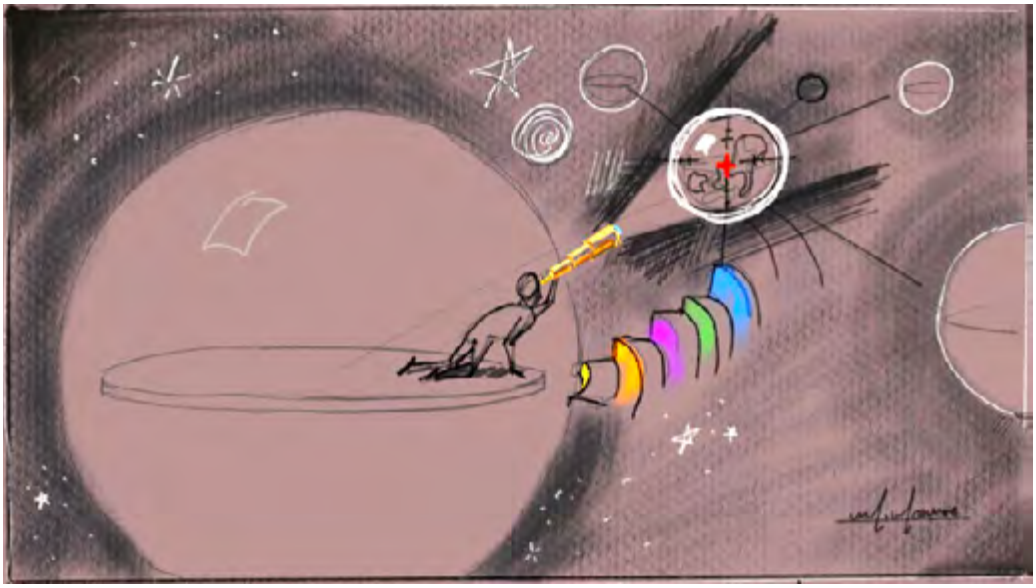


Figure 6. The Vision and Journey to Fruition.

The Narrative Crosscut—Story Matters

Simultaneous with the structured core-qualities framework is the novel insight that conceptual leaps are best mapped and planned with a storytelling approach and toolset.

The core of this insight comes from observation about what tools and processes have resulted in the greatest "leaps" of human conceptual thought. One way to envision this is the Hero's Journey Spiral, illustrated in Figure 7. We adapted it from the classic hero's journey, a common narrative taught in writing classes. The latter involves the hero enbarking on a journey—leaving the familiar world behind, learning a lesson, applying the lesson to win a victory, and returning home a tranformed person. In the Hero's Journey Spiral, the hero "spirals around" thinking, then comes up with an idea that begins to take him out of the spiral, past the familiar or status

quo threshhold—indicated with the dashed line—onto an innovation journey, resulting in a breakthrough—the star in Figure 7. The hero comes back and contemplates again.

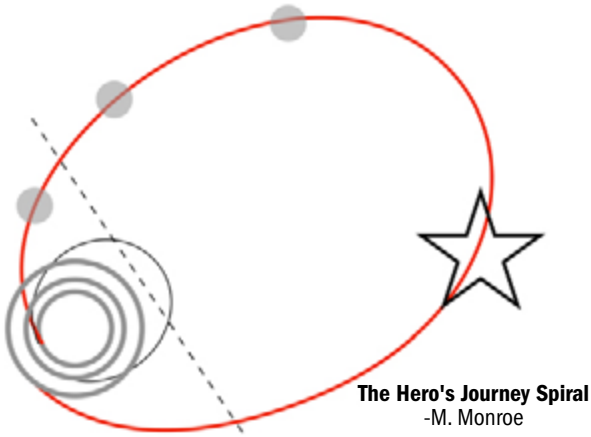


Figure 7.

Let us journey back in this inquiry to the ancient Greeks and their invention of the concept of drama as a tool and process for inquiry and collaborative thought. The Greeks not only engaged language and discourse but also pioneered a new, deeper application of stage and proscenium (forestage) for the purpose of examining the relational and associative elements of the human condition and the nature of existence. We can look to the landscapes of Greece and Rome to see how significant this concept became to their society. The amphitheater pictured in Figure 8 outside Florence, Italy is a great example.

Figure 8. Photo of amphitheater outside Florence, Italy.

Theater helped initiate massive leaps forward in concepts of democracy, social order, rule of law, property rights, and a civic logic. Story and story arts, therefore, formed a key component of the engine and thrust of Western values and successes.

As such, this modality of examination and conceptual exploration has come to the center of the Quantum Leap Mechanics model. We see there are two broad categories of theater:

- Recreational, Kinetic, Acrobatic, and Visually Mesmerizing Theater
  - Emphasis on Presentational Delight, Daring, and Physical Agility
- Deeper, Relational, and Associative Conceptual Theater/Drama/Opera
  - Consisting of narratives that reflect more profound subjects and themes
  - These deeper models can achieve a transformation of consciousness

Story, Drama, Theater, and History

From a historical perspective, storytelling has been a survival factor all the way back to the cave paintings. We capture the ancient Greeks and Romans as advancing the concepts of theater, then we see Shakespeare and his stunning aptitude for language and conveyance in the form of a five-act play. Into the modern age, we see Walt Disney discovering the new art of animation, along with television and film; he took story into a new dimension with the invention of the theme park. Finally, today, computer graphics enable an entirely new engagement with story, and we engage these technologies in the Quantum Leap Mechanics toolkit, including in the QLMx Scenario Centers and in the Quantum Hologram Workstation (QHW) Development.

Courting the Muse

This framework does not prescribe a thought process or a specific sequence of events that will lead to great ideas and fruition because the specifics of process vary greatly by application and circumstances. Consequently, the QLMx framework provides a way to dislodge an individual's or a team's thinking from a rut and shift it to a new angle, with core qualities like facets of a finely crafted diamond. It is an audit of sorts, but an audit with process implications.

As such, the system outlined in this chapter is conveyed and communicated in various "vehicles," depending on the audience age, culture, and sophistication. For young people, the prevailing metaphor is a space shuttle–type rocket ship, with the liquid and solid rocket boosters being analogous to skills, reference research, and discipline. Distant stars and the orbiter are analogous to dreams and new ideas. For adult professionals, the model can be shared using a diamond analogy, with facets and precision analogous to the core-qualities refinement model, with implications of creating an object or result of enduring value. In some cases, the topic can remain more abstract and theoretical, but only when the audience is prepared for such an approach. In all cases, the premise is the transition from an existing, or "normal," state to a more preferable elevated, or "energized," state.

Application Dimensions

The Quantum Leap Mechanics framework is applicable at multiple levels. Each of these operational dimensions contributes to overall innovation and fruition performance.

Talent and Team Elements

Everyone has the capacity to use their imagination. It is the harnessing of this ability through literacy and skills development that this fundamental ability is leveraged. While some people can be trained for excellence in all areas of the orbital-quality matrix, it is often better to build a small team that together covers all the bases of need. This is a result of the cognitive and personal uniqueness of human personalities and types, which may or may not include personal life experience and context.

Facility and Tools

This new doctrine has strong implications for what kind of environment and tools are optimal for accelerated, high-velocity innovation. Innovation and quantum activities are messy. They also do not lend themselves to hipster interior environments and a constant spotlight of evaluation. Picture a garage. A garage of someone who likes to make stuff and try things. Now add advanced manufacturing, an art atelier for concepts, a television soundstage, and a feature-film-grade animation and postproduction suite. This mix of venues is not typically colocated. But this is a concept kitchen. Talent and tools must be quantum and omni-lateral. One process map is shown below in Figure 9.

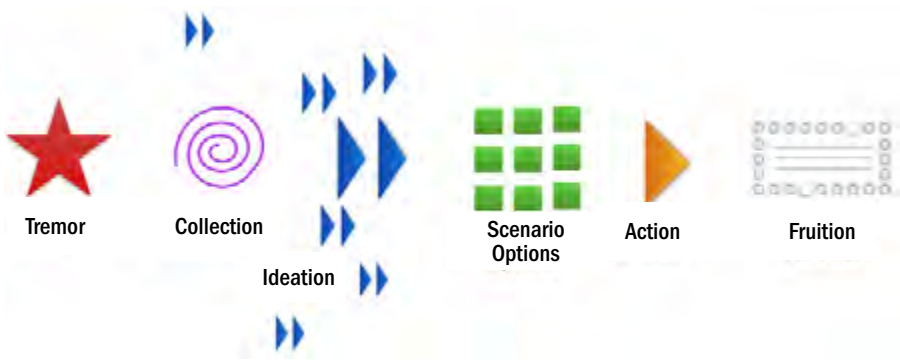


Figure 9. Process Framework: From project initiation to fruition (M. Monroe).

As we study this topic in concept, we are also building specialized tools designed specifically to use the frameworks and increase the velocity of innovation in individuals, teams, enterprises, and metaorganizations. One such tool is MIXONIUM, a content-management platform that allows for the rapid mash-up of disparate file types into a URL post that can be easily tagged, enriched, and shared. Another tool is VibeWyre, which allows one to follow social media sources easily under a channel

topic. This allows for a near real-time monitoring of ideas and insights in a particular field or on a particular topic.

Organizational Scale

Individual/Personal—Q-Self
This technology and related systems lend themselves to personal assessment and increased performance. The idea is to explore and optimize the "Quantum Self" by taking individual capability to the next level, using the quantum orbitals as a framework for assessment and reflection. We are building a personal development program at the Magic Canyon Institute that identifies strengths, weaknesses, and growth opportunities for civilian and military personnel at all levels. A key management factor is realizing that every individual that touches an innovative effort has power to substantially enhance, or hinder, optimal outcomes. The core objective is actionable literacy.

Small Team—Q-Cell(s)
At this scale, the system is ideally suited for training and enhancement of existing SOF. Not only could the system improve existing specialty teams, but there could be a regimen assembled for the creation of an entirely new SOF team—tentatively dubbed "Q-Cell"—that is specifically selected and trained in this quantum type of problem-solving.

Enterprise—The Quantum Horizon Laboratory
In situations where an enterprise has an interest for a purpose-built organizational element in the service of quantum innovation, we have developed the Quantum Horizon Laboratory concept, which includes conceptual, rapid prototyping, field survey, intellectual property (IP), and management elements. This approach is not classical "R&D" but rather applied development, or "research and deployment," with a constant tether to operational elements of the overall enterprise mission. This allows for disruptive concepts as well as ongoing support for existing operations.

Intra-Enterprise—Quantum Latency Council
At the large scale, we envision a system like the quantum-horizon concept to be taken to an even higher level at the Department of Defense (DOD) or Department of Energy (DOE) level, or even the intelligence community (IC) level, wherein innovation is fostered across enterprises via an information-technology empowered advisory hub. This could be an extension of the existing strategic latency concept, leveraging existing efforts and reinvigorating some older advisory concepts that have lost relevance in the highly dynamic environments faced today by special operators.

Heuristics—Blue Sky and Reduction to Practice

One key finding about applied creativity is that when high levels of performance are required, the best path to improvement is actual practice and kinesthetic involvement. An analogy is that one might read for years about playing the violin, but upon picking up an instrument, the sound would be less than worthy of Carnegie Hall. Applied imagination is a muscle-memory and tools domain.

Yes, we do believe that lightning can strike—an idea can pop to a random person and they capture it—but the QLMx process is about fostering literacy and capacity from ideation through fruition, which requires more rigor and preparation, and can increase the probability of seismic success. As such, training and certifications in this field must involve actual problem-solving or creative practice.

An additional element of heuristics is that we firmly believe the model of a new science should be tested against reality and evaluated against actual successes and failures. Hence, we study many case histories through a growing program of Quantum Walkabout guided tours, to see and consider innovations in their environments—as in Walt Disney World, inside laboratories, and in private-sector environments. This includes bloopers—like the steel ball shattering a Tesla truck window (which Elon Musk attributed to damage of the window before the test) during a live demonstration.[5]

One internal descriptive term for this audit approach is "omni-lateral" thinking and orientation. This framework is not just an area of focus during ideation. It is critical to maintain this "worldview" through production and implementation. Hence the strong emphasis on real-world engagement.

Science Fiction—Quantum Corps—A Glimpse to the Forward Operating Environment

Imagine that we find ourselves in something we might call the Info Stone Age. As transformational as digital tools have been in the twenty-first century, we are only at the beginning of what they can imply for the publishing, sharing, and access to capability and ideas. A simple example would be the area of learning music. The access to video as a communication tool has transformed the art form and democratized who has access to "inside-baseball" information about the theory, practice, and production of world-class music recordings. Kids the world over can find out how to make great electric guitar distortion sounds, how to mic a classical guitar, and how to stack vocals—techniques reserved for the inner sanctums of recording studios just a few years ago. Digital access has altered the landscape of competition globally, expanding the field of competent practitioners, and reducing the advantage of incumbant experts. This trajectory is at once exciting and vexing for those using innovation as a platform for advantage.

Now imagine that the Special Operations Command leadership embraces the sweeping change being brought on by digital technologies and information systems, and the result is a new kind of specialized tiger team. In order to achieve and sustain

innovation superiority, the team would be trained in the optimal applied imagination platforms, with skills identified and honed with continuous training, on the order of how current teams are trained for marksmanship, communication, or intelligence, surveillance, and reconnaissance (ISR). There would be drills. Lots of drills. Quantum innovation is like marksmanship or flying an aircraft. It is best done through routine practice and updating certifications. One can envision a quantum corps dedicated to rapid and agile innovation, scanning the globe for new concepts, integrating them into larger systems deployments, crafting agile first-article deliverables, and traveling to theaters of operation as needed. This corps would have a patch, a regimen, and a coach—or set of coaches—in the same manner that special operations teams have strength and cognitive performance coaches.

As part of this new capability initiative, it is important to continually revisit the notion that the focus of a Quantum Leap Mechanics innovation velocity effort is the creation of utterly new systems and solutions. This is a shift from drilling on known exercises with predicted outcomes. The outcomes in this case are new things, new concepts, and new ways of succeeding or meeting mission requirements. It is like a form of magic—bringing into existence something that has not existed before.

In Figure 10, a team coordinates to bring a fictitious "rabbit out of a hat," using a new practice or a new coalition of skills. In the future, this may be an endeavor in the traditional kinetic area of combat or operations, but it may also be in the realms of soft power, in an emerging world of ubiquitous ISR, or in a real world we have yet to discover and inhabit.

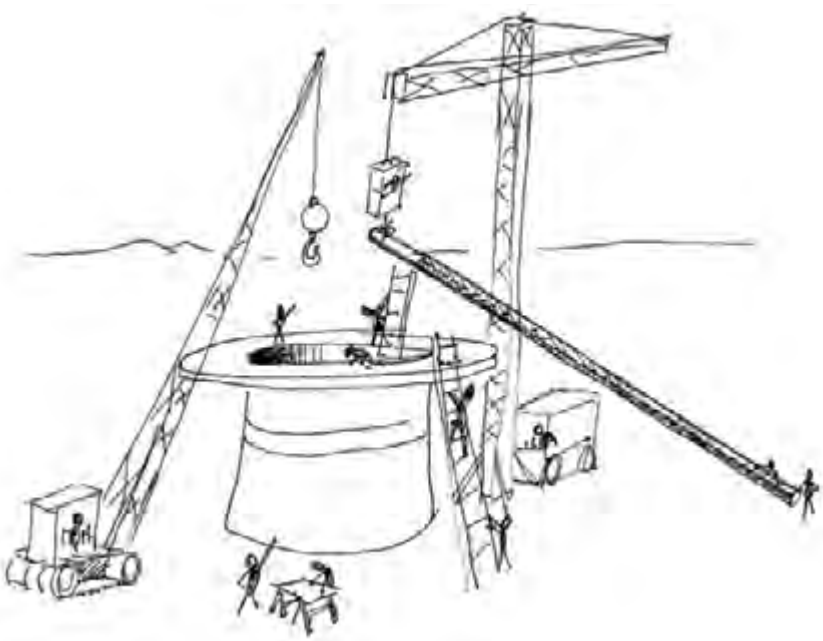


Figure 10. Making Magic: A fictitious collaborative endeavor to pull a rabbit out of a hat (M. Monroe).

Recommendations

Q-Cells, New SOF Corps

There needs to be an aggressive effort to take the existing Quantum Leap Mechanics framework and translate it into a curriculum that special operations personnel and policy leadership can use in confronting nonstandard national security challenges. This type of program could spawn utterly new concepts, and it could be activated to help solve new and emerging operational needs for the SOF and the Joint Special Operations Command (JSOC). Like air, ground, and cyber superiority, there needs to be a new priority placed on "conceptual agility superiority" in the US national security enterprise. In its most actualized form, this could be the genesis for a new special force, operationally named the Quantum Corps, with specialized training for unconventional situational response and planning. The prototype for this could be a heightened, elevated, and expanded JSOCx.

Q-Cells Training Camp, Facility, and Program

We believe there should be a physical center and virtual collaboration toolkit to aid in the operation of a training and concept-development regimen. Prototypes of this type of experiential, location-based programming have been tested at the Magic Canyon Institute, Ranch, and Wildlife Park in northern New Mexico, and the proprietary digital content management system MIXONIUM has been implemented as a key element of creative collaboration operations. Programs can range from low-intensity workshops to extreme and intense boot-camp-type immersion, including tangible adversity. We also suggest exploring a location-based facility and program in or near the Walt Disney World area of central Florida, because of the unprecedented concentration of innovative constructs and designs within that roughly 20-mile radius region. One key reason for the location-based approach in this digitally connected age is that true literacy and skill in this domain requires dialogue and self-confrontation at a level that warrants close human contact for support, instruction, and adaptation of principles to specific operational requirements. The young generation of today that is buffeted by countless false and subversive messages, and credentialed authenticity will be a pillar of success for any program like this.

Quantum Council

We believe while various advisory boards and commissions in the national security system for advising on science-and-technology (S&T) areas already exist, there should be a new board—perhaps as a replacement for the DOD Jason program—that is based on these agile innovation principles. This structure is sourced from the rapidly moving private sector, and as globalization and digital networks continue to advance, the "velocity" of innovation in the US government will need to keep pace. This framework and the organizational implications could assist in this area. As an example, we believe an effective approach would be to take the SOCOM strategic

latency initiative and expand it with resources and a talent network to fit this goal. There should be a specialized university partner construct.

New Digital Tools—Augmented Innovation

As a new and unified field theory of applied imagination and innovation velocity continues to take shape, we can actively develop tools to improve the process of formulating ideas and concepts, for bringing them to life and fruition. The emerging QLMx framework provides a superstructure for tools advancement and at least partial automation. At Marshall Monroe MAGIC, this vision is taking shape across a number of technology platforms. These include the incubation of MIXONIUM Ultra Media, a patented technology for curating and passing packets of rich media that transcends file types and represents a new communication form. It is a format ready-made for code automation via artificial intelligence, machine learning, and spatial computing. These efforts include a comprehensive look at telematics, and how augmented, mixed, and virtual reality can be used not only to play games or reproduce the existing world but also to play with ideas—to augment the practice of innovation itself. This work also includes the invention of a new type of collaborative scenario studio—leveraging digital tools and rich natural environments to create an optimal setting and "space" for the birthing and deployment of new ideas. We will continue to advance the concepts, with implications for partners and allies as the demand for transformation and the "need for speed" of concept development increases.

Freedom to Innovate

As the pressure from aggressive authoritarian dictatorships and communism continues to be felt across the globe and right in our pockets on every smartphone, we believe this topic might be an important vehicle for raising awareness and valuing the concepts of Western free enterprise and democracy—including the right to the pursuit of happiness and of reimagining one's station in life, rather than a hollow promise of guaranteed equal outcomes as prescribed by the state. As such, one engagement option would be to open an applied creativity workshop or "boot camp" for young and old who wish to engage with this profound topic. This could be an expanded "makers fair"–type venue, or something with a more artistic focus, akin to a writer's workshop or music camp. This type of youth and family programming has also been tested at the Magic Canyon Institute, Ranch, and Wildlife Park. One extreme example of this notion would be to connect an effort like this with the original vision for EPCOT—the Experimental Prototype Community of Tomorrow—in Walt Disney World. This is a matter of national competitiveness at a consequential scale.

Conclusion

As a student of new ideas and their pathways to fruition, I am honored and consider it a privilege to contribute to a volume like the *Strategic Latency Unleashed*. Unlike extraction industries, which consume resources and may be at best "renewable"

or "sustainable," applied imagination is "*exponentiable*," in that with each new advancement, more becomes possible, and the raw material of capability and capacity is not reduced or preserved, but, rather, increases.

Looking ahead with a "2020 Vision" and beyond, we anticipate the current conditions of a high-delta national security environment will continue, as artificial intelligence, machine learning, global soft-power networks, robots, automated/UAS vehicles, metamaterials, big data, mixed-reality systems, spatial computing, digital devices, and virtual worlds continue to evolve. Consequently, a new science directly applicable to navigating and leveraging new contexts could, and should, be explored further.

Appendix: QLMx Innovation Literacy and Articles Compendium

Component-detail articles by M. Monroe illuminate additional factors and practical models for an optimal applied creative process. These insights and approaches are original and based on empirical observation and testing. They include the following:

1. Orders of Innovation: Check Your Passport—Q.CON 0-1-2-3[xvi]
2. The Oak and the Acorn—Legacy v. Novelty in Managing Innovation Strategy
   Concepts of Routine, Habit, Confirmation Bias, and Hidden Algorithm
3. "Heat Vision"—Soft Focus, Nonverbal Communication, and Equestrian Arts
4. Epic Creativity Stories: Glory (Disneyland) and Bloopers (Kodak, Sears)
5. Virus/Host—a Procreation Model for Spawning, Identity, and Ownership
6. How to Brainstorm and Make Meetings Not Suck
7. The History of Creativity: A Humbling View—World Events, USG S&T, VC, USPTO
8. State-Sponsored, Weaponized Innovation—PRC, EU, S. Korea, Airbus
9. Resiliency, Determination, Obstacles and the Quicksilver Quotient
10. Rendering and Movie Poster—The End-State Nirvana Image
11. The Nirvana Scenario—Dream for Ultimate Success and Work Backwards
12. Holodex, MxR.HIVE—Inventory of Industry, Markets, Situation Awareness
13. Blue Sky Project Management—The QLMx Method
14. The Omni-Lateral Team—Casting and Assessing Small Groups for Creative Agility
15. Explaining the Dream—Walt and the Wonderful World of Disney (Disneyland)
16. Reality Radar—Deep Dive Assumption Assessment and Inventory
    Patterns of life, habits, sacred-cow tipping
17. Media Mindfulness—The Potential and Perils of Infinite Digital Content
    Black box algorithms, plausible deniability, and platform bias
    The Power and Risks of Weaponized Peer Pressure, Propaganda, IW
18. Creative Dark Matters—How to Poison the Well and Reduce Creative Output

xvi This is a work mode for the program analogous to the DEFCON status system, with numeric designations indicating "CONditions" for readiness and response. In this case, Q.CON represents the quantum conditions of a situation. For example, Q.CON-0: Stasis and Precision Desired—No Need for Innovation (typical military/franchise operations—execution priority); Q.CON-1: Orderly, Incremental Improvement Desired (product development, design, or iteration—oak innovation); Q.CON-2: Need for Mild Structural Realignment; Adjacent Ideas (venture pivot, core capacity intact, management disruption); Q.CON-3: Radical and Revolutionary Ideas Required or Desired—Acorn (seismic shift, values, and survival fear awakened, threatened).

Anti-creative infections and sabotage strategies; clutter and distraction

19. Phases of Quantum Transformation
    Phases of Vision—background scan, prior art inventory, ideation, scenarios
    Phases of the Fruition Journey—rapid prototype, mobilize, test, repair, deploy
20. Divine Intervention—Why Western Cultures Innovate and Discover More
21. Consumer v. Innovator—Transcending Imitation and Conformity with Integrity
22. Teatro Magico—Drama, Story, and Concept Development
    The scenario video; role playing; living laboratories
    New applications of 3D real-time cgi systems—AR/XR/MxR
23. Monroe Muscle Theory of Mind
    Isometric cognitive modalities, fluency and agility; the human figure
24. Boot Camp, Fitness, and the Anatomy of Optimal Creativity
    Exercise, health, dopamine, fatigue, and stimulation
25. Fuel Mixture, Vectored Thrust—Role of the Producer and Production Assistant
    A New View on "Management" and Administration
26. Linguistics—Words Matter
    Selective use of words, in a plural world
27. Ownership Topology—Managing the Invisible Physics of Attribution
    Virus, host, and the biological strategies for offspring
28. The Diamond Mine—Exercises for Lateral Leap Literacy Aptitude
    Including case studies and related rich media

Bibliography

A curated suggested reading list on applied imagination or innovation. Each publication touches on elements of the overall topic, sometimes focusing mainly on generating new concepts, other times in the execution of a well-articulated vision. These are selected intentionally to offer a cross section of the topic, and the list is not comprehensive.

Adams, James, *Conceptual Blockbusting*, Basic, 1979/2001.

Arnold, Stephanie, *The Creative Spirit: An Introduction to Theater*, McGraw-Hill, 2010.

The Bible, New International Version, Zondervan, 2011.

Bird, Kai, *American Prometheus: The Triumph and Tragedy of J. Robert Oppenheimer*, Vintage, 2006.

Boorstin, Daniel J., *The Discoverers: A History of Man's Search to Know His World, and Himself*, Vintage, 1985.

Boorstin, Daniel J., *The Creators: A History of Heroes of the Imagination*, Vintage, 1993.

Campbell, Joseph, *The Hero with a Thousand Faces*, Pantheon, 1949.

Cervantes, Miguel de, *The Ingenious Gentleman Don Quixote of La Mancha*, Ecco, 1605/2005.

Christensen, Clayton, *The Innovator's Dilemma, When New Technologies Cause Great Firms to Fail*, Harvard, 1997.

Crawford, Matthew, *Shop Class as Soulcraft: An Inquiry into the Value of Work*, Penguin, 2010.

Csikszentmihalyi, M., *Flow, The Psychology of Optimal Experience*, Harper, 1990/2008.

Cussler, Clive, *Poseidon's Arrow*, Putnum, 2012.

Eames, Charles, and Ray Eames, *Powers of Ten: A Flipbook*, Freeman, 1998.

Feynman, Richard, *Lectures on Physics*, Pearson P.T.R., 1970.

Golden, John, *Principles of Patent Law, Cases and Materials*, Foundation, 2018.

Goleman, Daniel, *The Creative Spirit: Companion to the PBS Television Series*, Dutton, 1992.

Goleman, Daniel, *Emotional Intelligence: Why It Can Matter More than IQ*, Bantam, 2005.

Gordon, William, *Synectics: The Development of Creative Capacity*, Harper, 1961.

Gordon, William, *The Practice of Creativity, a Manual for Dynamic Group Problem-Solving*, Echo, Point, 2012.

Hofstadter, Douglas, *Goodel, Escher, Bach: An Eternal Golden Braid*, Basic, 1979.

Johnston, Ollie, *The Illusion of Life: Disney Animation*, Disney Editions, 1995.

Kelley, Tom, *The Art of Innovation*, Currency, 2001.

Lefevre, Michael, *Managing Design*, Wiley, 2019.

Levey, Sydney, *Design-Build Project Delivery: Managing the Building Process, from Proposal through Construction,* McGraw-Hill, 2006.

McKim, Sam, *Experiences in Visual Thinking*, Cengage Learning, 1980.

Miles, Barry, *Paul McCartney: Many Years from Now*, Holt, 1998.

Monroe, Marshall M., *Dream Too BIG?,* MMMAGIC, 2001.

Monroe, Marshall M., *The Oak and the Acorn, a Model of Applied Imagination*, 2019.

Moore, Graham, *The Last Days of Night: A Novel*, Random House, 2017.

Neuhart, John, *Eames Design*, Abrahms, 1989.

Newton, Sir Isaac, *Opticks, or a Treatise on the Reflections, Refractions, Inflections, and Colours of Light*, Dover, 1675/2012.

Porter, Michael E., *Competitive Strategy: Techniques for Analyzing Industries and Competitors*, Free Press, 1998.

Rich, Ben, *Skunk Works: A Personal Memoir of My Years at Lockheed*, Back Bay, 1996.

Storr, Anthony, *Music and the Mind*, Ballantine, 1993.

Tipler, Paul A., *Physics for Scientists and Engineers*, 6th ed., Freeman, 2007.

Ueland, Brenda, *If You Want to Write: A Book about Art, Independence, and Spirit*, Martino, 2002.

Windsor, H. H., *The Boy Mechanic, Volume 1: 700 Things for Boys to Do*, Popular Mechanics, 1913.

Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* Public Affairs, 2019.

Endnotes

1 Merriam-Webster, https://www.merriam-webster.com/dictionary/science.

2 "The 9/11 Commission Report: Executive Summary," Final Report of the National Commission on Terrorist Attacks upon the United States, August 21, 2004, https://govinfo.library.unt.edu/911/report/911Report_Exec.htm.

3 For example, Adams, James, *Conceptual Blockbusting*, Basic, 1979, and Christensen, Clayton, *The Innovator's Dilemma, When New Technologies Cause Great Firms to Fail*, Harvard, 1997.

4 William Gordon, *Synetics, the Development of Creative Capacity*, Harper, (1961).

5 Valdés-Dapena, Peter. "Elon Musk Explains Why the Cybertruck's Windows Broke," *CNN Business*, Cable News Network, November 26, 2019, https://www.cnn.com/2019/11/25/cars/elon-musk-tesla-cybertruck-window-glass-broke/index.html.

CHAPTER 6

Russia's Special Purpose Forces: A Strategic Weapon

Major Jonathan N. Fagins, Michael Nacht, and Glenn Chafetz

Introduction

When Russian president Vladimir Putin authorized military intervention in Syria in 2015, the international community turned its attention to Russia's use of unconventional forces, most notably Spetsnaz. Western states, however, remain unsure about what Spetsnaz is, what it does, and how it fits in among other Russian "unconventional" (or "hybrid"/"special") forces. The confusion stems from nomenclature, the breadth and variety of Spetsnaz itself, and the fact that the Russian government has used a variety of different institutions and methods to achieve its goals in Syria, Ukraine, and elsewhere.[i]

This chapter argues primarily that Putin uses the full range of these institutions and methods to achieve his two highest strategic priorities without having to resort to full-scale war: (1) to weaken and destabilize the West, and (2) to bring the countries of the so-called near abroad closer into Russia's orbit (or at least prevent those countries from becoming closer to the West). The chapter begins with a discussion of definitions and history. It then places Russia's use of special forces in political-strategic context, that is: to what purposes does Putin put these tools? Next, the chapter provides the conceptual context for Russia's contemporary use of these kinds of methods and forces, relying principally on how Chief of the General Staff Valery Gerasimov has articulated Russian political and military leadership thinking on conflict and the role of unconventional forces. The chapter then illustrates how the Russians applied Gerasimov's ideas in Ukraine and Syria. In addition, we clarify which tools the Russians used for which missions and why. The chapter concludes with thoughts on the effectiveness of Russian use of special forces and the likelihood of success for similar efforts in the future.

What Is Spetsnaz?

The Russians have used the word *Spetsnaz* to refer to a variety of different units attached to intelligence, police, or military institutions and forces. The term itself is a portmanteau of the Russian words *spetsial'noe* and *naznacheniya*, meaning "special designation" or "special purpose." Spetsnaz units have no common or standard institutional home, uniform, insignia, training, or qualifications.[1] Forces calling themselves Spetsnaz are or have been attached to many military units, the Soviet Committee for State Security (KGB), its post-Soviet successor institutions—the Federal Security Service (FSB) and External Intelligence Service (or Foreign

i In this chapter, we use *Spetsnaz* to refer to only the various forces that call themselves by that name. We use "SSO" to refer to only that institution. We use "special forces," "special purpose forces," "unconventional tools," or "methods" to refer broadly to the full range of institutional means at Putin's disposal.

Intelligence Service; SVR)—the Main Directorate of the General Staff (GRU[ii]),[2] the Ministry of Interior (MVD) and other police units, the Russian Airborne Forces, the Special Operations Forces (SSO),[iii] and other institutions.[iv]

Beyond the application of the term, another source of confusion is that Spetsnaz missions are quite broad and have included raids and sabotage, assassination, special reconnaissance, intelligence collection, combating adversary special operations forces (SOF), subversion, psychological operations, military assistance, support for Russia's conventional forces, search-and-rescue operations, and peace support operations.[3] Of greatest interest in this book are the strategic covert actions—including those of Spetsnaz—that give the Russian government plausible deniability for visible actions for which it wishes to avoid responsibility (and wants to attribute to others),[v] as exemplified by the Russian shadow invasion of Ukraine, which included the seizure of Crimea, the attack on the Donetsk Basin (Donbas or Donbass), and the various destabilization efforts against the Kiev government.[4]

History of Spetsnaz

While much of the recent attention has been on Russian Spetsnaz pretending to be Ukrainian "self-defense irregulars" (the famous "little green men") in Crimea and the Donbas, these types of covert use of forces for sabotage, assassination, misdirection, and reconnaissance are not new.[vi] The Bolsheviks used concealed or misattributed forces during the Russian Civil War. The Soviets employed partisans and long-range special-mission teams during World War II and planned to use them during any war with NATO.[5] Special forces also supported and trained pro-Soviet forces against anti-Soviet governments and factions in the Soviet sphere and the developing world.[6] Other previous uses include the preservation of the Soviet regime and support to pro-Soviet forces in North Korea, East Germany, Hungary, Cuba, Czechoslovakia, and Afghanistan and throughout Africa.[7] After the collapse of the

ii Although the GRU became the GU in 2010, for purposes of consistency, the authors use the term GRU throughout the remainder of the chapter.

iii For the sake of readability, we have listed translations of institutional names in the text for the following transliterated Russian names: Komitet Gosudarstvennoy Bezopasnosti (KGB), Federalnaya Sluzhba Bezopasnosti (FSB), Sluzhba Vneshney Razvedki (SVR), Glavnoye Razvedyvatelnoye Upravlenie (GRU), and Sil Spetsialnykh Operatsiy (SSO).

iv For varieties of Spetsnaz and difference between Spetsnaz and other forces, see Fainberg, "Russian Spetsnaz," 8-9; and Atay, "Strategic Utility of the Russian Spetsnaz," Naval Postgraduate School, master's thesis, December 2016, p. 52. Atay relies significantly on Mark Galeotti and Johnny Shumate, *Spetsnaz: Russia's Special Forces (Elite).* Ed. Martin Windrow. Oxford: Osprey, 2015, 206.

v Note: briefly, "plausible deniability" allows individuals in an organization to deny either responsibility for or knowledge of damnable actions based on a lack of evidence that confirms their participation. While covert action has public results but obscures the responsible actors, clandestine action like espionage conceals even the fact of the action or result, most notably the theft of protected information. See also Bennets, "Putin Rules Deaths of Russian Troops in 'Special Operations' a State Secret," 2015.

vi On the use of assassination in Russian and Soviet history, see Amy Knight, *Orders to Kill: The Putin Regime and Political Murder.* New York: Thomas Dunne Books, 2017, 11-30. See also Sukhankin, "Russian State's Use of Irregular Forces," 2019.

Soviet Union, and before its involvement in Ukraine, Spetsnaz played roles in the First and Second Chechen Wars and in Georgia.[8]

Political-Strategic Context and Purpose of Russian Special Forces

Because of the varied range of strategic and foreign policy purposes of Russian special forces, we focus on Putin's highest priorities: to bring the former Soviet constituent states closer into Moscow's orbit and to weaken NATO and the United States. Putin defines Russian and Western interests as zero sum: that which is bad for the West is good for Russia, and vice versa.[vii] Key to serving that interest is weakening ties between the West and Putin's closest neighbors, such as Ukraine, whose legitimacy and independence from Russia Putin has never accepted.[viii] (It is worth noting Putin assigned primacy for "near abroad" special operations to the FSB, Russia's internal security service, and not the SVR, the external intelligence service. From this assignment, one could infer how much respect Putin gives to the independence and sovereignty of those countries).

Putin openly directs much of his foreign policy toward weakening ties between the near abroad and the West and preventing former Soviet constituents from moving closer to the West, a goal he has pursued most vigorously in Ukraine, Belarus, Latvia, Lithuania, Estonia, Georgia, and Kyrgyzstan. In short, Putin believes that if the former Soviet states cannot be returned to Moscow's control, then, at least, they will be denied the independence and capability to choose to align with or cooperate meaningfully with the United States. As of yet, Putin has not decided to pursue that policy through full-scale conventional warfare (although the war with Ukraine is open, partly conventional and undeniably Russian, if not a full-scale war). Instead, Putin has relied on limited war, subversion, deception, local proxies, information warfare, misdirection, and distraction.

Conceptual Foundations: General Valery Gerasimov's Views of Modern Conflict

Valery Gerasimov, Russia's chief of the General Staff and deputy minister of defense, has provided the modern intellectual framework undergirding the current Russian approach to conflict. Some controversy exists as to whether the model Gerasimov described and advocated rises to the specificity and coherence of doctrine. Gerasimov did not reveal anything particularly new in his concepts, except perhaps the inclusion of the latest technologies and institutions. The blurred distinctions between war and peace, the use of deception, and the preference to achieve a political goal without

vii See US ambassador Michael McFaul's report of his conversation with Russian first deputy prime minister in fall 2013 regarding Ukraine. McFaul, *From Cold War to Hot Peace: An American Ambassador in Putin's Russia*. Boston: Houghton Mifflin Harcourt, 2018, 395. There is a domestic political component to this policy; Putin needs an external threat to justify his dictatorship.

viii A useful discussion of Putin's views about Ukraine can be found in Myers, *The New Tsar*, 462-480. See also Gerard Toal, *Near Abroad: Putin, the West, and the Contest over Ukraine and the Caucasus*. New York: Oxford University Press, 2017, 237-273 and Steven Lee Myers and Ellen Barry, "Putin Reclaims Crimea for Russia and Bitterly Denounces the West," *New York Times*, March 19, 2014, https://www.nytimes.com/2014/03/19/world/europe/ukrainehtml.

fighting existed in Sun Tzu's time. Still, Gerasimov articulated a set of preferences for the use of some tools and techniques over others, and his position as chief of the General Staff makes his preferences worthy of attention. His views also merit consideration because Russian actions in Ukraine, Syria, and elsewhere have hewed closely to what he described. Furthermore, both Gerasimov's articulation and recent Russian action have implications for other countries in the near abroad where Putin feels a sense of grievance, insecurity, and threat.

Gerasimov has spoken and written widely, but no one message garnered as much attention as a 2013 article published in the *Voyenno-Promyshlenniy Kuryer* (Military-Industrial Courier).[9] The article is short and general but, in retrospect, seems to explain what the Kremlin executed in Ukraine the following year. Gerasimov's main points follow:

- There is no clear distinction between states of war and peace.
- War cannot be regarded as solely military.
- Success will depend on the deployment of mixed, asymmetrical forces operating in a single information and intelligence space.
- This method of war will erase existing differences among tactical, operational, and strategic forces; toward that end, one focus should be neutralizing the enemy using special operations forces and internal opposition "to establish a permanent front throughout the opposing state."
- Many of the measures employed will be hidden; "The open use of force is often limited . . . under the guise of peacekeeping and crisis resolution only at some stage, mainly to achieve ultimate success in the conflict."
- Many of the measures will rely on the "protest potential of the [local] population."
- Russia will apply the lesson from its experiences in Georgia, Afghanistan, and World War II.

How exactly all this would unfold in an actual conflict depends on a number of factors. The following sequence from Gerasimov's concept of hybrid warfare[10] largely resembles what happened in Ukraine, and can be used to judge the extent to which Russian political-strategic theory is reflected by its praxis:

- Covert origins: The initial phase in which political opposition and resistance in the form of political parties and other groups are formed against the opposing regime. This phase includes a comprehensive information warfare campaign to shape the environment toward a Russian purpose, with employment of strategic deterrence. Potential for miltary activity emerges in this phase.

- Escalation: In this second phase, political and military leaders become aware of the developing conflict. Russia exerts political and economic pressure on the targeted regime, including economic sanctions and the suspension of diplomatic relations.
- Start of conflict: The third phase starts with hostile acts such as demonstrations, sabotage, assassinations, and paramilitary engagements. Russia then begins deployment of its forces toward the region.
- Crisis: Russia commences military operations alongside a persistent information campaign in order to change public opinion in favor of Russian intervention.
- Resolution: This stage focuses on the best paths to resolve the conflict with change of leadership in the state or region in which the conflict took place. The goal is to reset the political, military, and economic situation to return to peace and order.
- Restoration of Peace: The final stage involves Russian attempts to reduce tensions and conduct peacekeeping operations. This protracted phase includes diplomatic and political measures required to establish a postconflict settlement that addresses the original causes of conflict.

Russian Strategy in Ukraine

Just as Putin denies the legitimacy of an independent Ukraine, he also threatens the independence of three NATO member states: Latvia, Lithuania, and Estonia.[ix] Therefore, the West must understand the thinking underpinning Russian goals and methods—as well as their results—in Ukraine. While the conflict in Ukraine has not unfolded in exactly the sequence laid out above, Gerasimov's model helps us to understand Russian strategic thinking.

Ideally, as Gerasimov argued, the tools used in the first stage or stages of a conflict could achieve the state's strategic goals instead of facilitating further escalation. The events in Ukraine in the run-up to February 27, 2014[x] illustrate what these first stages look like in a practical sense. In 2013-2014 in Ukraine, Russia's nearest-term goal was to prevent Ukraine from signing a European Union Association Agreement. By that point, Russia had already employed a variety of covert and overt means—including information warfare, political and economic sanctions, and likely attempted assassination—to keep Ukraine in the fold. However, once the Maidan protests started on November 21, 2013, subsequently forcing the pro-Russian

ix On Putin's views of Ukraine and the Baltics, see Myers, 466-467. See also R. D. Hooker Jr., "How to Defend the Baltic States," *Jamestown Foundation,* October 17, 2019, https://jamestown.org/product/how-to-defend-the-baltic-states. Putin and his lieutenants have been quoted repeatedly claiming a right to defend Russians anywhere, most frequently mentioning Ukraine and the Baltics.

x Officials dispute precisely when Russian forces arrived, but most reports list this date.

Ukrainian prime minister Viktor Yanukovych from power, Putin decided he had to resort to military use, though covertly at first. Had Yanukovych managed to stay in power, Russia could have achieved its goal without ever resorting to additional military measures.

Putin famously described the collapse of the Soviet Union as the greatest tragedy of the twentieth century. He first made that comment in 2005, and in 2018 added he would reverse the collapse of the Soviet Union if he could.[xi] Ukraine was the second largest constituent Soviet republic at the time of the collapse, and had been the jewel in the crown of the Russian empire. Putin found intolerable the possibility that Ukraine would align itself with the United States, NATO, and the European Union.[11] In the Russian view, the overthrow of Yanukovych and election of a pro-Western government required some kind of countervailing action. However, for both domestic and foreign policy reasons, Putin was not willing to risk a wider war. He wanted to achieve his goals for the least amount of blood and treasure. Moreover, a narrative in which the Ukrainians themselves opposed a strategic realignment and chose Russia over the West served Putin's domestic and foreign policy goals (in part because of Putin's claims the Russians and Ukrainians are one people).

On February 27, 2014, several hundred members of the 45th Spetsnaz regiment helped establish what Russia media called a "popular uprising." The Spetsnaz forces seized key road intersections and facilitated a larger Russian military intervention.[12] Russia used enough deception to cause confusion and provide some degree of plausible deniability, at least initially. While most observers strongly suspected the Russian hand, the Kremlin made an effort to attribute the action to local Russian-speaking Ukrainians, who constituted the majority in Crimea and Donbas. The Russian troops wore no insignias and claimed to be local self-defense forces. However, the assertion these "little green men" were local could not withstand scrutiny. The forces were armed with new, modern 7.62 mm PKP machine guns and wore new camouflage combat uniforms, tactical vests, and composite helmets. Not even regular Ukrainian military units, let alone local militia, carried such up-to-date weapons and equipment. Many of the Spetsnaz also spoke Russian in nonlocal accents and were obviously not Ukrainian. Despite these inconsistencies, Putin and other senior Russian officials denied the presence of Russian forces in Crimea until mid-April 2014, almost two months after the first deployments.

The fighting in Donbas that began in March 2014 followed a similar pattern of deception, denial, and confusion as in Crimea. One Reuters correspondent reported seeing dozens of heavily armed men with Russian accents set up a roadblock 10 kilometers from the Russian border. Wearing white arm bands and no identifying insignia, they were referred to in a BBC report as a "Ghost Army." Spetsnaz led the initial armed action, and after establishing control of key junctions and facilities,

xi Putin made the first comment in 2005 and the second in 2018. Adam Taylor, "Putin Says He Wishes the Soviet Union Had Not Collapsed: Many Russians Agree." *Washington Post,* March 3, 2018. https://www.washingtonpost.com/news/worldviews/wp/2018/03/03/putin-says-he-wishes-he-could-change-the-collapse-of-the-soviet-union-many-russians-agree/

prepared the way for a larger, more conventional force. By the end of 2017, the Organization for Security and Cooperation in Europe (OSCE) observer mission counted about 30,000 military personnel crossing from Russia to Donbas at the two border checkpoints it was allowed to monitor.[13] Again, Russia started with information operations and followed with special purpose forces pretending to be locals. In Donbas, Russia did not formally annex the territory it controlled and, thus, did not have to acknowledge the presence of its forces. Russia continues to insist it has no forces in the Donbas, and that all the antigovernment forces in the area are local residents.

Russian Strategy in Syria

While it does not hold the same strategic importance for Russia as Ukraine does, Syria has been a long-term, reliable ally, and the port of Tartus is the site of both a Russian navy base and Russia's foremost signals' collection platform in the Mediterranean and Middle East. Furthermore, in Putin's zero-sum worldview, any adversary of the United States is a friend of Russia. Therefore, supporting Bashar al-Assad was in Russia's interest. It is unclear when Russia first became involved in the Syrian revolution; however, Spetsnaz forces have been training and assisting Syrian forces since at least July 2015.[14] However, Spetznaz was neither the only or arguably most significant Russian actor in Syria. Others included SSO, Zaslon,[15] various contractors, the air force, and the GRU, FSB, and SVR in their larger capacities.

Direct-action forces (analagous to top-tier US direct-action operators), SSO played a particularly key role in Syria. The SSO reports to the Komandovaniye Spetsialnykh Operatsiy (KSO; established in 2010), Russia's special operations command, analogous to US JSOC.[16] Unlike Spetsnaz forces, which have broad and varied training, and distinguished from other forces by their purpose, SSO are all highly trained, volunteer troops. (In contrast, Spetsnaz forces sometimes still rely on conscripts to fill their ranks.) SSO operatives focus on three main areas of Russia's strategic deterrence: counterterrorism, special operations in martime affairs, and special operations abroad.

SSO's involvement in Syria focused on the "strategy of limited actions"[17] to employ the full spectrum of military power on behalf of Russian interests. SSO fought alongside Syrian troops, ambushing behind lines and attacking critical communication facilities. SSO actions were critical in enabling President al-Assad's military to advance in many areas of the country. For example, in March 2016, Russia's elite forces helped liberate Palmyra from the Islamic State after weeks of Russian airstrikes and close-quarter fighting.[18] Because of Palmyra's strategic location in central Syria, the battle represented a decisive victory for the Syrian government.

Different Tools for Different Missions

In Crimea, Donbas, and Syria, events unfolded in ways Gerasimov described. In each case, the Kremlin relied on a variety of different tools matched to the different strategic requirements and conditions. Because Russia intended from the beginning

to annex Crimea—an open and formal act—it needed to employ misattribution only until it could move sufficient forces into Crimea to seize control of key transportation, communication, military, and political facilities. Just as Gerasimov described, in the first stages of the conflict, covert methods and forces enabled subsquent overt conventional forces.

Russia had a different goal in Donbas, which required diffent methods and, therefore, different tools. In Donbas, Russia sought to weaken the legitimacy of the anti-Russian, pro-Western government in Kiev by showing how the Ukrainian people did not support their own government. Achieving the goal required an actual invasion by large numbers of regular Russian troops, but Russia has never given up the fiction that the conflict is among Ukrainian factions only. In this case, almost every facet and stage of Gerasimov's model entered into play, from the most covert methods to massive employment of conventional forces, including advanced air and antiair power. Russian actions in Crimea and Ukraine differed from its actions in Syria, where Russia relied less on information operations (which Syrians largely handled) and more on the SSO and air power to achieve its goals.

Russia's Special Operations Tools and Methods

The special operations tools and methods Russia has employed have depended on particular mission goals and situations. Organizations, missions, and methods have overlapped, and Russian leaders often have applied different instruments—opportunistically, haphazardly, and simultaneously—for the same mission. Let us first consider Russia's three primary intelligence services—GRU, FSB, and SVR—before examining other operators Russia has employed.

The GRU is Russia's military intelligence agency. In the Soviet era, the GRU provided intelligence to the military and the government. The GRU reports directly to the chief of the General Staff, Gerasimov (who also controls 25,000 Spetsnaz forces across all branches of the military[19]), and plays a critical role in cyber warfare. The GRU's Unit 22951 appears to be the organization responsible for carrying out foreign assassinations and assassination attempts, such as that of former Russian intelligence officer Sergey Skripal in the United Kingdom in 2018.[20] Further, the GRU intervened in the 2016 US presidential election. When most people talk about Spetsnaz, they refer to units within the GRU. The GRU Spetsnaz formed in 1949, disbanded in 2010, and was reconstituted in 2013.

The GRU's missions overlap principally with those of the FSB and the SVR. The FSB has two primary roles—counteresponiage and counterterrorism[21]—but also bears responsibility for border security (and border troops), the coast guard, and information security. Most significantly for the case of Ukraine, President Putin, a former KGB officer and former head of the FSB, granted the FSB greater authority to carry out operations abroad, particularly in the countries of the former Soviet Union. (Putin, who famously served a tour in East Germany before the collapse of the Soviet Union, spent the bulk of his KGB career working domestically against internal dissent, an FSB task).

The SVR inherited the KGB's foreign intelligence role, collecting mostly civilian strategic intelligence. However, SVR missions overlap with the FSB in the areas bordering Russia and the GRU, which also collects foreign political, scientific, and technical intelligence of interest to the Russian military.[22] Each of these institutions have Spetsnaz of their own, but each also plays a role in advancing Putin's geopolitical strategy independent of any use of forces called Spetsnaz.

Other tools include the Internet Research Agency (IRA), various contractors,[23] even soccer hooligans, volunteer associations, businesses, and a pro-Putin motorcycle gang known as the Night Wolves. Per the concept Gerasimov outlined, these institutions and groups can act in different combinations at different points to achieve Russian ends.

To support unrest, protests, and influence operations, the Kremlin used several proxy forces to advance Putin's political objectives. The Kremlin has also used right-wing training camps,motorcycle gangs, and neo-Nazi soccer hooligans to influence operations in Western countries. For example, in Slovakia, retired Russian Spetsnaz soldiers trained young men from a right-wing paramilitary group to create disturbances.[24] Russia also used the Night Wolves gang as a proxy group in Slovakia to promote Russian sympathies; the gang drove en masse to a Soviet War memorial and laid red carnations in front of the memorial.[25] In France, authorities detained the leader of the Russian Union of Supporters (a soccer fan club) reportedly under FSB guidance to foment disorder at EURO 2016 soccer matches.[26] As Putin's intelligence services lure angry young men into their sphere of influence and radicalize skinhead nationalists to provoke protests, Moscow advances its goals of destablizing Western societies.[27]

Russia has also employed fake social media accounts and internet trolls to motivate political action and stir unrest, most famously, but not exclusively, in the 2016 US presidential election. Elements of both the GRU and the Internet Research Agency (IRA) were linked to these efforts.[28]

Putin tries to set Russia apart by defending what he considers "traditional" values against Western liberal values.[29] He uses this self-appointed role to sow internal division among his adversaries, most famously in Ukraine and in the United States during the 2016 election, but also throughout the West. The various groups and institutions constituting the Kremlin's strategic information toolbox therefore promote anti-immigrant, antifeminist, anti-LGBTQ, and nationalistic rhetoric. Russia's attempts to erode the legitimacy of democratic institutions are intended to strengthen Russian claims that Western (i.e., NATO) democracies are not morally superior to the Russian or other authoritarian forms of government.[30] Russian intelligence services and other pro-Kremlin groups fuel such culture wars, paving the way for the active measures Gerasimov outlines . In this way, Russia integrates its multifaceted special forces units (broadly and inclusively defined) into a strategy that extends from peacetime influence operations to hybrid war and even strategic signaling.

Implications

Russia has integrated the full range of its covert and special purpose capabilities into its overall national security strategy. As General Gerasimov made clear, the Russian conception of conflict denies any meaningful distinction between peace and war; therefore, Moscow considers itself free to use all its capabilities at any time to achieve Russian goals. Putin's agenda focuses on bringing former Soviet states into Moscow's orbit, or at least denying those countries the opportunities for close economic integration and security cooperation with the West.

Russian special purpose forces (including Spetsnaz), one of the tools at Putin's disposal, helped enable Russia to gain control of Crimea and integrate it politically into the Russian Federation and to seize large areas of eastern Ukraine and maintain a force that destabilizes the rest of Ukraine. Russia's involvement in Syria served as a test case for its influence in the developing world and provided an opportunity to weaken the West. It also provided a test case for Russia's use of contractors, the SSO, and air-ground coordination as elements of its strategic political strategy. Furthermore, Russian's experience in Syria demonstrated that relatively small investments could yield large dividends: Russian special forces and air power likely kept Bashar al-Assad in power. Russia's continuing special operations information war on the United States, the United Kingdom, France, Germany, and other NATO allies serves to divide these countries both internally and from one another. The aftermath of the 2016 election attack in the United States and inteference in the Brexit referendum in the United Kingdom illustrate clearly the effectiveness of the Russian effort.[31]

As impressive as Russia's accomplishments have been in Ukraine, Crimea, the United States, and the United Kingdom, much of what Russia has achieved depends on factors that may not be replicable against targets such as Estonia, Latvia, and Lithuania. First, Russian success in Ukraine came against an unprepared, divided, and weak adversary. While the Baltic states are no match for Russia militarily, they are much more politically developed and united than Ukraine. More significant, they are NATO members. Article V of the North Atlantic Treaty commits NATO member to defend one another when attacked militarily, a provision that likely would compel Putin to think twice before undertaking any attributable hostile act against Estonia, Latvia, or Lithuania. Second, Russia's intervention in Ukraine provided lessons for Baltic states, allowing them to prepare appropriately. Third, while each of the three Baltic states has significant Russian populations, those populations are both economically stronger than their Russian Federation compatriots (which was not true of Ukraine) and more geographically dispersed than in Ukraine. (The fact that Ukraine is split regionally into a pro-Russian east and pro-Western west aided Russia's objectives). These conditions make the Baltics less susceptible to the kinds of operations Russia carried out successfully in Ukraine, though they do immunize them from constant information operations, cyberattacks, and other covert attacks.

Russia's success in Syria also will not be easy to replicate. First, while many developing countries deal with conflict and instability, few offer Putin the advantages

he had in Syria: a longtime Russian ally, an existing naval base and port, and relatively easy lines of transport. Second, Russia might not be financially strong enough to engage in multiple adventures in the developing world. Moreover, combat means dead soldiers, and Putin has shown himself apprehensive about the domestic political risks of the deaths of Russian soldiers.[32]

Finally, the West was slow to recognize and react to the threat and damage of Russian cyberattacks and information operations, which have proven to be costly and stunningly divisive. However, Russia cannot count on a delayed response from the West in the future. In short, Russia's successful efforts against Ukraine, al-Assad's opposition in Syria, the United Kingdom's Brexit debate, and the 2016 US presidential election might be short-lived, as Russian adversaries decide to react more aggressively and effectively.

Endnotes

1 Polek, Matthew J., "Evolution of Spetsnaz and Operations with Russian Special Forces, *Military Intelligence Professional Bulletin*, v. 43, no. 4, October 1, 2017.

2 See, for example, Andrey Soldatov and Irina Borogan, *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB*. New York: Public Affairs 2010, 159.

3 Bukkvoll, Tor, "Military Innovation Under Authoritarian Government: The Case of Russian Special Operations Forces," *Journal of Strategic Studies* 38, no. 5 (July 29, 2015): 602–8, https://doi.org/10.1080/01402390.2015.1056342.

4 Kramer, Andrew E., "G.R.U., Russian Spy Agency Cited by Mueller, Casts a Long Shadow," 2018/07/13 https://www.nytimes.com/2018/07/13/world/europe/what-is-russian-gru.html.

5 Sukhankin, Sergey, "The Russian State's Use of Irregular Forces and Private Military Groups: From Ivan the Terrible to Soviet Period," *Jamestown Foundation*, April 12, 2019, https://jamestown.org/program/the-russian-states-use-of-irregular-forces-and-private-military-groups-from-ivan-the-terrible-to-the-soviet-period/.

6 Sukhankin, "Russian State's Use of Irregular Forces," *Jamestown Foundation,* April 12, 2019; MacFarlane, S. Neil, *Superpower Rivalry and Third World Radicalism: The Idea of National Liberation* (Baltimore: The Johns Hopkins University Press, 1985.

7 Mark Galeotti, "The Rising Influence of Russian Special Forces," *IHS Jane's Intelligence Review*, 2004, 1–2, https://www.janes.com/images/assets/299/46299/The_rising_influence_of_Russian_special_forces.pdf.

8 Atay, Abdullah. "Strategic Utility of the Russian Spetsnaz," Naval Postgraduate School, master's thesis, December 2016, pp. 50-54.

9 Gerasimov, Valery, "*Geopolitika," Voyenno-Promyshlenniy Kuryer*, No. 8 (476) 27 *Fevralya*—5 *Marta* 2013 goda, s. 2.

10 See "Land Warfare in Ukraine: Modern Battlefield of Europe, FIN ABEL, European Army Interoperability Center, May 2019.

11 Myers, Steven Lee, *The New Tsar: The Rise and Reign of Vladimir Putin*. New York: Knopf, 2015, 462-480.

12 US Department of Defense, "Little Green Men: Modern Russian Unconventional Warfare, Ukraine 2013 2014." United States Army Special Operations Command, n.d. https://www.jhuapl.edu/Content/documents/ARIS_LittleGreenMen.pdf., 53–55.

13 DOD, "Little Green Men," 53–55.

14 Fainberg, Sarah, "Russian Spetsnaz, Contractors and Volunteers in the Syrian Conflict," December 2017, Russie.Nei. Visions, No. 105, 2-8, https://www.ifri.org/sites/default/files/atoms/files/fainberg_russian_spetsnaz_syrian_conflict_2017.pdf.

15 Thomas Gibbons-Neff, "How Russian Special Forces Are Shaping the Fight in Syria." *Washington Post*, March 29, 2016.

16 "Russia's Special Operations Forces Command and the Strategy of Limited Actions," *RealClearDefense*, 2, accessed October 7, 2019, https://www.realcleardefense.com/articles/2019/05/22/russias_special_operations_forces_command_and_the_strategy_of_limited_actions_114447.html.

17 "Russia's Special Operations Forces," *RealClearDefense*, 2.

18 Gibbons-Neff, "How Russian Special Forces Are Shaping the Fight in Syria," 2016.

19 Smith, Ben. "Russian Intelligence Services and Special Forces," December 4, 2018, 9, https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-8430. "Russian Intelligence, 5–8.

20 US Department of Justice, *The Mueller Report: The Final Report of the Special Counsel into Donald Trump, Russia, and Collusion*. New York: Skyhorse Publishing, 2019, 52-75; Michael Schwirtz, "How a Poisoning in Bulgaria Exposed Russian Assassins in Europe," https://nytimes.com/20191/2/22/world/europe/bulgaria-russia-assassination-squad.html; Kramer, "G.R.U., Russian Spy Agency Cited by Mueller, Casts a Long Shadow," 2018/07/13, https://www.nytimes.com/2018/07/13/world/europe/what-is-russian-gru.

21 Smith, "Russian Intelligence Services and Special Forces," 3–8.

22 Smith, "Russian Intelligence Services and Special Forces," 5.

23 Gibbons-Neff, Thomas, "How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria," *New York Times,* May 24, 2018, https://www.nytimes.com/2018/05/24/world/middleeast/american-commandos-russian-mercenaries-syria.html.

24 Carpenter, Michael, "Russia Is Co-Opting Angry Young Men," *The Atlantic*, August 29, 2018, 1, https://www.theatlantic.com/ideas/archive/2018/08/russia-is-co-opting-angry-young-men/568741/.

25 Orenstein, Mitchell A., and Peter Kreko, "How Putin's Favorite Biker Gang Infiltrated NATO," October 15, 2018, 1–3, https://www.foreignaffairs.com/articles/russian-federation/2018-10-15/how-putins-favorite-biker-gang-infiltrated-nato.

26 "Russian Fan Leader Back in France," *BBC News*, June 20, 2016, sec. Europe, 1, https://www.bbc.com/news/world-europe-36579532.

27 Carpenter, "Russia Is Co-Opting Angry Young Men," 3.

28 DOJ, *The Mueller Report*, 52-75.

29 See Lionel Barber and Henry Foy, "Vladimir Putin: Liberalism Has Outlived its Purpose," Financial Times,

30 Barber and Foy, "Vladimir Putin: Liberalism"; Alina Polyakova, "Lessons from the Mueller Report on Russian Political Warfare," *Brookings* (blog), June 20, 2019, 1, https://www.brookings.edu/testimonies/lessons-from-the-mueller-report-on-russian-political-warfare/.

31 Department of Justice, *The Mueller Report*.

32 Bennets, Marc, "Putin Rules Deaths of Russian Troops in 'Special Operations' a State Secret." *Telegraph*, May 28, 2015. http://www.telegraph.co.uk/news/worldnews/europe/russia/11636160/Putin-rules-deaths-of-Russian-troops-in-special-operations-a-state-secret.html.

CHAPTER 7

Sharp Swords of the Future Battlefield: The Chinese Military's Special Forces and Psychological Operations

Elsa Kania and Peter Wood

The Chinese People's Liberation Army (PLA) is prioritizing innovation in the theories and capabilities for future warfare.[i] Building upon a long tradition of military science, the PLA is currently exploring the challenges and opportunities of what is seen as a new Revolution in Military Affairs (RMA).[ii] The PLA has concentrated on developing "new-quality" (新质力量) forces for future combat, including those tailored for special operations, cyber operations, and electronic countermeasures.[1] Meanwhile, the PLA continues to implement a reform agenda that may have far-reaching implications for its future capabilities. According to "China's National Defense in the New Era," "new types of combat forces have been enhanced to conduct special operations, all-dimensional offense and defense (立体攻防), amphibious operations, far seas protection, and strategic projection, aiming to make the force composition complete, combined, multifunctional, and flexible."[2]

The PLA seeks to advance its capabilities to undertake "integrated joint operations," characterized by "system of systems confrontation" (体系对抗).[3] The PLA also seeks to contest operational advantage in the course of the transformation in the form of warfare from today's informatized (信息化) warfare toward intelligentized (智能化) warfare, in which artificial intelligence, among other emerging technologies, will be critical to future operations.[4] As the PLA seeks to become a world-class military, these developments in its strategic thinking and military modernization merit continued analytic attention. In particular, the PLA has concentrated on certain emerging technologies that present the possibility of strategic latency, including unmanned systems and artificial intelligence that are expected to deliver a decisive advantage in future operations.[5]

Chinese military leaders appear to believe any new technology will be inevitably weaponized. This quotation by Friedrich Engels is routinely referenced: "Once technological advancements can be used for military purposes and have been used for military purposes, they very immediately and almost necessarily, often violating the commander's will, cause changes or even transformations in the styles of warfare."[6] The PLA's transformation will involve a paradigm change in its model of military power. Currently, the PLA is "striving to transform from a quantity-and-scale model to that of quality and efficiency, as well as from being personnel-intensive to one that is S&T-intensive," according to the 2019 defense white paper, "China's National Defense in

i This chapter draws upon Chinese-language resources. Translations are provided by the authors.

ii The PLA has adopted the concept and terminology of the RMA that became prominent in US debates and discourse.

the New Era."[7] This transition demands drastic changes to the Chinese military as an organization, including its training, force structure, and talent cultivation.

The PLA continues to be influenced by formative historical legacies, from its early experiences with guerrilla warfare to contemporary concerns about how to confront a more powerful adversary as a still weaker military. Indeed, the PLA's thinking on conflict has been shaped by Marxist concepts and Maoist antecedents, including the continued salience of "people's warfare" (人民战争) as a concept.[8] The PLA has concentrated on "military struggle" (军事斗争), involving "the use of military methods to advance struggle among nation-states to achieve a definite political or economic objective, of which the highest form is warfare."[9] The PLA's reforms have looked to advance the integration of peace and warfare (平战一体) in its force posture, planning, and operations.[10] The realization of this concept in practice has involved developing an command architecture to mobilize rapidly for potential conflict scenarios and to operate across that spectrum between peace and warfare.[11] PLA strategists often argue those boundaries in conflict are blurring as an inherent feature of modern conflict.[iii][12] In the process, the PLA has been studying and intends to leverage lessons learned from recent Russian and American operations. Chinese military scholars and strategists are exploring concepts of hybrid warfare, proxy warfare, and asymmetric operations, intending to adapt these concepts to its own purposes.[13]

Historical Experiences and Influences

Certain elements of "hybrid" or unconventional warfare are already well-established within the traditions of Chinese military thinking. In fact, as victors of a multidecade insurgency, the principles of guerrilla warfare (游击战) arguably constitute integral elements of the intellectual DNA of the Chinese Communist Party (CCP) and its armed wing, the PLA.[14] It is important to be careful in distinguishing the origins of Chinese strategy relative to its intended operational employment.[iv] The PLA's contemporary understanding of "hybrid warfare" builds upon its study of antecedents in American and Russian thinking.[15] Initially, the Red Army, which was the predecessor to the PLA before 1945, had its defining experiences first as a failed urban insurgency that then pivoted to contest rural areas. "Our Party united the people and led them in embarking on the right revolutionary path, using rural areas to encircle the cities and seizing state power with military force," as that history is described in a contemporary recounting.[16] The Red Army engaged in insurgency against the Imperial Japanese Army and then concentrated on defeating the KMT's National Revolutionary Army.[17] The

iii Major General Ye Zheng, a leading PLA thinker on information warfare, has declared, "The strategic game in cyberspace is not limited by space and time, does not differentiate between peacetime and wartime, [and] does not have a front line and home-front." See: Kania, "A Force for Cyber Anarchy or Cyber Order? PLA Perspectives on 'Cyber Rules,'" *China Brief*, Jamestown Foundation, July 6, 2016, https://jamestown.org/program/a-force-for-cyber-anarchy-or-cyber-order-pla-perspectives-on-cyber-rules/.

iv For instance, the example of the "String of Pearls" strategy is illustrative, a label first applied to an emergent pattern of activity by American consultants, then translated into Chinese and reinjected to American discourse as if it were a wholly Chinese concept.

Red Army survived numerous encirclement campaigns by the governing Nationalist Party (also known as the *Kuomintang*, KMT), emerging after World War II to engage in conventional large-scale battles.

The PLA's earliest familiarity with unconventional warfare can be traced back to its roots in the Nanchang Uprising of 1927.[18] The CCP's "Long March" is sometimes described as having involved the use of special operations undertaken by the Red Army.[19] However, special forces in the modern sense can more directly be traced to the latter stages of the Chinese Civil War. At that time, the Soviet Union appears to have provided training to small groups of PLA soldiers, and specialized reconnaissance teams later played a role in attacks on KMT forces.[20] During the PLA's 1949 invasion of Xinjiang, Soviet aid provided significant contributions.[21] The PLA later targeted KMT-held offshore islands through the use of "frogmen" from its earliest amphibious reconnaissance units in the 1950s.[22]

China had to remain alert for insertion of KMT special forces throughout the 1950s and 1960s, while encountering hybrid conflicts involving the US-trained Tibetan guerrilla groups and as well as KMT forces operating from border areas of Burma (now Myanmar).[23] During the Vietnam War, China sent advisors and even entire air defense units to North Vietnam.[24] In China's 1979 conflict with Vietnam, certain evidence suggests specialized reconnaissance units operated behind enemy lines, continuing during the subsequent decade of minor border skirmishes.[25] The PLA adapted a hybrid approach by combining conventional and unconventional operations, including during its operations in Manchuria.[26]

The PLA relied heavily on intelligence gathering, first to survive and later in its fight with the KMT, throughout its initial operational experience. In the process, political and psychological warfare also played important roles in convincing enemy units to defect en masse, an incident that has taken on a certain mythology in the decades subsequent but has its roots in real historic events. The success of such subversion contributed to the creation of the then-nascent PLA Navy and Air Force.[27] During the Huaihai Campaign, the party and its army also launched a political offensive, seeking to mobilize an uprising among KMT forces.[28] According to claims in official Chinese military media, the success of this "enemy force work" (敌军工作) resulted in a total of 1.89 million defecting from the KMT, including 1,400 generals.[29] The PLA's continuing concentration on "disintegrating the enemy military" (瓦解敌军) can be traced back to lessons learned from these formative experiences.

The modern manifestations of these legacies can be seen in the PLA's evolving approach to special operations and psychological operations. While Chinese military thinkers have argued, famously, for "unrestricted warfare," capturing the imagination of American audiences,[v] the PLA already possesses established mechanisms and formal organizations to carry out nonkinetic operations in peacetime and war.[30]

v This book has received attention that is disproportionate to its actual influence or authoritativeness, as the frequency of its citation attests. Liang Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House Arts, 1999.

As Chinese military leaders and strategists look at a future conflict scenario, the PLA likely would be prepared to undertake attacks that would be targeted against Taiwan and the United States in particular. At the same time, the PRC is unique in the extent of its investments in building up its capacity to leverage whole-of-society capabilities, including extensive employment of reserves and militias through national defense mobilization.

The Sharpest of Swords

Chinese special forces have expanded significantly since their first units were officially established in the 1990s after the Gulf War. The available estimates of their size range from 7,000 to 14,000.[31] Chinese strategists have paid close attention to other countries' employment of special forces, particularly to British operations in the Falklands War.[32] These observations likely helped motivate and influenced the PLA's creation of its initial SOF units. Today, Chinese special forces units are expanding across all services, possessing a range of functions, missions, and training.[33] At least three of China's military services have brigade-or-larger size SOF contingents, and the PLA Rocket Force is believed to have a battalion-level unit. The People's Armed Policy (PAP), a paramilitary organization that is increasingly militarized and newly commanded by the Central Military Commission, has also established special forces in Xinjiang, the "Mountain Eagle" commandos, which are expanding as the PLA's concern with terrorism intensifies.[34] Looking forward, the PLA is exploring ways to increase joint special operations.[35]

Within the PLA ground forces exist multiple units dedicated to special operations across most of the group armies. These units appear to be expanding in their size and increasing the rigor and realism of their training. For instance, in 2018, the PLA Army organized the "Qingbing" (奇兵) series of "new-type force" competitions that have tested their skills in reconnaissance and intelligence, special operations, information security/assurance, electronic countermeasures, and army aviation.[36] The PLA Army's special operations units have concentrated on counterterrorism operations intended to increase actual combat capability, leveraging support from intelligence and reconnaissance and employing electronic countermeasures.[37]

The PLA Army's reforms have increased the proportion of new-type combat forces, including special operations within its overall force structure. "If long-range fires are the army's elongating fist, then the special forces are the daggers that the army inserts into the enemy's heart," claims one commentary in state media.[38] The PLA Army's special forces have engaged in counterterrorism drills in Xinjiang, which involved drones, employed multisource information fusion processing, and detected targets based on electronic and optical reconnaissance, as well as radar decection.[39] In 2018, the PLA Army organized the first "Special Warfare 2018" (特战奇兵—2018) contest in Guilin, testing their tactical proficiency, involving assault and snipers.[40] The exercise "tested all levels of command," involving special forces skills and command capabilities.[41] In 2019, this competition was again convened to focus on

the assessment of special warfare capabilities. The increase in the proportion of the personnel who were selected randomly marked a shift to "mass troop training and preparation" as its focus.[42]

Since the reforms, the PLA Navy has expanded its marine corps, including the PLAN Marines brigade of special operations forces (SOF), which appears to be a priority for expansion. The PLA Marines brigade could be involved prominently in operations against Taiwan, including seizing offshore islands, while disabling the Republic of China (ROC) artillery on Kinmen, Matsu, and other outlying islands.[43] The PLAN Marines recent addition of an aviation brigade will support this special operations capability to become more expeditionary.[44] The PLAN Marine Corps has been expanded dramatically, demonstrating the PLA's interest and increasing capabilities for expeditionary operations.

Pursuant to these reforms, it appeared there would be at least one brigade per fleet, potentially ultimately amounting to seven brigades of over 30,000 personnel in total by 2020. Sea Dragon's elite Jiaolong Assault Team, which is featured in the movie *Operation Red Sea* (2018),[45] has trained to conduct airborne, surface, and underwater infiltration missions.[46] As Chinese overseas interests have expanded worldwide, evidently so has the imperative to create the capabilities to defend them.

The PLA Air Force Airborne Corps also includes a SOF brigade, which could serve as pathfinders for the main force in a conflict scenario. Potentially, these units would undertake a role in fomenting active measures and undertaking the assassination of key leaders in a scenario of conflict with Taiwan. PLAAF airborne troops have trained to engage in airborne assaults, air assaults, special operations, and supporting operations. For instance, the "Central-2019" (中部-2019) joint exercise, involves the use of airborne troops, who were integrated into joint operations, starting with airdrops.[47] This SOF brigade is described as primarily preparing for "special penetration operations, including killing key figures of the enemy and destroying the enemy's command, control, reconnaissance and communication facilities."[48] The Thor Commandos unit, created in 2011, is described as "the most special of the special forces," capable of "giving the enemy a deadly blow at key junctures and critical moments."[49]

The PLA Rocket Force has also established its own special operations units. The PLARF has leveraged special forces units to guard DF-16 units.[50] The PLARF's "Sky Sword" (Tianjian) exercises have introduced new-type blue forces that create more demanding conditions on the battlefield, including strikes from special warfare forces electronic countermeasures.[51] The PLARF's exercises that involve "red-blue confrontation" have involved special forces representing the red (i.e., national) and blue (i.e., adversary) forces, engaging in the defense of strategic weapons systems and sabotage.[52] Potentially, special operations could be employed in reconnaissance of the targets of conventional and nuclear ballistic strikes, according to the *Science of Second Artillery Campaigns,* a textbook that is considered relatively authoritative on these issues.[53]

The People's Armed Police (PAP), a force that is internally focused but also under the command of the Central Military Commission, also includes several special forces contingents.[54] These units are believed to have a primarily internal security focus, though they have been seen as part of embassy protection units. The PAP has engaged in extensive antiterrorism exercises. For instance, China and Kyrgyzstan engaged in the "Cooperation One 2019 Joint Anti-Terrorism Exercise" in 2019 in Urumqi, in which the "Mountain Eagle" (山鷹) commando team from the Xinjiang Armed Police Corps, created since the PLA reforms, participated.[55] Their commander claimed, "On the front lines of antiterrorism, we must always keep the arrow on the string and lead to a high-alert state, acting as a 'ballast stone' to maintain national security and social stability."[56]

The PLA has also concentrated on ensuring that special forces are incorporated into the system of systems operations and long-range precision strikes.[57] "Special operations are comparable to the sharp swords of the future battlefield," declares one PLA commentator.[58] The PLA has also explored how electronic countermeasures could be leveraged in counterterrorism special operations, including for reconnaissance and interference against terrorist networks' command and communications.[59] The continued development of PLA SOF will leverage the use of unmanned systems in order to expand into domains where traditional special forces cannot readily operate.

Adaptation of Concepts of Hybrid Warfare

The PLA has carefully examined American and Russian concepts of hybrid warfare.[60] PLA strategists have questioned whether recent discussion on hybrid warfare involves "old wine in new bottles," pointing to antecedents dating back to the early 2000s.[61] The PLA has engaged in intense studies of foreign military's theories and concepts of special operations, including emphasizing cyber, space, and unmanned operations.[62] By the PLA's view, the US military was the first to propose the theory of hybrid warfare, but the Russian military has proven most successful in actualizing hybrid warfare on the battlefield.[63] Summarizing this literature across American and Russian thinking, Chinese defense academics believe hybrid warfare is characterized by features that include not only militaries but also nonstate actors and even individual civilians participating; the mixture of warfare styles such as conventional operations, unconventional operations, terrorist attacks, and riots; and the blending of political, military, economic, social, and informational means of war.[64] The PLA is also concerned with techniques for "counter hybrid warfare," including integrating defensive measures across multiple domains, reflecting concerns the US military could undertake these tactics against it.

Chinese observers often characterize Russian military intervention in Syria as strikingly effective, despite evidence to the contrary. For instance, according to one commentator: "The involvement of the Russian military in antiterrorism in Syria has broken the blockade of the West, overcome the obstacles on the way forward, (re)balanced the balance of power in the Middle East, and even reshaped the

Middle East pattern to a considerable extent."[65] In discussing Russian operations in Syria, Chinese military strategists have observed, "The unmanned combat systems debuted, and their operational effectiveness was remarkable."[66] Looking at trends on the Syrian battlefield, Chinese observers have frequently highlighted the prominence of "unmanned warfare" (无人化战争) and the successful employment of electromagnetic warfare, as well as the use of special operations.[67] Chinese military academics are also concerned with a trend of great-power intervention that leverages local proxies, including pointing to American assistance to anti-Assad forces in Syria.[68]

Such proxy conflicts and special operations are increasingly extending from physical domains into virtual spaces. Fittingly, with China's all-domain view of cyber warfare, the *Science of Campaigns* had noted "computer 'hacker' warfare will also become an important means of special operations." which could involve the PLA's new Strategic Support Force, which is also taking on a more expansive mission for information operations, including psychological warfare. The PLA is exploring how to increase the integration and utilization of unmanned systems in support of special operations, including, for instance, the use of unmanned ground vehicles for logistical support.[69] The PLA is also interested in pursuing research to enable the optimization and potentially enhancement of human capabilities, leveraging advancements in precision medicine and improvements in training.[70]

Battle of the Minds

The PLA's approach to future warfighting could include leveraging "three warfares" (三种战法) throughout the course of operations.[71] The three warfares include public opinion warfare (舆论战), psychological warfare (心理战), and legal warfare (心理战). In addition, the Chinese Communist Party maintains specialized departments with parallel mandates: the International Liaison Department (中联部), essentially a second foreign ministry with responsibility for developing contacts with foreign political parties, and, notably, the United Front Work Department (统战部), which has wide-ranging responsibility for internal stability maintenance and external liaison work.[72] This is not to mention China's Ministry of State Security (MSS), which has been characterized as comparable to the Central Intelligence Agency in its missions and capabilities, known to carry out a wide range of operations, from human intelligence to cyber espionage.[73] Significantly, in the course of the PLA's recent reforms, the PLA Strategic Support Force—which is responsible for space, cyber, electronic, and psychological warfare—has also incorporated Base 311, also known a the "Three Warfares Base," which would be responsible for political work/warfare and psychological operations,[74] primarily targeting Taiwan to date.[75] These recent changes in force structure could enable a more effective combination of capabilities for cyber and psychological operations.[76]

The PLA believes these "intangible" domains have become integral to modern informatized warfare, in which seizing "information dominance" (制信息权) is vital

to victory on the battlefield.[77] Similarly, Chinese military strategists believe the "three warfares" (三种战法) are critical to seizing "discourse power" (话语权), in political and military struggles.[78] Increasingly, PLA academics and strategists are also exploring the opportunities to leverage social media and emerging technologies to enhance their capabilities across these various dimensions of information operations, leveraging lessons learned from US and Russian activities in the process.[79] The PLA has explored concepts of "cross/all-domain asymmetric operations," envisioning attacks that could occur across political, economic, military, cultural, public opinion, religious, and other activities,[80] as well as the information, cognitive, and social domains. "When the weaker side is unable to effectively kill the opponent through military means, it can also win the war by other means by attacking the other party's psychology," argues one defense academic.[81] In contemporary confrontation, "cognitive warfare" has taken on particular prominence, involving techniques to attack and subvert the mind, cognition, and decision-making.[82]

The PLA continues its tradition of concentrating on the offensive and defensive dimensions of psychological warfare. According to the PLA's dictionary of official terminology, psychological warfare involves "operations using specific information and media to influence the target's psychology and behavior in order to advance the achievement of political and military combat objectives, based on strategic intent and operational taskings."[83] According to *Lectures on the Science of Information Operations*, an authoritative textbook on the topic, the objectives involve "breaking down the enemy psychologically while stabilizing and inspiring one's own troops."[84] These "combat measures" are intended to advance the "goal of winning without a fight or emerging victorious from a fight."

In particular, the conduct of psychological warfare is regarded as a continuum. "Because the execution of psychological warfare has no stringent time or space limitations, it runs throughout times of war and peace, and it permeates politics, economics, culture, religion, science and technology, society, and all other domains."[85] In the conduct of information operations, countermeasures that integrate these capabilities can be leveraged for purposes of influence, intimidation, and psychological subjugation."[86]

Increasingly, such a "battle of wits" has been playing out in real time against Taiwan and Hong Kong. In particular, the dynamics of "public opinion warfare" are believed to have "already broken through the boundaries of peacetime and wartime," thus becoming a contest of "you die, I live" (你死我活).[87] Today, public opinion warfare is the "second battlefield," critical to achieving winning without fighting (不战而屈人之兵).[88] PLA researchers have been exploring lessons learned from recent operations in Ukraine, Iraq, and Syria,[89] which are believed to demonstrate that social media can achieve effects on the battlefield that exceed and transcend those achievable through conventional capabilities.[90] Consistently, PLA thinking tends to emphasize the psychological dimensions of conflict in the information age, even

raising the notion of "cognitive dominance" (制脑权) as a critical factors for warfare in an age of pervasive information and connectivity.[vi]

Conclusion

The PLA's continued modernization has concentrated on a vast array of conventional and unconventional capabilities. While continuing to expand and modernize its special forces for high-end conflict scenarios, PRC also currently engages in what might be characterized as gray-zone activities, primarily associated with its militia and coast guard. As the PRC concentrates on "re-unification" with Taiwan as a key element of national rejuvenation, special operations could serve as the tip of the spear in future conflict scenarios. Pursuant to that operational imperative, the role of maritime special operations is expanding, including propaganda and the introduction of swimmer delivery vehicles (SDV).[91] While the PLA's focus remains on Taiwan, Japanese defense officials are concerned about the vulnerability of their offshore islands, whose air bases could be seized and used to continue forward operations against the main Japanese islands.

Ultimately, special forces represent a critical component of what the PLA is working toward, a high-tech, decentralized/dispersed [分散], and highly capable force. At the same time, the continued development of psychological operations capabilities may have immediate relevance in peacetime competition. In a scenario of high-end conflict, the PRC's expansive architecture for national defense mobilization could realize Mao Zedong's vision of people's warfare, but leveraging new theories and technological capabilities.

vi Since these terms have been raised primarily in less authoritative writings to date, it is unclear the extent to which such concepts will reflect actual strategic/doctrinal thinking.

Endnotes

1 "Reshape the New-Quality Combat Force System to Deal with "Cyber War," [重塑新质作战力量体系应对" 网络战"], Study Times [学习时报], https://web.archive.org/web/20200104222539/http://www.cac.gov.cn/2015-06/15/c_1115613607.htm.

2 See the latest defense white paper that provides an official discussion of the reforms: "China's National Defense in the New Era," Xinhua, July 24, 2019, available at http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm.

3 "'Lifeline'" integrated into system of systems confrontation," [生命线" 全方位融入体系对抗], China National Defense Network, June 6, 2018, http://www.81.cn/jfjbmap/content/2018-06/06/content_207938.htm. "A brigade of the naval aviation in the northern theater aims at actual combat training" [北部战区海军航空兵某旅瞄准实战练兵备战], PLA Daily, June 10, 2019, http://www.legaldaily.com.cn/army/content/2019-06/10/content_7899427.htm.

4 For instance, China's National Defense University recently convened a symposium on intelligentized warfare: "The First "Intelligentized Warfare" Symposium Convened in Beijing" [首届" 智能化战争" 研讨会在京举行], December 28, 2019, https://web.archive.org/web/20200104223315/http://www.china001news.com/edu/20191228_5937.html

5 On the impact of technology on PLA tactics, see Dennis Blasko, "'Technology Determines Tactics': The Relationship between Technology and Doctrine in Chinese Military Thinking," *The Journal of Strategic Studies* 34, no. 3 (2011): 355-381.

6 The original sourcing for this quotation has been difficult to determine. See this quotation referenced in, for instance: Cai Yubin [蔡渭滨] and Huang Xuebin [黄雪斌], "Vigorously Cultivate the Fighting Spirit of Scientific and Technological Personnel" [大力培育科技人员的战斗精神], *PLA Daily*, May 6, 2019, available at http://www.xinhuanet.com/mil/2019-05/06/c_1210126997.htm.

7 See the latest defense white paper that provides an official discussion of the reforms: "China's National Defense in the New Era," *Xinhua*, July 24, 2019, available at http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm.

8 For more context on people's warfare, see: Dennis J. Blasko, "Chinese Strategic Thinking: People's War in the 21st Century," *China Brief*, March 18, 2010, https://jamestown.org/program/chinese-strategic-thinking-peoples-war-in-the-21st-century/.

9 See the PLA's official dictionary. All-Military Military Terminology Management Committee [全军军事术语管理委员会], People's Liberation Army Military Terminology [中国人民解放军军语], Military Science Press [军事科学出版社], 2011, p. 660.

10 See, for instance: "Requirements for the operation of the new system in the main battle zone" [把好战区主战这个新体制运行要求], Xinhua, February 26, 2019, http://www.xinhuanet.com/mil/2019-02/26/c_1210067723.htm.

11 "Accelerate the Construction of a New Pattern of National Defense Mobilization in the New Era," [加快构建新时代国防动员建设新格局], *PLA Daily*, September 18, 2019, http://www.81.cn/jmywyl/2019-09/18/content_9627047.htm.

12 Ye Zheng [叶征]. A Discussion of the Innate Characteristics, the Composition of Forces, and the Included Forms" [论网络空间战略博戏的本质特征，力量构成与内容形势], *China Information Security* [中国信息安全], August 2014.

13 "Syrian Conflict—A "Prism" for Proxy Warfare" [叙利亚冲突一透视代理人战争的" 棱镜"], PLA News, April 26, 2018, http://www.xinhuanet.com/mil/2018-04/26/c_129859623.htm.

14 "Fight Together: Massive Enemy Guerrilla Battle" [齐会战斗：大量歼敌精锐的游击战], *PLA Daily,* July 11, 2019, http://www.81.cn/jfjbmap/content/2019-07/11/content_238073.htm.

15 "How Should the Future War Be "Played?" [未来战争应怎样" 打], *PLA Daily*, July 30, 2019.

16 "China's National Defense in the New Era," *Xinhua*, July 24, 2019, http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm.

17 For historical context, see also: Elleman, Bruce. *Moscow and the Emergence of Communist Power in China, 1925-30: The Nanchang Uprising and the Birth of the Red Army*. Routledge, 2009.

18 Urbansky, Sören. "Moscow and the Emergence of Communist Power in China, 1925-30. The Nanchang Uprising and the Birth of the Red Army." (2010): 199-200.

19 Liu Jie [刘杰], "Special Operations in the Long March" [长征中的特种作战], Contemporary Elderly [当代老年], issue 12, 2016, http://www.cqvip.com/qk/80153x/201612/670725912.html

20 For context, see Thomas P. Bernstein, et al. *China learns from the Soviet Union, 1949–present*. Rowman & Littlefield, 2010.

21 Charles Kraus, "How Stalin Elevated the Chinese Communist Party to Power in Xinjiang in 1949," May 11, 2018, https://www.wilsoncenter.org/blog-post/how-stalin-elevated-the-chinese-communist-party-to-power-xinjiang-1949. See also: Kraus, Charles. "Creating a Soviet "Semi-Colony"? Sino-Soviet Cooperation and its Demise in Xinjiang, 1949-1955." Chinese Historical Review 17, no. 2 (2010): 129-165.

22 Kevin McCauley, "PLA Yijiangshan Joint Amphibious Operation: Past is Prologue," *China Brief*, September 13, 2016, https://jamestown.org/program/pla-yijiangshan-joint-amphibious-operation-past-is-prologue/.

23 John Kenneth Knaus, *Orphans of the Cold War: America and the Tibetan Struggle for Survival,* Public Affairs, New York, 1999.

24 Chen Jian, "China's Involvement in the Vietnam War, 1964–69," China Quarterly 142 (1995): 356-387.

25 "China: Military Options against Vietnam" [Declassified] CIA-RDP84S00928R0003000050006-0, National Archive CIA Records Search Tool (CREST), p. 5 https://www.cia.gov/library/readingroom/docs/CIA-RDP84S00928R000300050006-0.pdf; Lai, Benjamin. *The Dragon's Teeth: The Chinese People's Liberation Army—Its History, Traditions, and Air Sea and Land Capability in the 21st Century*. Casemate, 2016. Kindle edition. Loc. 1944.

26 Tanner, Harold Miles. "Guerrilla, Mobile, and Base Warfare in Communist Military Operations in Manchuria, 1945-1947." Journal of Military History 67, no. 4 (2003): 1177-1222.

27 Julie Makinen, "Communists' Version of China's Wartime Record Frustrates Taiwan," September 2, 2015, https://www.latimes.com/world/asia/la-fg-china-taiwan-nationalists-20150901-story.html.

28 "Battle of Huaihai: 600,000 Victory over 800,000 War Miracles," [淮海战役：以60万战胜80万的战争奇迹], Central Military, January 8, 2019, http://www.mod.gov.cn/education/2019-01/08/content_4834146.htm.

29 "Upholding the Righteousness, Shaking the Enemy Camp—The Red Army's Long March" [秉持大义撼敌营—红军长征途中瓦解敌军记事], Ministry of National Defense, September 19, 2019, http://www.mod.gov.cn/education/2016-09/19/content_4733311.htm.

30 Paul Huang, "Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate," Foreign Policy, June 26, 2019, https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/.

31 For context and prior writings, see Dennis Blasko, "PLA Special Operations Forces: Organizations, Missions and Training," China Brief, 1 May 2015, https://jamestown.org/program/pla-special-operations-forces-organizations-missions-and-training/. See also: Kevin McCauley, "PLA Special Operations: Combat Missions and Operations Abroad," China Brief, 3 September 2015. https://jamestown.org/program/pla-special-operations-combat-missions-and-operations-abroad/.

32 Alastair Finlan, "British Special Forces in the Falklands War of 1982," *Small Wars and Insurgencies* 13, no. 3 (2002): 75-96.

33 "A Certain Special Combat Brigade of the Army in the Central Theater Organizes Parachute Assault Training in Nine Cold Days," [中部战区陆军某特种作战旅数九寒天组织伞降突击训练], Workers Daily, January 2, 2020, http://military.workercn.cn/32817/202001/02/200102081041238.shtml.

34 DM Chan, "China Unveils Special Counter-Terror Force in Xinjiang," Asia Times, August 20, 2019, https://www.asiatimes.com/2019/08/article/china-unveils-special-counter-terror-force-in-xinjiang/.

35 Chen Zhiqi [陈志奇] and Zhao Yunfeng [赵云峰], "New Characteristics of Joint Special Operations Missions in the Context of Information Warfare" [信息化战争背景下联合特种作战任务新特点], National Defense Science and Technology [国防科技], 2019,40(3).

36 "For the First Time, the Army Organized Five New Types of Power Competitions to Promote Transformation and Construction," [陆军首次组织 5 类新型力量比武竞赛推进转型建设], Xinhua, July 9, 2018, http:// www.xinhuanet.com/politics/2018-07/09/c_1123100617.htm.

37 "Army Special Forces Anti-Terrorism Combat Actual Combat Drill" [陆军 特种部队反恐作战实兵实弹演练], CCTV, May 26, 2018, http://news.cctv.com/2018/05/26/ARTIHNuKwLHkN7D5G2OHDKRE180526.shtml

38 "如果说远火是陆军伸长的拳头，那么特种兵则是陆军插入敌人心脏的匕首." "The Army's Programming Structure Is Further Optimized: The Proportion of Special Operations, etc. Forces Is Greatly Increased," [陆军部队编程结构进一步优化：特种作战等力量比例大幅提升], CCTV, July 19, 2017, https://www.thepaper.cn/newsDetail_forward_1736564.

39 "The Gods Are Falling! Directly Attack the Army Training Site in xinjiang" [神兵天降！直击陆军新疆集训现场], May 24, 2018, http://www.js7tv.cn/news/201805_146040.html.

40 "The Army First Organized a Special Combat Force Assessment Contest" [陆军首次组织特种作战部队考核比武], Xinhua, July 16, 2018, www.xinhuanet.com/politics/2018-07/16/c_129914444.htm.

41 "The PLA Army Tests Its Special Forces Capabilities," OE Watch, August 2018, https://community.apan.org/wg/tradoc-g2/fmso/m/oe-watch-past-issues/241432/; "Real Shooting Army 'Special Fighter-2019' Assessment Competition" [实拍陆军"特战奇兵-2019"考核比武], Central Military [央广军事], May 15, 2019, https://web.archive.org/web/20200105002130/http://military.cnr.cn/ycdj/20190515/t20190515_524613759.html

42 "PLA Army Tests Its Special Forces Capabilities," OE Watch, 2018; "Real Shooting Army,' Central Mililtary, 2019.

43 Dennis J. Blasko and Roderick Lee, "The Chinese Navy's Marine Corps, Part 1: Expansion and Reorganization," *China Brief*, February 1, 2019, https://jamestown.org/program/the-chinese-navys-marine-corps-part-1-expansion-and-reorganization/. Dennis J. Blasko and Roderick Lee, "The Chinese Navy's Marine Corps, Part 2: Chain-of-Command Reforms and Evolving Training," *China Brief*, February 15, 2019, https://jamestown.org/program/the-chinese-navys-marine-corps-part-2-chain-of-command-reforms-and-evolving-training/

44 Blasko and Lee, "Chinese Navy's Marine Corps, Part 1, 2019; Blasko and Lee, "The Chinese Navy's Marine Corps, Part 2, 2019.

45 "China's Navy Saves the World in 'Operation Red Sea,'" *Military Times*, June 12, 2018, https://www.military.com/undertheradar/2018/06/12/chinas-navy-saves-world-operation-red-sea.html.

46 "The Jiaolong Commandos," China Military Online April 15, 2019, http://eng.chinamil.com.cn/view/2019-04/15/content_9478613.htm.

47 "Central-2019 Exercise Kicked Off" [中部-2019"演习拉开帷幕], China Military Online, September 16, 2019, http://www.81.cn/jfjbmap/content/2019-09/16/content_243420.htm.

48 "A Close Look at Chinese Airborne Troops," China Military Online, August 30, 2017, http://eng.chinamil.com.cn:80/view/2017-08/30/content_7736996.htm.

49 "Close Look at Chinese Airborne Troops," China Military Online, 2017.

50 "The Special Forces of the Rocket Army Guarding the Dongfeng 16 are Exposed, Going through Brutal 'Hunter Training'" [守护东风16的火箭军特种部队曝光，要经历残酷的"猎人训练"], March 23, 2019, https://new.qq.com/omn/20190523/20190523A0N4MZ.html.

51 "Rocket Force Regularly Conducts 'Sky Sword' Series of Exercises," [火箭军常态开展"天剑"系列演训], Guancha, May 30, 2018, https://www.guancha.cn/military-affairs/2018_05_30_458380.shtml.

52 "Lin Hai Xueye Breaks through the Attack—Experience the Special Combat Training under the Severe Cold Conditions of a Certain Blue Army Init of the Rocket Army," [林海雪野破袭战—亲历火箭军某蓝军部队严寒条件下特战训练], Xinhua, February 4, 2019, www.xinhuanet.com/politics/2019-02/04/c_1124085458.htm.

53 *The Science of Second Artillery Campaigns* [第二炮兵战役学].

54 Joel Wuthnow, China's Other Army: The People's Armed Police in an Era of Reform. National Defense University Press, 2019.

55 "'Mountain Eagle' Commando First Battle China-Kyrgyzstan 'Cooperation 2019' Joint Anti-Terrorism Exercise," [天山亮剑！"山鹰"突击队首战中吉"合作—2019"联合反恐演练], Global Times Online, August 20, 2019, https://china.huanqiu.com/article/9CaKrnKmk97.

56 Mountain Eagle' Commando, Global Times, 2019.

57 "Sharp Blade—2016 True Mountain A" Exercise Army Special Forces Full Embedding System of Systems Operations," ["利刃-2016·确山A"演习陆军特种部队全程嵌入体系作战], People's Daily, October 25, 2016, http://military.people.com.cn/n1/2016/1025/c1011-28805385.html.

58 Yang Jianyi [杨建懿], "Thoroughly Analyzing the Trends in Development of Informatized Special Operations" [透析信息化特种作战发展趋势], China Military Online, August 16, 2018, http://www.81.cn/theory/2018-08/16/content_9254392.htm.

59 Chen Bingyi [陈炳毅], "Discussion on the Application of Electronic Counter-Strike Force in Anti-terrorism Special Operations under the Condition of Plateau Mountain in Border Areas" [边境地区高原山地条件下反恐特种作战电子对抗力量运用浅议], 32159 troops; 《国防》 2017年11期

60 "Hybrid Warfare": Is It a New Bottle of Old Wine, or Is It a Special Dish?" ["混合战争"：是新瓶旧酒，还是别开生面], *PLA Daily*, May 16, 2019, http://www.sohu.com/a/314219527_628598.

61 Chen Hanghui [陈航辉] and Deng Xiumei [邓秀梅, "Is It a New Bottle of Old Wine, or Is It A Noodle? Analysis of the Characteristics of Hybrid Warfare Theory," [是新瓶旧酒，还是别开生面—浅析混合战争理论的特点], *PLA Daily*, May 16, 2019, http://www.legaldaily.com.cn/army/content/2019-05/16/content_7876256.htm.

62 Feng Donghao [冯东浩], "Pay Attention to the Development Trend of Foreign Military Operations Theory" [关注外军作战理论发展趋势], *PLA Daily*, June 12, 2018, http://www.81.cn/jfjbmap/content/2018-06/12/content_208433.htm.

63 Xie Lei [谢蕾], "Pay Attention to the Study of Anti-Hybrid Warfare" [重视反混合战争问题研究], *PLA Daily*, May 30, 2019, http://www.qstheory.cn/llwx/2019-05/30/c_1124560384.htm.

64 Xie Lei, "Pay Attention to the Study of Anti-Hybrid Warfare," 2019.

65 Zhang Wei [张犟] "Use 'Eyes' to Create with "Mental Power"—Innovative Use of "Gerasimov Tactics" [凭”眼光”拿来用”脑力”创造—有感于”格拉西莫夫战术”的创新运用], China Military Online, March 29, 2018, http://www.81.cn/jfjbmap/content/2018-03/29/content_202673.htm.

66 Liu Yuqi [刘玮琦], "Russian Version of "Hybrid Warfare" Bright Swords on the Syrian battlefield," [俄版”混合战争”亮剑叙利亚战场], *PLA Daily,* September 20, 2018, http://www.81.cn/jfjbmap/content/2018-09/20/content_216355.htm.

67 Li Ruijing [李瑞景], "Looking at the Future War from the Syrian Battlefield," [从叙利亚战场看未来战争模样], China Military Online, February 8, 2018, http://www.gfdy.gov.cn/defense/2018-02/08/content_7937162.htm.

68 Li Ruijing [李瑞景], "Local Warfare's "Proxyization" Is Intensifying" [局部战争”代理化”愈演愈烈], *PLA Daily*, June 5, 2016, http://www.81.cn/jfjbmap/content/2016-06/05/content_146616.htm.

69 Cheng Ming [程明], Yang Yong [杨勇], and Lu Minglei [路明磊], "Analysis of Development Needs of Special Operations Unmanned Support Vehicles" [种作战无人支援车发展需求分析], Science and Technology Vision [科技视界], (20) 2019.

70 Ding Mingchao [丁明超], et al., "Theory and Practice of Special Operations Training: From the Improvement of Recovery Ability to the Optimization of Human Ability," [特种作战训练的理论与实践——从恢复能力的提高转向人类能力最佳化], Sports Science Literature Bulletin [体育科技文献通报], 10 (2019): 28.

71 Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," *China Brief*, August 22, 2016. https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/.

72 Brady, Anne-Marie. Magic Weapons: China's Political Influence Activities under Xi Jinping. Vol. 18. Wilson Center, 2017.

73 Peter Mattis, "The Analytic Challenge of Understanding Chinese Intelligence Services," Studies in Intelligence 56, no. 3 (2012): 47-57.

74 For recent sourcing discussing the PLASSF 311 Base's engagement with concerns of innovation in political work for the cyber era, see "Working Diligently to Promote the Innovative Development of Political Work" [努力推动政治工作创新发展], China Military Network, April 23, 2019, https://web.archive.org/web/20190423033915/http://www.81.cn/2018hldk/2018-10/30/content_9326217.htm

75 Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," China Brief, Volume: 16 Issue: 13, Jamestown Foundation, August 22, 2016, https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/. Mark Stokes and Russell Hsiao, The People's Liberation Army General Political Department Political Warfare with Chinese Characteristics, Project 2049 Institute, October 14, 2013.

76 John Costello and Joe McReynolds, "The Strategic Support Force: A Force for a New Era," National Defense University, October 2, 2018, http://ndupress.ndu.edu/Media/News/News-Article-View/Article/1651760/chinas-strategic-support-force-a-force-for-a-new-era/; Elsa Kania and John Costello, "The Strategic Support Force and the Future of Chinese Information Operations," Cyber Defense Review, Spring 2018, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf?ver=2018-07-31-093713-580

77 For an authoritative article that addresses this topic, see "Academy of Military Science President: Reforms Must Resolve the Restraints upon Systematic Assurance for a Powerful Military" [军事科学院院长:改革要解决羁绊强军的体制性障碍], *PLA Daily*, November 2, 2015, http://www.chinanews.com/mil/2015/11-02/7600724.shtml.

78 Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部] (ed.), *The Science of Military Strategy* [战略学], 2013.

79 Mou Shan [牟珊], "Information Weaponization and Military Social Media Strategy" [信息武器化与军队社交媒体战略], China National Defense Report [中国国防报], http://www.mod.gov.cn/intl/2015-07/22/content_4605755.htm.

80 Wang Hongyou [汪洪友], "Fight Cross-Domain Asymmetric Warfare" [打好跨域非对称作战], PLA Daily, http://www.81.cn/jfjbmap/content/2019-08/29/content_242008.htm.

81 Xu Shiyong [许世勇], "New Solution to the Connotation of Asymmetric Warfare" [非对称作战内涵新解], *PLA Daily*, January 31, 2019, http://www.81.cn/jfjbmap/content/2019-01/31/content_226616.htm.

82 See, for an excellent assessment of these trends, Nathan Beauchamp-Mustaphaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," China Brief, September 6, 2019, https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/

83 *Military Terminology of the Chinese People's Liberation Army*, Military Science Press, 2011.

84 Ye Zheng [叶证], *Lectures on the Science of Information Operations* [信息作战科学教程].

85 Ye Zheng, *Lectures on the Science of Information Operations*.

86 Ye Zheng, *Lectures on the Science of Information Operations*.

87 Liu Huiyan [刘惠燕], et al., "Thoughts on Promoting the Development of Cognitive Domain Combat Equipment in the Whole Media Environment" [全媒体环境下推进认知域作战装备发展的几点思考], Defense Technology, Issue 5, 2018, http://www.cqvip.com/QK/96765A/201805/676887804.html. The authors are affiliated with Unit 61716.

88 Jiang Xinghua [姜兴华], *Invisible Bright Sword: Accelerate the Transformation of Communication Power Generation Model* [无形亮剑——加快转变传播力生成模式], Long March Publishing House [长征出版社出版], May 2015.

89 Chen Hanghui [陈航辉], "Social Media Warfare, the New Dimension of War in the Information Age," [社交媒体战,信息时代战争新维度], *PLA Daily*, September 25, 2015, http://www.81.cn/jfjbmap/content/2015-09/25/content_124476.htm.

90 Zhong Jianchang [钟建昌], "Analysis on the Coping Strategies of Social Media Information Warfare—Taking Russia to deal with the Ukrainian crisis as an example" [信息舆论兵临城下 政治干部天天在战斗], *PLA Daily*, August 6, 2014, https://web.archive.org/save/http://www.81.cn/jwgd/2014-08/06/content_6080875.htm; Mou Shan [牟珊], "Information Weaponization and Military Social Media Strategy" [信息武器化与军队社交媒体战略], China National Defense Report [中国国防报], http://www.mod.gov.cn/intl/2015-07/22/content_4605755.htm.

91 Sam LaGroe, "New Chinese Nuclear Sub Design Includes Special Operations Mini-Sub," USNNI, March 25, 2015, https://news.usni.org/2015/03/25/new-chinese-nuclear-sub-design-includes-special-operations-mini-sub.

SECTION 2

BIOLOGY AND THE BODY POLITIC: MESSING WITH MOTHER NATURE

CHAPTER 8

What COVID-19 and China's Grand Strategy May Teach about a History of the Future

Capt. L. R. Bremseth and James Giordano

The SARS-CoV-2 (COVID-19) virus is not a biological weapon. But, certainly, it is an agent creating mass disruption—and destructive effects—to human life, health, economies, and social stability. Media coverage and political discourse are rife with language that speak of "waging war" against the virus—and perhaps rightly so in calls for mobilizing resources, goods, services, and personnel in a fight for health and survival. However, despite (1) awareness of the United States' relative weaknesses in biosecurity; (2) viability—if not likelihood—of current and future biological threats capable of large-scale impact (e.g., inclusive of natural, human-made, and/or combination of human-induced natural threats); and (3) past modeling and gaming exercise to assess both possible trajectories and US readiness of such events, COVID-19 has illuminated inadequacies in US preparedness. This failure of recognition, in conjunction with a relative collective rigidity in thought and institutionalized preparedness and response processes, has enabled our strategic competitors to gain advantage over the United States in these irregular and often unrestricted engagements. To be sure, the world is watching.

How might such vulnerabilities be mitigated, if not prevented in the future? We believe that while the US special operations forces (SOF) have been utilized effectively—and in some cases overextended in their prior and current utilization—a reevaluation and redirection of key SOF elements and resources could be employed in engagements that contribute strongly to surveillance and interdiction of radical leveling technologies and emerging risks and identified threats on the global stage. But such use of SOF, or any other Title 10 or Title 50 asset(s), is predicated on governmental coordination and collaboration in recognizing the extant need for risk/threat identification and mitigation, coupled with a national ability to rally and coalesce in directed efforts to assure security, stability, and sustainability of multicomponential efforts and enterprises (i.e., a unified national, state, and local governmental, research, and commercial endeavor).

The US population's visual witnessing of attacks and destruction, such as those that occurred at Pearl Harbor on December 7, 1941 and at numerous sites within the United States on September 11, 2001, has been shown to evoke rapid public and governmental response, often with predictable patriotic fervor. But, thankfully, such overt attacks remain few and far between, in part because of the frank bellicosity of their intent and the resulting justification of any retaliatory action. Such explicit acts of war are not and, we argue, will not be the norm. Rather, engagements to evoke disruptive and influentially "down-range" destructive effects on various aspects of US infrastructure, socioeconomics, and international position will be increasingly nonkinetic.

Scenario Vignette: A History of the Future

China's Grand Strategy

The year is 2049, and China reigns supreme. Since 2032, China has had the world's largest economy with the yuan as the global reserve currency, and Mandarin has been recognized language of business, trade, and commerce. The United States barely achieves ranking in the top five global economies, and its international market leverage remains prominent only in limited domains (e.g., automotive and commercial aircraft production).

During the late 2020s, socialism replaced capitalism in the United States as the preferred socioeconomic model. Whereas China had succeeded in becoming a global economic power by embracing capitalistic economic principles while retaining communist political and social principles, the United States embraced socialist economic approaches that decades before had failed to produce Chinese economic success. China clandestinely (and in some instances covertly) influenced the United States' move toward this inefficient form of socialism by discretely funding US academic programs, media, and public enterprises by employing large-scale psychological operations (psyops) to both pulse and affect US culture. Additionally, China funded Mexican cartels to smuggle considerable quantities of illegal drugs and and an iteratively growing number of illegal immigrants across the US southern border to incur sociopolitical discord, disrupt the social fabric, and both tacitly and explicitly change US social demographics to establish ideologies and perspectives aligned, rather than competing, with those of China.[1] It took several decades, but these nonkinetic, asymmetric engagements were instrumental in China realizing its "grand strategy" of assuming status as the global superpower. The United States was reduced to a significantly lesser force in international relations and capabilities. China overcame long-standing tensions with the United States for power dominance without the need (or burden) of armed conflict. Durable, dogged adherence to the philosophy and teachings of Sun Tzu, with specific emphasis on both achieving victory prior to or without conventional warfare as well as *deception* had assured China's success.

The success of China's grand strategy to achieve global dominance was the result of careful, deliberate planning and successful implementation of successive Five-Year Plans. During the 1980s and 1990s, both US and Chinese officials debated current and future intentions of US-Chinese relations and relative positions in the evolving world order. By the late 1990s, China's leadership was influenced and directed predominantly by military and former military officials (i.e., pro-conflict "hawks" [*ying pai*]) who advised strategic steps to avenge China's "hundred years of humiliation" (1845-1945) and, in the process, replace the United States as the economic, military, and political leader of the world by 2049).[2] The Chinese accomplished the strategic intent to "revise the US-dominated economic and geopolitical world order founded at Bretton Woods and San Francisco at the end of World War II"[3] by

developing and executing the "hundred-year marathon."[i] Deception provided the key to the ultimate and durable success of this plan, preventing the United States from gaining insight and/or access to China's strategic intentions until it was too late to effect any change or mitigation. This plan required decades of effort and patience, and it succeeded brilliantly.

China's Military Dominance

By 2049, Chinese culture has obtained broad-scale global effects as a function of the outreach capabilities provided by its vast media and entertainment industries. Further, China's dominance in science and technology (S&T) is uncontested given its decades of investment. A consequence of these S&T advancements is China's control of space and the global maritime (surface and subsurface) domain(s), thereby ensuring Chinese commercial, as well as military, global access and influence. The People's Liberation Army Navy (PLAN) can exercise activity wherever and whenever desired, as it is the most advanced, largest, and most powerful navy in the world.

The US Navy (USN), while still a capable military force, has fallen significantly behind PLAN, both in number of combatant ships and global influence. Thus, while the USN continues to conduct transits to and from the Indo-Pacific theater of operations, it remains careful not to antagonize the PLAN or Chinese commercial vessels. The USN's prior role as a guarantor of maritime free passage in both the Indo-Pacific region and globally is now assumed and performed by the PLAN. But rather than providing and assuring "freedom of the seas" navigation for any and all vessels, the PLAN serves as an instrument to advance China's economic and military influence worldwide.

The comparative impotence of the USN affords China tremendous military capability. China eschews conventional land and/or air warfare, instead focusing on naval power to assure global military and trade dominance. By reducing the viability of the USN, China essentially guaranteed regional anti-access, area denial (A2AD), thereby negating US Army and Air Force assets by preventing them from reaching key geographic domains of China's global power. Instead, any form of kinetic warfare is relegated to "proxy geographies" (e.g., Africa and South America). Taken together, these dynamics fortified China's political and military sovereignty in and across Asia, the Indo-Pacific region, and, ultimately, worldwide.

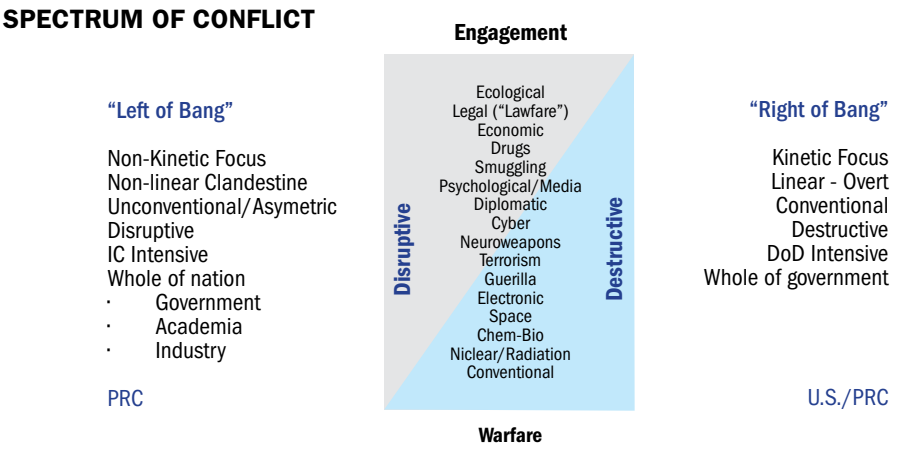
China absorbed Taiwan politically in 2034. The United States was unable to mount an effective naval military deterrent for fear of losing numerous carrier battle groups and other assets to advanced Chinese hypersonic and space-based weapons. US military power was essentially "check-mated" and forced to acquiesce to China's demonstrated power and demands. From that point, US military capacity, influence, and prestige began a precipitous decline from which it did not recover.

i In Chinese, the word "marathon" refers to a long-term effort of rejuvenation or restoration.

> *"The highly developed Chinese body of doctrine is particularly relevant today because of China's long-term strategy to expand its influence worldwide through a well-integrated mix of diplomacy, propaganda, intelligence, technology acquisition and innovation, and commercial trade. . . . Deception continues to play an underlying role, increasingly augmented by an unprecedented expansion of overt military power, as in the establishment of de facto control over disputed waters in the South China Sea, in violation of international law."*[4]
>
> ***—Arturo Muñoz, 2018***

Essential to its success, China adhered strictly and unwaveringly to the teachings of Sun Tzu, particularly Sun Tzu's emphasis that, "All warfare is based on deception."[5] The United States failed to appreciate or understand Sun Tzu fully and, consequently, did not recognize China's highly effective employment of deception, especially as implemented through its well-established three nonkinetic warfares: media, psyops, and law/lawfare. The view by some in the US government that no definitive proof of deception existed failed to acknowledge 1) evidence in Chinese and Western sources indicating the historical and cultural proclivity of Chinese officials to undertake coordinated activities to mislead perceived opponents, whether internal or external, about the country's intentions or capabilities, and 2) the innate susceptibility of people to deception.[6]

While deception was certainly vital to China's success, another contributory element was China's continual quantitative measurement of success of the numerous nonkinetic engagements it had implemented during preconflict ("left of bang") conditions. These included economic, cyber, precision biological and chemical enterprises, and narcoterrorism, in addition to the aforementioned three nonkinetic "warfares" (Figure 1).



"Victorious warriors win first then go to war, while defeated warriors go to war first then seek to win" - *Sun Tzu*

Figure 1: Schematic depiction of the spectrum of engagement, with relative foci and loci of application and effect.

Moreover, following the collapse of the Soviet Union in 1989 (when the USSR possessed the world's second most powerful military), China changed its system of geopolitical power assessment to emphasize economics, foreign investment, technological innovation, and ownership of natural resources, while de-emphasizing military strength. In these efforts, China's political, commercial, and military institutions adhered strictly to the nine elements of the hundred-year marathon:

- Induce complacency to avoid alerting your opponent.
- Manipulate your opponent's advisors.
- Be patient for decades or longer to achieve victory.
- Steal your opponent's ideas and technology for strategic purposes.
- Recognize that military might is not the critical factor for winning a long-term competition.
- Acknolwedge that the extant hegemon will often take extreme, even reckless action to retain its dominant position.
- Never lose sight of *shi*—the guiding knowledge, principle, and/or force that establishes "the way" of power.
- Establish and employ metrics for measuring your status relative to other potential challengers.
- Always be vigilant to avoid being encircled or deceived by others.[7]

Adherence to *shi* was the most important element contributing to China's success, as it was (and remains) at the heart of Chinese strategy. This concept is somewhat difficult for Western societies to understand. Various Chinese translations describe it as "the alignment of forces," "propensity of things to happen," "to shape a situation," "to build up posture," "to assess the overall situation," and "to seek a balance of power."[8] Pillsbury has claimed that "only skilled strategists are able to exploit *shi* for ensuring victory over a superior force", and "only a sophisticated adversary is able to recognize how he is vulnerable to the exploitation of *shi*."[9] The United States and its Western allies could (or would) not fully comprehend the concept of *shi.* Consequently, they failed to recognize its role in China's geopolitical and military plans and activities. Arguably, this lack of recognition and understanding facilitated the decline of US and Western hegemony in global affairs.[10]

China predicated its strategic approach to global competition and power dominance primarily on deductive planning. The potential breadth and scope of the objectives that the country desired to achieved by 2049 served as the basis for retroactive planning to identify the actions necessary for achieving milestones and ecologies essential to the strategic end goal. In progressing toward 2049, China iteratively included

inductive planning to assure its ongoing efforts would align with established goals and milestones, as measured by successive evaluation of multi-domain successes.

The incorporation of long-term, nonkinetic disruptions were pivotal for inducing US complacency and keeping the United States from being alerted to China's real intentions. This accorded with the first dictum of the hundred-year marathon: *induce complacency to avoid alerting your opponent.* China achieved global-power dominance operationally through an articulate program and networks of cyber-hacking, employment of Chinese espionage agents inside and outside the United States, and numerous other penetrations of academia, industry, and military infrastructures. Philosophically and practically, China considered such theft and diversion of truth legitimate components of deception, especially if and when leveraged to attain its predominance of global power.

China's Efforts to Destabilize US Society

Synergizing these efforts were the implementation of numerous programs of broad-scale bio-socioeconomic disruption. For example, the importation of drugs (e.g., fentanyl and/or its precursors) had devastating impact and consequences on several dimensions and domains of US society; incurring hundreds of thousands of deaths, weakening the US economy both directly (i.e., in revenues devoted to care, treatment, and/or incarceration of the addicted) and indirectly (e.g., via greater than 20 percent diminution of the total US prime-age workforce because of drug addiction).[11] Further, drug addiction affected US military and governmental stability, as addicted individuals could not qualify for jobs in these sectors.

Much less visible but nonetheless effective, China directly (yet often cladestinely) funded US academia (and research), selected politicians, and media and entertainment industries. By quietly and sometimes secretly funding American academia, China gained deepened insight into S&T trajectories and therefore was able to invest in emerging sectors. This would prove to be both economically profitable and valuable in acquiring intellectual property rights in influential scientific, technological, industrial, and military capabilities. Additionally, China influenced social and political narratives, constructs, and perceptions of truth through both overt and clandestine funding of scholarly resources (i.e., academic/professional journals) and print, visual, online, and entertainment media. China's overall objective was to shape values, attitudes, and opinions of the next generations of US citizens and voters. Augmenting these efforts, China funneled money to select politicians for the purpose of shaping US (and other nations') political climate and postures.[12]

China understood and respected the global power and influence that American media and entertainment had achieved and enjoyed for decades. Therefore, it began developing its own film industry while simultaneously providing funding for the production and distribution of American films. Whereas English had historically been the default language for much of international media, the movies that China financed and/or helped to produce offered a variety of languages from which to select when

viewing. While subtle, this effectively informed and influenced audiences' perceptions that English was losing its prominence as the globally-accepted and -used language. Further, making Mandarin the accepted language of business and finance contributed to worldwide sentiments of China's multidimensional hegemony, which subsequently enabled the the yuan to replace the dollar as the global reserve currency.

China's stellar execution of its grand strategy and its strict adherence to the nine elements of the hundred-year marathon proved vital to its eventual success in replacing the United States as the sole global superpower. Focal to each and all these efforts was the maxim: *Be patient for decades or longer to achieve victory*. Although these enterprises were determined and perseverant, the United States' continual failure in and across multiple domains facilitated and ultimately guaranteed China's success. China repeatedly indicated its true intentions, goals, and objectives via dialogue and actions, but US governmental entities did not heed. Whether through hubris, ignorance, greed, or a combination thereof, the United States surrendered global hegemonic power despite being provided sufficient warning and ample opportunities to prevent such loss. The United States was unprepared for, and too slow to recognize and respond to China's escalating use of means and tools for mass disruption and the devastating rippling effects they incurred throughout several (and perhaps all) aspects of US society. US political and military leadership looked continuously for the proverbial "smoking gun" to reveal China's sponsorship and execution of these clandestine (and sometimes covert) activities. But given the intentional ambiguity of nonkinetic engagements, explicit evidence was absent. Thus, the motivations for and political and legal justification of US responsive action(s) were considered to be lacking.

US Failures, Chinese Successes

China executed successfully a series of "check and mate" maneuvers to establish and enable strategically latent assumption of global power. Changes in federal budgetary appropriations and allocations further impacted US ability to counter and/or avoid such multidomain "cornering." These budget cuts and redirections disempowered military and intelligence communities as well as key government and public resources vital to national security. This iterative loss of capability and effectiveness became evident to the US public and professional sectors. Consequently, the social contract Americans had historically maintained with their government (and its associated services) began to deteriorate quickly, and this decline became unstoppable. The denigration of confidence steadily progressed to the point where the majority of Americans lost faith in both their government and the ability of the US to sustain a leading role in global politics, economics, and balances of power.

Perhaps first among the United States' numerous failures was an inability to recognize the evolution of warfare. Even during the period of 2020-2030, the United States retained belief that it would likely engage China in a conventional (kinetic) force-on-force war in the Pacific. Given this focus upon kinetic warfare, the United

States continued to commit billions of dollars to fund equipment and technology (e.g., ships, aircraft, missiles, bombs, and bullets) for a war that was unlikely and, in fact, never occurred. The United States persisted in its dedication to a Clausewitzian (and somewhat Napoleonic) approach to war. This dogmatic view was wedded to an errant belief that a superior number and extent of technological assets would be the decisive factor in determining the outcome of any future conflict. Clearly, the United States had little regard for the fifth dictum of the hundred-year marathon: *Military might is not the critical factor for winning a long-term competition*. Such views and beliefs contributed to the United States' failure to recognize that China (1) had gone to war with the United States decades earlier, using nonkinetic, low-visibility engagements (pro Sun Tzu), and (2) had been winning decisively in this domain.

While the United States spent enormous sums for military equipment and assets, China allocated more of its gross domestic product toward S&T developmental efforts and global engagements. China's extant cultural values, philosophies, and somewhat different (and more permissive) ethics (i.e., than the United States and its Western allies) enabled a wider scope and accelerated pace of research efforts. China's rapid S&T achievements in artificial intelligence, big data, bioscience, and engineering eventually outpaced and surpassed those of the United States and its global allies combined. Fundamentally, China was more insightful regarding global conditions and vulnerabilities and, consequently, made better long-term strategic investments and decisions than the United States, if not "the West" at large.

In contrast, the United States maintained an antiquated, World War II–era perspective of warfare, and adhered to the institutionalized processes and thinking that had served it well from the 1940s through the 1970s. However, by the year 2000, these processes—especially the collective channelized thinking that accompanied them—became increasingly burdensome. In these ways, the United States repeatedly could not to respond effectively to being confronted with ever-more rapidly emerging threats and associated technologies. In essence, the United States became captive to its own bureaucratic rigidity and stagnation. It had lost the infrastructural systems and flexibility to promote and provide imagination, innovation, and creativity that in decades earlier had enabled it to challenge adversaries quickly and adroitly. Clearly, the United States no longer possessed the speed, dexterity, and purpose of action that once contributed significantly to its position as the definitive global superpower.

China effectively recognized and exploited vulnerabilities within US institutionalized governmental and bureaucratic processes. No US organization or agency was authorized to coordinate among and across other government organizations for integrated, comprehensive responses to grave national crises. Yet, US governmental and bureaucratic systems failed to identify or correct their inherent flaws in structure and function. This inchoate arrangement (and relative ineptitude) of organizational authorities and responsibilities further enabled China's success in executing serial and escalating campaigns of nonkinetic engagements against the United States.

The opioid crisis of circa 2010-2020 provided an example of how badly US governmental stovepiping failed the American people. In restrictingly categorizing the opioid crisis as a medical issue, rather than correctly identifying it as at least partly a nonkinetic chemical engagement or attack by China (via its proxy clients, the Mexican cartels), it was not clear which agency was in charge of, and responsible for taking action. These failures led to the disruption of multiple facets of US society and the ongoing loss of US capabilities. Whereas China had a grand strategy for shaping and directing its long-term enterprises to achieve global power, the United States lacked a counterpart strategy. Certainly, it had the National Defense Strategy and other, more tactically-oriented initiatives that were updated every few years, often with incoming presidential administrations, but these were focused primarily on preparations for conventional warfare. Thus, in keeping with outdated Western doctrine, the United States failed to appreciate or heed Sun Tzu's admonition that "tactics without strategy is the noise before defeat."[13]

The United States continued to embrace precepts of conventional force-on-force warfare, while China never deviated from strict adherence to the teachings of Sun Tzu that emphasized nonkinetic engagement as the most effective and efficient model for winning without fighting. But even von Clausewitz advocated the need for flexibility in preparing for and maneuvering on the battlefield. Simply put, the United States failed to acknowledge that Clausewitzian dictate, and in so doing, had forgotten how to change and foster reinvention to keep pace with (or outdistance) an adversary. Hence, the United States was doomed to become another second-rate nation, vying for position among many others in their dependence upon, and subjugation to, the prominent global superpower.

This vignette prompts the pressing question: *Is this scenario inevitable*?

Meeting Challenges and Seizing Opportunities

Now, let us turn back the clock: the year is 2020, and the United States is the dominant global superpower, but is quickly losing the lead in and across numerous domains. As noted in a series of US Army Science and Technology Trend reports, this is especially the case in S&T enterprises.[14] The United States government and polis recognize the need for strategic leadership and planning at the highest levels to maintain a position of predominant global power. However, implementing such leadership and plans remains uncertain; questions persist about how to effect such change, and where and how to begin. Long-established US processes, procedures, and policies inhibit (or prevent) the timely coordination of US governmental agencies and private-sector resources needed to respond to rapidly accelerating and ever-expanding emerging threats.

The extant partisan divide has led to a legislative quagmire that further exacerbates the situation. Is the United States prepared to identify, quantify, and respond to such risks and threats? We believe it is not. To reiterate, no evidence exists to indicate or imply that the COVID-19 crisis resulted from an intentionally

developed or deployed (weaponized) biological agent. Nevertheless, the crisis is a proverbial "shot across the bows," bringing into stark relief the inadequacies of US infrastructural coordination of biosecurity information, resources, and response. In many ways, we believe this bespeaks a larger, undergirding issue and problem. In a 2019 *PRISM* interview, General John M. Murray, commanding general Army Futures Command, stated:

> *[Russia and China's] concept of layered standoff—which we think is fundamental to their theory of victory—beginning below the threshold of war, sees constant competition below that threshold. We have seen it in Ukraine, the South China Sea, and the Baltics; all attempting to achieve strategic objectives below the threshold of war. In Western society we tend to see long periods of peace interrupted by short periods of war as the norm, while many of our adversaries see the world in constant competition—not necessarily always military, but through all elements of national power; diplomatic, information, economics, as well as military. That's a different kind of world perspective. . . . In a different way, they are achieving many of their strategic objectives below the threshold of war.*[15]

General Murray references Russia's and China's intent and capabilities to exercise power in non-traditionally bellicose ways, so as to avoid conventional kinetic armed conflict with the United States, while simultaneously attempting to achieve strategic objectives via constant competition in what is known as phase 0. Phase 0 is the domain of preconflict in which strategically-oriented efforts incur war disguised as peace. As General Murray stated, "as long as they can continue to achieve objectives below the threshold of outright war, what is needed is a whole-of-government effort to counter it."[16]

Arguably, the United States disadvantages itself by not appreciating, and not engaging, the ways that nonkinetic enterprises can be used to achieve national strategic objectives. Further, by employing all elements of national power, a whole-of-nation approach can be exercised, which extends (i.e., force multiplies) the activities of whole-of-government efforts. Of course, and as the COVID-19 crisis has illustrated, whole-of-government coordination and cooperation is essential both to initiate and sustain whole-of-nation enterprises of preparedness and response. To be sure, the old adage, "an ounce of prevention is worth a pound of cure" aptly applies, as such coordinated, collaborative preparedness is far more conservative—and conservational—of economic and human costs than stalwart, conflictive competition.

Principles of, and preparedness for, kinetic warfare do not necessarily or appropriately apply to addressing, mitigating, or preventing nonkinetic threats, especially those that occur in phase 0 preconflict conditions. As we have noted previously, nonkinetic engagements are not intended for "destruction" in the classic

sense, but can and should be regarded as efforts toward disruption, intended to exert rippling effects that destabilize nations, societies, and populations and, in these ways, gain purchase to affect economic, sociocultural, political, and power capabilities and relative global position and security.

Therefore, as the COVID-19 crisis has revealed, whether a naturally occurring pandemic, a bioengineered contagion, or the leveraging of key bio-psycho-socio-political vulnerabilities in infrastructure and function, disruptive effects can evoke devastating multi-domain and -dimensional impacts. In sum, COVID-19 has brought to light US inadequacies and vulnerabilities in biosecurity and other factions of threat preparedness and response that could be exploited via nonkinetic means and engagements.

Despite such trends, it still may be possible for the United States "right its ship," but the time for such action is quickly expiring. Certain government and military sectors recognize that the United States is consistently reactive, instead of proactive, in recognizing and responding to emerging threats. Some consensus exists that the established processes, procedures, and policies will need to be modified or changed completely to enable the speed and breadth of action required to address evolving challenges expediently, efficiently, and effectively. The United States possesses the organizations required for such efforts, but these resources tend to be operationally stovepiped and constrained by their specified authorities and responsibilities. Therefore, an existing organization, or new entity, must be empowered with cross-organizational authority to coordinate the activities of the Department of Defense, the intelligence community, the Department of State, the Department of Justice, the Department of the Treasury, other governmental agencies, and private-sector institutions and resources toward developing and executing enterprises to limit or prevent these emerging threats.

Within this effort should be an accompanying strategic narrative articulating the necessity of employing all elements of national power to achieve long-range national objectives (as the US principal strategic competitors articulate currently and effectively). It would be foolish to presume COVID-19 will be the last pandemic to occur. Also, we believe it would be equally unwise, if not remiss, not to expect rivals to recognize and attempt to exploit vulnerabilities in US, and international, systems and functions for biosecurity and national stability. To prepare for and mitigate, if not deter such threats, we propose establishing a Joint Interagency Task Force (JIATF) along with a Program Management Office and/or a Program of Record for executing, supervising, and administering a whole-of-nation approach to maximize efforts in national security to meet both natural threats and those of intentional origin and deploy. A prudent, cost- and resource-efficiernt redirection and deployment of SOF—and its associated and derivative organizations—may serve as both "tip of the spear" in key elements of surveillance and interdiction (i.e., mitigation and prevention) in the nonkinetic domain. Indeed, COVID-19 has fostered a crisis. We opine it is important to take the term "crisis" in its literal sense—a time of change—and use this challenge as an opportunity for a call to colors.

Endnotes

1 Coats D. Report to the Special Senate Committee on Intelligence, January 2019.

2 Pillsbury M. T*he Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower.* NY: Griffin, 2016, 12.

3 Pillsbury, *The Hundred-Year Marathon,* 12.

4 Muñoz Arturo. Intelligence in Public Media: Review of *Lever of Power: Military Deception in China and the West* by Ralph D. Sawyer. Studies in Intelligence 62(3), 2018.

5 Sun Tzu. *The Art of War*. London: Chartwell, 2011.

6 Anderson, E. C., and J. G. Engstrom. China's Use of Perception Management and Strategic Deception. US-China Economic and Security Commission Report, November 2009. https://www.uscc.gov/research/chinas-use-perception-management-and-strategic-deception Accessed 15 May 2020.

7 Pillsbury, *The Hundred-Year Marathon,* 35-36.

8 Pillsbury, *The Hundred-Year Marathon,* 42-43.

9 Pillsbury, *The Hundred-Year Marathon*, 42.

10 Pillsbury, *The Hundred-Year Marathon,* 42.

11 Gitis B. "State by State: The Labor Force and Economic Effects of the Opioid Crisis," *American Action Forum,* September 2018.

12 Coats, *Report to the Special Senate Committee on Intelligence*, 2019.

13 Sun Tzu, *Art of War,* 2011.

14 Office of the Deputy Assistant Secretary of the Army (Research & Technology). *Emerging Science and Technology Trends: 2017-2047. A Synthesis of Leading Forecasts.* November 2017; Office of the Deputy Assistant Secretary of the Army (Research & Technology). *Emerging Science and Technology Trends: A Synthesis of Leading Forecasts*, 5th Ed. March 2019.

15 Miklaucic, Michael, "'Thinking about What Could Be,' An Interview with General John M. Murray, Commanding General, Army Futures Command," *PRISM* 8 no. 3, January 11, 2020.

16 Miklaucic, "'Thinking about What Could Be,'" 2020.

CHAPTER 9

Cyborg Soldier 2050: Human-Machine Fusion and Its Implications

Diane DiEuliis and Peter Emanuel

As the worlds of digital machinery and biology continue to intersect, and the pace of discovery in biotechnology accelerates, the potential for altering human beings is also growing—creating both promise for and concern about the possible outcomes. The latent ability to alter physical or behavioral human attributes as they pertain to warfighters, particularly special operators, is generating both operational opportunities and ethical concerns, at the levels of both the individual warfighter and the Department of Defense (DOD). Few guidlines have been conceived for operational or ethical decision-making regarding altered human performance, largely because of the lack of studies on potential human performance futures and how they should be assessed in the context of special and DOD operations.

This chapter describes the results of a year-long study representing a first foray into forecasting and evaluating specific prototype human-machine interface capabilities likely to be introduced between 2030 and 2050. To conduct the study, a team of 75 scientists, engineers, lawyers, ethicists, and military personnel came together to frame the issues, conduct reviews of current and future research, and hosted site visits with subject-matter experts across the nation. The study team sought to evaluate strategic operational, ethical, legal, and societal implications (ELSI) of cyborg technology for the military. The study team used use the term "cyborg"[1] purposefully, as we predict an acceleration in the convergence of man and machine between 2020 and 2050. The cyborg technologies we assessed go beyond augmentation—those used to restore function from injury or disease—to those capable of enhancing performance (through a range of modifications, from the functional to the radically structural) beyond the normal baseline for the human population.[2] We also assume genetic engineering, synthetic biology, nanotechnology, artificial intelligence, or any number of emerging and converging technology fields will enable aspects of cyborg capabilities.

This chapter identifies four potential future military-use cases for cyborg technologies and assesses their impact on DOD's organizational structure, warfighter doctrine and tactics, and interoperability with allies and civil society. It offers a framework through which any variety of potential performance enhancements can be assessed and a set of recommendations for DOD in the short term to prepare for this latent future.

Selection and Assessment of Case Studies

Given the broad and exploratory landscape of human-machine interfaces, the study team determined it would be more impactful to select case studies relevant for

defense considerations. We developed individual case studies based on technologies capable of enhancing human performance either now or potentially by 2050. They represent both predicted technology and concrete examples to illuminate and discuss operational and ELSI concerns. We prioritized individual capabilities of a soldier from most to least impactful on a warfighter's battlefield performance when enhanced above baseline performance:

- Situational awareness
- Strength and speed
- Imaging and sight
- Communication
- Physiology (endurance/sleep/health)
- Virtual (avatar) control
- Attention and memory
- Learning
- Sense of smell

These priorities informed the development of four vignettes based on emerging global trends in human-machine enhancement research.

Case Study 1: Ocular Enhancement for Imaging, Sight, and Situational Awareness

Army analysts project battlefields in 2050 will be dense urban environments or subterranean megacities that will challenge target identification and tracking. In these scenarios, a warfighter's vision is enhanced to enable sensory perception beyond the normal visible spectrum, which combine with computational capabilities that

would allow for target identification, selection, and data sharing with other individuals or military systems. Enhanced individuals would have the ability to analyze images from various wavelengths atop one another to better discriminate targets and allow identification in complex and cluttered environments.

Ocular enhancement would offer small dismounted teams the ability to acquire and share data in real time. Fast-moving expeditionary units could employ enhanced individuals as part of teams engaged in a multidomain battle space in which communications will likely be contested or denied. The enhanced individual would be part of the expeditionary unit and capable of performing functions autonomous of external data feeds, thus providing intelligence data drawn from multiple sensory-fusion inputs. In short, the individual possessing the ocular enhancement would provide the squadron with a portable sensory-fusion capability.

The enhancement technology could manifest itself in one of two ways. In the first scenario, an ocular enhancement system could overlay existing ocular tissue, retaining use of the retina (similar to ongoing research to treat adults with advanced retinitis pigmentosa). Such capabilities will likely be available and mature by 2030, given current research efforts.[3] A second, more complex scenario, would require complete replacement of the eye, with data feeds passing directly into the optical nerve bundle. In this enhancement, anticipated to be mature by 2050, the sensory input for visualization is completely mechanical or electronic in composition, allowing data feeds of all types and across all spectra, including those previously not capable of being visualized by humans.

It is unlikely individuals would willingly undergo removal of healthy tissue in a sensitive area, so ocular enhancement would be an attractive medical option for those with eye tissue damaged or destroyed by injury or disease. Further, given the critical role vision plays in society, warfighters who have lost part, or all of their vision, might be motivated to undergo voluntary surgery that could restore or even improve their ability to visualize the world beyond their service in the military.

Case Study 2: Restoration and Programmed Muscular Control through Optogenetic Bodysuit Sensor Web

Musculoskeletal injuries represent the second leading cause of lost duty time in the US armed forces,[4] and warfighters and special operators perform increasingly challenging tasks that push them to the limits of their physical capability.

In this scenario, a network of subcutaneous sensors deliver optogenetic stimulation through programmed light pulses to enhance muscle control. An optogenetic control network could be employed to restore muscle or nerve function in the wake of an injury. It could also allow warfighters to interface with external systems not permanently adhered to their bodies or control their bodies to perform complex tasks for which they are not trained or accustomed. Ongoing efforts to develop warfighter exosystems to reduce energy expenditure has revealed that current technologies often impede operator performance and increase metabolic costs.[5] An

optogenetically controlled bodysuit could better sense the human state and provide a real-time interface between the human and the exosystem. This human enhancement would allow dynamic adaptive coupling of the human body with an external exosystem, leading to more stable and agile physical behaviors, and optimize energy expenditure in operational environments.

The enhancement is best described as an implanted digital sensing and stimulation system coupled with external sensors (e.g., boot inserts and wearables), all of which link to a central computational controller. In effect, the human body would have an array of small optical sensors implanted beneath the skin in the body areas that need to be controlled. This could manifest as thin optical threads placed at regular intervals over critical muscle and nerve bundles and linked to a central control area designed to stimulate each node only when required to recruit the muscles below it. Optical control would occur across the network of optical threads in a programmed manner to effect a fluid muscular action in a choreographed "dance." Such a network of implantable muscle sensing, computation, and stimulation provides a closed-loop suite that could be used to decrease injury and mortality rates for soldiers through automated hazard avoidance, while enhancing their physical capabilities on the battlefield.

Case Study 3: Auditory Enhancement for Communication and Protection

Battlefield-associated hearing loss resulting from acute or prolonged exposure to high-intensity sounds such as gunfire, explosions, or military machines is one of the most prevalent service-connected disability for US veterans. A 2012 study suggests that ~10 percent of veterans suffer from tinnitus, while ~6 percent have been diagnosed with some level of hearing loss.[6] Existing technology such as the Army-sponsored Tactical Communications and Protective System affords some protection but does not offer enhanced capabilities to the user.

In this proposed enhancement scenario, enhancement of auditory capabilities would occur by replacing or modifying the middle-ear bones and the cochlea, affording a more dynamic hearing range, both to protect from high-intensity noises and to increase sensitivity to low-amplitude sounds. As the technology matures, it could expand the range of sensory perception to infrasonic and ultrasonic levels, allow for positioning and localization from passive sensor transmissions or echolocation, and create advanced communication capabilities.

Given this technology requires invasive ear surgery, it would be used only for individuals with significant hearing loss. Direct replacement or modification of both inner and middle components would be irreversible, and therefore those with healthy auditory capabilities would be unlikely to accept this type of enhancement. Advances in external processor capabilities and minimally invasive electrode implantation in neural networks could make these technologies more accessible to the general population by 2050.

For military personnel, auditory enhancements would afford protection from high-intensity noises, provide a wider dynamic range of detectable sounds, and afford integrated communication capabilities. In the near-term (2020 to 2030), the study team anticipates the enhancement will be coupled with networking capabilities and used to track human detection of salient objects in an acoustic environment. In squads with limited enhanced personnel, the enhanced individual(s) would detect salient auditory information in the environment and relay it to other squad members using conventional forms of communication. For squads with multiple enhanced individuals, acquisition and distribution of auditory cues to spatially separated individuals could direct attention across an entire squad to actionable stimuli.

Later iterations of auditory enhancements would likely target two key areas: 1) the capability for communication via imagined or covert speech, and 2) significantly less invasive and/or reversible implants. In regard to imagined speech, within this extended timeline (2050), significant advances in the understanding of neural pathways will enable not merely improvements to an individual's auditory signal transduction but also conversion and transmission of these signals to others across distances.[7] This capability could lead to increased acceptance and adoption of this enhancement in areas outside the military, such as by intelligence officers, police forces, and others who would benefit from using imperceptible forms of communication. Technologies that allow real-time translation of multiple languages would be useful to military operators, as well as civilians.

Case Study 4: Direct Neural Enhancement of the Human Brain

Remote weapon systems and/or unmanned vehicles have increasing prevalence on the modern battlefield. Vehicle and infrastructure-associated remote weapon systems allow for operators to control the battlefield while remaining some distance away in relative safety. Similarly, unmanned vehicles will play an invaluable role in reconnaissance and long-range targeting of enemy infrastructure, equipment, and

personnel. Our current state of technology allows remote weapon systems and unmanned vehicles to be controlled by work stations that can be either fixed or portable. While effective, these current systems are limited by the complexity of user interfaces and limited information that can be conveyed to the user.

In this scenario, neural implants for brain-computer interfacing (BCI) would allow for seamless interaction between the individual and secondary assets (i.e., machines). This control could extend to drones, weapon systems, and other remote systems controlled by an enhanced operator. The enhancement would not simply entail user control of equipment (brain to machine) but also transmission to operator (machine to brain), and human to human (i.e., command-and-control dynamics) to enhance situational awareness as drone, computational-analytic, and human information is relayed to the operator. Neural enhancement through implantation of modulatory electrodes in the brain will allow for rapid interaction between machine and operator via a read/write type of mechanism.[8] These enhancements will enable the enhanced operator to have rapid and integrated control of multiple assets by improving battlefield awareness and warfighter lethality.

As this technology matures, the study team anticipates specialized operators will likely be utilizing neural implants for enhanced operation of assets by 2030. These operators will include special forces teams, military pilots, UAV/USV-drone operators, and intelligence personnel.[9] By 2050, scientists will make significant advances in the understanding of the neural network and neural implant technology, enabling deployment of these technologies to military forces for use-controlled operation of weapon systems, network communication and interaction (e.g., corpspeople speaking with doctors or specialists in hospitals to aid in field treatments of combat injuries), and improved warfighter awareness through machine-to-brain (and machine-enabled remote brain-to-brain) communication via the use of distributed sensors, transmitters, and reconnaissance drones.

For the warfighter, neural implants would have broad battlefield applicability. External processors and transmitters would allow for interaction with battlefield assets (weapon systems, reconnaissance drones, UAV/UMVs) as well as personnel both within proximity and across distances through hierarchical relays with a central network. Early deployment of BCI to enhanced individuals would be limited to small-scale specialized teams where one or more enhanced personnel would offer squad support through asset control. The level of invasiveness of early iterations and the potential irreversibility of these implants may limit acceptance by military personnel and society, although specialized teams (e.g., Navy SEALs, US Army Rangers) may be more inclined to accept these technologies if they could provide significant improvements in capability, lethality, survivability, and overall battlefield superiority.

Improvements in neural implant technology could be significant by 2050. Anticipated improvements would focus on reducing the level of invasiveness of the implant itself. This could be accomplished through location-specific assembly of electrodes using biocompatible nanoparticles that can be directed via an external force (doped iron-oxide nanoparticles that can be positioned through the use of directed magnetic fields) or through improvements to the signal-acquisition capabilities of externally placed electrodes and processors. The study team expects warfighter needs will influence these technological advancements; however, such advances would plausibly lead to revolutionary changes in how society interacts with machines on a daily level. Technologies such as personal robots, entertainment options, and vehicles would be driven and sustained by commercial entities.

Case Study Analysis

Societal Perceptions as Either Impediments or Drivers of Cyborg Soldiers

Our study considered whether near-peer competitors/adversaries' would be willing to pursue genetic alterations or invasive human-machine enhancements the United States would be more hesitant to conduct, because of differing ethical frameworks, regulatory requirements, or social attitudes. For example, in 2017, Chinese researchers manipulated myostatin genes in canines to increase their musculature several fold, resulting in what many considered a prelude to the potential creation of "super soldiers."[10] Another Chinese research team added more fuel to these concerns when it announced the germ-line manipulation of human embryos for the stated purpose of avoiding HIV infection passed from parents.[11] Months later, a Russian scientist claimed he intended to implant gene-edited embryos into women.[12]

Current DOD perceptions about near-peer adversaries' strategic intent are based on such anecdotes. While we know both China's political and military institutions are involved in all aspects of technology research and development[13] and China maintain explicit differences in cultural values and norms governing the conduct of research,[14] researchers have not assessed systematically global perceptions on the ethics of human enhancement. To what extent, if any, are the research-and-development

(R&D) activities of different regions of the world constrained by different moral codes or swayed by popular regional opinion? What characteristics—such as education, religious beliefs, or doctrine—affect willingness to allow advanced technology to enhance the human condition, and to what extent do these attitudes among members of the public impact the activities of a particular government?

The Pew Research Center concluded a survey of 4,726 people within the United States to understand domestic attitudes toward human-enhancement technologies.[15] They examined public attitudes about three emerging technologies that could improve human health, cognitive abilities, or physical capacities. The study revealed the majority of Americans greet these technologies more with wariness and worry than enthusiasm and hope. For example, a majority of US adults say they would be "very" or "somewhat" worried about brain chips (69 percent) and synthetic blood (63 percent). Some said they would be both enthusiastic and worried, but, overall, concern outpaces excitement. Opinion is closely divided on the fundamental question of whether these potential developments are "meddling with nature" and cross a line that should not be crossed or are "no different" from other ways that humans have tried to better themselves over time. People's views differ depending on how religious they are; on average, more religious Americans are less affirming of these enhancements than those considered less religious, who are more inclined to see use of these techniques as the continuation of a millenia-old quest by humans to try to better themselves.[16]

The Pew Research study results suggest an American's willingness to accept or reject a human enhancement technology is associated with their understanding of the technology and their degree of religious commitment. Comparable data from other

countries is not available, and near-peer adversaries like China exert heavy control over information sharing, making data collection challenging. Moreover, the attitudes and opinions of the general public do not necessarily represent what government authorities or research teams are willing to pursue. Therefore, US leadership has little data about what other countries' societies, scientists, governments, or military leaders would support. Value exists in understanding societal awareness and global perceptions of human-machine enhancement technologies because it can be used to predict where adoption cyborg technologies may be difficult to introduce and where adversarial adoption of offset technologies is likely to be more readily accepted.

Interoperability and the Politics of Enhanced Soldiers

Our subject-matter experts expect commercial medical applications will accelerate the pace of development of cyborg technologies between 2020 and 2035; thus, defense forces around the globe will likely adopt them apace. Adoption of new and potentially sensitive technologies will have implications for interoperability of military forces. However, interoperability of military units in a tactical sense is not the only hurdle that must be overcome when bringing together populations from different countries. Countries base their policies on the shared social norms and beliefs of the population, which may or may not align on the issue of human-machine enhancement technologies.[17] The aforementioned Pew Research study suggests allies with strong religious demographics may be more reluctant to accept foreign cyborg soldiers operating on a shared military base within their borders. Based upon current postures of key strategic competitors,[18] the global community will likely not establish consistent and harmonized approaches to integrating human-machine enhanced warfighters; the lack of harmonization will present challenges to the deployment of these assets in the years leading up to 2050. A robust multinational dialogue that identifies acceptable legal, moral/philosophical, and ethical frameworks for deploying these technologies in national defense may prepare the global communities for these eventualities.

Beyond allied acceptance and military interoperability, international political costs exist for fielding cyborg military assets. State and nonstate adversaries will seek to undermine DOD by portraying the United States as deploying technology unethically.

Demographics such as religion and political affiliation are anticipated to be a platform used to galvanize these arguments, with entertainment and social media reinforcement. Mass media, including film and literature, is a known stage for demonizing cyborgs. From *Frankenstein* to *Terminator*, popular media often depict technology's integration with the human body as robbing the human spirit of compassion and leading to violence and grave unintended consequences. In the name of entertainment, popular social and open-source media, literature, and film have often distorted or portrayed in dystopian narratives the use of machines to enhance the physical condition of the human species.

However, fiction can also reflect positive applications of emerging technologies or be a powerful tool for engaging the public in bioethics discussions.[19] More accurate

depictions of technology and its applications in both fiction and nonfiction media could lay the groundwork for a new generation who see opportunity for societal benefits in cyborg technologies. As technology increases the possibility for human physical enhancements, DOD must help alter distorted cultural narratives. A more realistic, balanced (if not more positive) narrative will serve to better educate the public, mitigate societal apprehension, and remove barriers to productive adoption of these new technologies. Although this is not intrinsically a DOD mission, defense leadership should understand that if they intend to field these technologies the public must understand and overcome misperceptions.

Legal and Privacy Implications for Cyborg Technologies

As many legal scholars will attest, current legal frameworks that govern the use of technology—including cell phones, email, and social media—are inadequate. As the pace of technological development accelerates and human-machine enhancements achieve reality in the years leading up to 2050, legal frameworks will almost certainly continue to be outpaced. In a 2014 study, "Our Cyborg Future: Law and Policy Implications."[20] Benjamin Wittes and Jane Chong discuss how the prolific use of cell phones and wearable devices brings technology closer to the human race and suggest we are, in effect, approaching a state in which we are "juvenile cyborgs" already. They suggest a more important and unique legal challenge associated with man-machine enhancements is the data generated by the machines:

> *The first consideration that must factor into our discussion is that cyborgs inherently generate data. Human activity by default does not—at least, not beyond footprints and fingerprints and DNA traces. We can think and move without leaving meaningful traces; we can speak without recording. Digital activity, by contrast, creates transactional records. A cyborg's activity is thus presumptively recorded and that data may be stored or transmitted. To record or to*

transmit data is also to enable collection or interception of that data. Unless one specifically engineers the cyborg to resist such collection or interception, it will by default facilitate surveillance. And even if one does engineer the cyborg to resist surveillance, the data still gets created. In other words, a world of cyborgs is a world awash in data about individuals, data of enormous sensitivity, and, the further cyborgidization progresses, ever-increasing granularity. Thus, the most immediate impact of cyborgidization on the law of surveillance will likely be to put additional pressure on the so-called third-party doctrine, which underlies a great deal of governmental collection on transactional data and business records. Under Third Party Doctrine, an individual does not have a reasonable expectation of privacy with respect to information he voluntarily discloses to a third party, like a bank or a telecommunications carrier, and the Fourth Amendment therefore does not regulate the acquisition of such transactional data from those third parties by governmental investigators.[21]

The authors argue further that the more essential the role machines play in our lives, the more integral the data they produce are to our human existences and the more inextricably intertwined the devices become with us—socially, physically, and biologically. If this is true, what are the implications for the enhanced individual? Further, what are the implications of these data when they are generated by warfighters and special operators? Who owns such data, and for what purposes can they be used? From a legal perspective, an enhanced human will likely find themselves generating huge amounts of data that makes them uniquely susceptible to targeting and surveillance, and legal frameworks, structured currently, cannot to do anything about it. Further, the data could be hacked by adversaries for harmful purposes.

Cyborg technology will also collect data from those around the enhanced individual. Some of the technology predictions within this study envision human-machine enhancements in which audio, video, geolocation, and time stamps would all be recorded and distributed. From a national security perspective, this enhances situational awareness and clearly has military applications. But in a civilian setting, like in a coffee shop or the gym, it will have other implications, including impact on bystanders. Even if an individual volunteers for enhancement and any corresponding collection of their personal data, bystanders are unlikely to have granted the same permission. Some likely scenarios to consider include:

- Are an enhanced individual's capability to monitor, record, and communicate conversations and images bound by the same legal frameworks that govern wiretapping and privacy laws for cell phones and other recording devices?
- If an enhanced warfighter is caught and captured, do they have the same protections under the Geneva Convention, and will their enhanced status alter the treatment they are likely to receive?
- Can a person be prevented from having or using an enhancement under special circumstances (e.g., entering a bank or sensitive compartmented information facility [SCIF], gambling in a casino, taking a test, or negotiating a contract)?
- Can an employer discriminate against hiring an enhanced—or unenhanced—person? Can a business refuse to serve? If an employer desires the enhanced individual, can they be paid more for their services?
- Is the misuse of enhanced technology on the part of an employee grounds for deactivation or removal of the technology?
- Is there a legal precedent for passing laws that restrict or modulate technology integral to our bodies?

- Who is liable for any accidents caused by malfunctioning of the technology?
- Can a person sign away legal authority or control over something inside their body (i.e., akin to a delegation of authority/responsibility)?
- Will people be required to disclose the presence of enhancements within their bodies? If so, when, why, and to whom?
- Can someone be screened to reveal an enhancement that is *not* visible through the use of a metal detector or body scanner? What is the expectation of privacy for both enhanced individuals and people interacting with them?

Current legal frameworks are insufficient to predict the myriad challenges to privacy and security that will arise from these situations. The DOD should explore the development of dynamic legal, security, and ethical frameworks that anticipate these questions. Forward-leaning policies, both internal and external to the department, should protect privacy, sustain security, and manage personal and organizational risk. Because a core DOD mission is the operationalization of technology for national security, these frameworks should be agile and responsive to new technologies, whether developed in the United States or elsewhere. Moreover, frameworks should be adaptable to the entire lifecycle of technological advancement, from early-stage research through fielding and operational use.

Safety and National Security

Cyborg technology might be classified as a threat; it is almost impossible to detect, difficult to deter, and challenging to defend against. If the strategic landscape advances sooner than expected, or contains ambiguous threats against which we lack capabilities to detect and defend, the balance of power, as well as the very definition of "asymmetric warfare," will be altered. The introduction of human-machine enhancements into military and civilian populations will create new vulnerabilities that will need to be mitigated by security architectures. As noted above, cyborg individuals would automatically record images and audio or generate geographic coordinates and time stamps; they will, in effect, create "transactional records,[22] enabling collection or interception of that data. Unless one specifically engineers the cyborg to resist such collection or interception, it will facilitate surveillance by default. Relatedly, because of their surveillance capabilities, cyborgs could be selectively tracked and targeted unless proper shielding is undertaken.

From a national security perspective, adversaries may piggyback surveillance and tracking technologies onto implanted cyborg technologies. In the words of one study participant, "If I can't walk into a [SCIF] wearing an iWatch or carrying a cell phone, how will security be confident it is safe to allow a cyborg to walk in there?"

Machines respond to commands, and if command-and-control systems are hacked, the human-machine will be compromised. External hackability could generate the fear

of control by others. Even if this risk can be mitigated through enhanced encryption methods, variable authentication requirements, or other methods, the perception that control could be subverted might lead to issues of trust among peers. For example, if a hostile actor could override an optogenetic bodysuit or neural implant that controls muscle movement, this could not only create a true threat to the individual, organization, and mission but also promulgate fears among the ranks of both unenhanced and enhanced alike.

Lastly, these advanced technologies will be able to travel the world outside of traditional exploitation-preventative security controls. Technology ownership and chain of command of an enhanced soldier is nontraditional (e.g., an enhanced soldier plans a vacation to foreign countries, posing diplomatic and security risks). Thus, individual user must trust the system will perform reliably and sustainably—i.e., that the system has been verified and validated—in and across a range of settings and circumstances. In short, an enhanced soldier with a machine interface presents a potential multilevel security risk in need of mitigation.

Military Opportunities to Enhance Capability

Human augmentations and enhancements carry with them a number of security and privacy concerns at both the national and global societal level. These technologies, however, also offer significant advantages to the DOD and other national agencies. In addition to enhancing warfighter performance, these technologies have many technical applications with the potential to improve warfighters' survivability significantly, allowing them to operate safely and securely in austere environments.[23] One could argue that failure to invest in the responsible development of these potentially lifesaving technologies would be unethical.

With variable combat environments, conditions, and adversaries, military technology is advancing rapidly to provide enhanced situational awareness to warfighters. DOD forces regularly deploy a wide array of unmanned aerial and/or

marine vehicles (UAV/UMV) to collect data and relay it back for assessment. UAV-gathered intelligence is often collected at a central location and then disseminated to forward operators through conventional communication networks, which can prove limiting in some situations. As discussed in vignette 4, neural enhancements—portable independent communication systems both between squads and squad members, as well as with computer systems themselves (such as UAVs)—could enable warfighters to operate "off of the cloud" or "on the edge." In a multidomain battle space where fast moving expeditionary forces will contest communications and movement, these types of portable communications could lead to enhanced targeting, tracking, and situational awareness organic to the squad level, thereby enabling rapid decision-making and operational flexibility.

The ability to passively record environmental situations and personal interactions and observations without external equipment or devices would also be invaluable to clandestine surveillance. In dense urban environments, operators would be able to move seamlessly through crowded city streets capturing environmental intelligence, targeting conversations, and acquiring other valuable information that would be digitally stored for later analysis and interpretation. Additionally, while clandestine operators are trained to capture and remember key details, digital (audio and visual) recordings can capture minute details that may be missed by even the well-trained eye.

Safety Concerns and Benefits

For any enhancement or augmentation, safety is a critical issue, and, challengingly, the cognitive and physical effects of these technologies cannot be known fully a priori. The DOD must support rigorous science in these domains, not only to validate usefulness of the technologies but also to identify and prevent short- and long-term harms. Even when measures are taken to ensure the highest level of safety for the end user of these technologies, each human's physiology is slightly different, and the technologies could result in unforeseen side effects. DOD personnel, especially those at the "tip of the spear" (e.g., SOF), are prone to seek an advantage over adversaries even if the chosen technology has not been shown to be fully effective or nonhazardous (e.g., the use of dietary supplements by SOCOM). Although speculative at this stage of development, the early adoption of low technology-readiness-level (TRL) enhancements to keep up with enhanced adversaries may prove an area of concern in the future. Given DOD's particular needs and applications, many of these enhancements will likely be unique to the DOD; therefore, collection and accrual of data to validate the utility, and establish the safety, of these technologies may be more difficult than in the civilian sector, where more opportunities exist to collect data or conduct studies with sufficient sample size. Also, long-term side effects will likely be unique to each augmentation. The remapping of neural networks resulting from an implant will be vastly different than muscular stimulation via optogenetic implants. Each implant type, location, and mode of action will carry its own safety and regulatory concerns.

Human enhancement and augmentation could be implemented as a viable technology in DOD personnel for the sole purpose of adding a competitive edge to and improve survivability of warfighters. Each of the technologies we have discussed have the potential to offer improved situational awareness through 1) enhanced sensory perception, 2) streamlined interaction with assets such as UAVs and sensors, and 3) improved communication between squad members, which would directly translate into improved warfighter performance and safety through "left-of-bang" approaches. While these examples would provide more tangible and predictable safety enhancements, secondary benefits could also be possible based on current understanding of neural plasticity and overall brain function. For example, studies of Alzheimer's dementia have shown early and frequent brain stimulation leads to reduced plaque formation in aging populations.[24] It is possible enhancements that rely on a neural implant or other method of brain stimulation may increase overall brain activity, leading to slowed aging of neural pathways and long-term benefits to individuals with these types of enhancements. Many of these technologies will incorporate some sort of biometric log to ensure the stability of the implant. As has been discussed elsewhere, these logs could allow for numerous biomarkers to be monitored, which could lead to early recognition not only of implant degradation and/or failure but also other disease states (or conditions that the recipient may experience or develop during their lifetime). By revealing actionable medical information that would not otherwise be detected, the enhancement may provide a safety benefit to the individual.

Long-Term Effects of Human-Machine Fusion

Enhancement technologies may be integrated intimately within the human body and enable decades of exchange information with the human nervous system. As mentioned, long-term effects on the human body (and cognitive and/or psychological functions) cannot currently be wholly foreseen, and will need to be determined through rigorous prospective studies. Once short-term safety and efficacy have been demostrated, initial deployment would likely be in small specialized teams monitored extensively both during and after military service. These specialized teams could serve as "probe cohorts" to enable ongoing evaluation of benefits, burdens, and potential harms incurred by such interventions. While the targets will be ever-evolving, we discuss below some of the questions and concerns that will need to be addressed.

Many of the enhancements described here and possible by 2050 will require us to to deepen our understanding significantly both of the brain and how to engineer technologies affecting its structures and functions. Most cyborg technologies will likely require a neural component/implantation to allow efficient utilization, which will require a massive two-way data feed to/from the brain, as scientists develop iterative methods and techniques to "learn" proper placement of implants and to accommodate vast types and amounts of data required to sustain these technologies' optimal functioning. We do not know yet how the use of integrated technologies will affect existing brain architectures and functions; arguably, we can know this only by

implementing the particular intervention(s) in question. Augmentation of individual senses may have secondary consequences for multisensory integration and sensory motor coordination and will require information displays that can be digested by the human brain without causing spatial disorientation, negative impacts on coordination, and disequilibrium.[25] Furthermore, if these data streams become corrupted, improper sensory relays and interpretation could lead to poor or incorrect decision-making by the operator. For example, an operator could falsely identify of targets, leading to friendly fire. Would this lead to a "my implant made me do it"—type defense where technology is blamed for such actions and mistakes?

With age, the tissues, integrity, and functions of the human body change in relative capability, plasticity, and sustainability. We do not yet know whether and/or how implants will change the rate, extent, and effect(s) of aging, or the influence and manifestations of the implants over time. In the long-term, the body might lose it ability to interact with the implant as neural connections degrade or muscles and connective tissues change or atrophy. Will an individual who receives these enhancements during their years of service become even more infirm later in life as their body and implant ages? Can enhancements be recalibrated as the body ages to restore functionality, or at least ensure operability at some basal level? Or, will the technology provide some measure of protection against or mitigation of aging effects, thereby rendering the enhanced individual with durable capabilities?

Active Military Considerations

Our study team projects the Integration of enhanced troops into warfighter populations will increase in frequency as we approach 2050, and these populations will persist for extended periods of service. This "new normal" will require changes in the way the DOD recruits, trains, deploys, and protects troops and systems under its span of control. At present, all soldiers and support personnel constitute a significant DOD

investment. This is not just an investment in the equipment and training, but also in the in-service and long-term postservice care. The total life-cycle cost in enhanced personnel will require a change in the way the various branches of the DOD organize and position individuals in their command.

- Does this create new quid pro quo service criteria? For example, should the DOD mandate substantially longer commitments of service for enhanced individuals if the DOD is required to maintain these implants in perpetuity?
- Should all enlistees be eligible for enhancement, or should only select groups—e.g., those who are able to meet certain physical and mental criteria—be eligible or selected? Can an individual join the military if they have a preexisting augmentation?
- How do enhanced individuals rank compared to unenhanced ones, and how does this change current hierarchies and criteria for promotion and recognition/awards?

These questions and others will require serious attention by each branch of the service as they adapt to the previously discussed "new normal," key aspects of which we address below.

Integration of Enhanced Soldiers into Active-Duty Forces

While human-machine enhancements could potentially increase operational effectiveness of military units, the technologies and techniques to employ them will require study and optimization. These adjustments to current practice will not simply be how we handle personnel but also how we organize enhanced personnel into existing hierarchies, how we utilize them on the battlefield, and how the rules of

warfare may need to be modified to accommodate the use—and to prevent misuse—of these technologies.

Classifying military personnel as enhanced or unenhanced would add another level of categorization to military status, fitness for duty, and/or rank that will have to be considered. Enhancement will effectively change the capabilities and professional status of active-duty soldiers and will require policies and procedures that take into account how these new capabilities will impact the professional qualifications and military occupational specialties assigned. Additionally, in today's military, individuals can take courses or receive additional training to further their career and potential for advancement. Is there a future where obtaining an augmentation conveys an equivalent benefit to an individual's career path? In contrast, could an enhancement limit this potential? For example, what if the enhancement is so unit- or task-specific (i.e., targeting, reconnaissance) or necessary that it constrains or restricts an individual being promoted from field service, or from receiving a different enhancement that is not compatible?

In the early stages of development and deployment, individuals augmented through use of invasive procedures will not likely be prevalent in the general population of troops. Deployment of mixed populations will require changes in doctrine, organization, training, materiel, leadership and education, personnel, and facilities to maximize impact and better achieve the mission. DOD leaders must consider that integrating enhanced personnel within military units that contain unenhanced soldiers is likely to create an imbalance in capabilities. This will almost certainly incur differences in permissions, treatments, or requirements for long-term sustainment. Consideration should be given to how this would impact unit cohesion or morale of the military unit, and whether and to what extent "super soldier" myths will (positively or adversely) affect unit performance. For this reason, the study group recommends that DOD fund and conduct related psychosocial research as development of these technologies advances.

Finally, current DOD rules of engagement require a human-in-the-loop for lethal actions. As technology blurs the line between system and solider, new policies will

need to be developed that define permissions for when to engage in lethal actions for systems under direct human neural control. Is it sufficient for a single human in control of multiple deployed assets to interpret intelligence independently and decide upon the best course of action? In addition to considering how these technologies will alter our own rules of engagements, decision-makers must develop methods of understanding our adversaries' capabilities, intentions, and permissions in this space.[26]

Reintegration of Enhanced Soldiers Back into the Civilian Population

An enhanced military cohort will eventually return to civilian life, requiring secession planning and institution of transition policies that take into account the unique needs of service members with long-term enhancements. The obligations for long-term care of the individual, the security of the technology, and the capabilities afforded by the technology must be considered for each type of augmentation, and policies will have to be tailored to address each consideration and concern effectively. While a soldier with a prosthetic arm is not expected to return the arm after service, an individual who can control a UAV (or other BCI-device or system) with a neural implant may require different considerations upon retiring from service.

Enhancements designed for military applications will likely enable warfighters to perform at a level greater than the previous or general norm, whether via enhanced hearing, vision, stamina, or cognitive capabilities. As an enhanced individual leaves military service, will the military downgrade or deactivate (demilitarize) the capabilities of an enhancement technology, and, if so, what will be the (biopsychosocial) impact upon the individual? While this could seem obvious for individuals able to interact with complex weapon systems or communications capabilities, what are the protocols established for people with enhanced auditory, optical, or cognitive capabilities. If the brain has developed new neural pathways to interpret and use information from these sources, what happens if and when these systems are diminished or deactivated,

and would it be ethical to do so? For enhanced physical capabilities such as strength or stamina resulting from a boost-limb or exoskeleton, how would an individual be psychologically and socially impacted when this physical enhancement is removed? We recognize the possibility of a "post-enhancement distress syndrome" (PEDS) of feelings of inferiority, withdrawal, or even a form of depression associated with the now disenhanced state.[27]

However, as previously discussed, we must consider what it will mean for enhanced individuals to "return to normal." An individual reentering civilian life with enhanced limbs that allow for increased strength or stamina, an eye that provides infrared and/or ultraviolet vision, an auditory device that provides ultra- and subsonic hearing, and/or a neural device that optimizes cognitive capability would have a defined competitive advantage over unenhanced individuals in society. Given the competitive edge imparted to the individual, will there be a propensity for bias in favor or against those enhanced? Would enhanced individuals be "throttled" back to normal levels? Who determines what these levels should be? Will these enhancements be "reverse dual-used" in the civilian population for personal performance optimization, or as "neurocorrective" measures for certain types of behaviors? Policies and protections will need to be established to ensure the sound treatment of both vulnerable populations and those who have received enhancing interventions.

An enhanced individual would need to be monitored for years for the possibility of postenhancement mental health disorders; but what about those who are able to maintain their implants after service? As previously stated, a prosthetic limb or eye would not be removed when an individual leaves the DOD; but what would policy dictate for long-term maintenance and care of indwelling enhancements (e.g., auditory, visual and/or brain implants)? When would the military's commitment to taking care of the individual be an obligation to sustain the enhancement system itself? How would this kind of specialized care and sustainment be coordinated with the Veterans Administration? We must also assume technology will continue to advance the type

and extent of enhancements that are available and of value. While one might not expect that a veteran would receive a postservice "upgrade" that affords improved capabilities, what if such an upgrade maintains functionality, prevents degradation, and/or provides comfort? Or, what if the original system has become obsolete by technological advances? Would technological obsolescence resulting from lack of upgrade(s) (and/or occurrence of PEDS) constitute a compensable disability?

In the cases described, the enhancements all involve a degree of permanence. We recommend, where possible, developing enhancement technologies that could be donned or doffed easily, although the group acknowledged that, for certain enhancements, this may not be feasible in the future. Given this, the possession and security of the enhancement technology becomes an issue during and after military service. For example, if the individual possesses a technology that is not currently available, or if the technology is vastly superior to what is available in other nations, could the individual travel abroad without posing a security risk? What restrictions could reasonably and ethically be placed on someone who has received an enhancement that they cannot doff? To what extent could or should DOD restrict the individual's movements and/or track the device's location? At present, policies are not in place to deal with these questions, issues, and problems.

Ethical Considerations

At all stages, ethical considerations must be at the forefront of DOD's approach. Landmarks in both the lifecycle of product development, as well as the lifecycle of a service member, are touchpoints for a discussion of ELSI issues. For example, the R&D stage of a product raises unique considerations and invokes existing ethical and regulatory structures for research, including the Belmont principles of autonomy, beneficence, and justice, which DOD investments must satisfy. Likewise the needs of, and DOD responsibilities to, a service member change throughout the course of the individual's military career and postmilitary life; each stage merits discussion of ethical considerations.[28]

It should not be taken for granted that principles and frameworks appropriate to one lifecycle stage (either of the product or the individual) will necessarily apply to another. For instance, DOD-supported research has stringent requirements for voluntariness and informed consent. Thus, a service member receiving an investigational enhancement as part of a study must be informed of known risks and benefits and must agree to participate without undue influence. As technology matures and leaves the investigational stage, those interventions that are part of clinical care (i.e., used to prevent, treat, or rehabilitate injury) would also be regarded under existing codes of clinical ethics. However, for enhancements that go beyond clinical care and which are no longer investigational, new frameworks and related policies must be established to illuminate and mitigate ELSI concerns in a rigorous and systematic fashion. In other words, ethical concepts and tools likely need to be modified or created to more precisely address and resolve emerging dilemmas.

Among the most significant ethical considerations that the study group posited is the issue of voluntariness: under what circumstances, if any, could a service member be compelled to undergo an enhancement that has been fielded (i.e., one that is no longer in the R&D stage)? Even if enhancement is voluntary, the extreme nature of many such enhancements will incur both physical and mental health effects immediately after a procedure, during military careers, and over the long term. Can volunteers make an informed decision when these techniques and technologies are new, and when mid-to-long-term effects remain unknown?[29] If potential burdens and risks are to be communicated—and accepted by individuals who receive such interventions—is the DOD obligated to provide ongoing research into long-term effects as well as care for enhanced individuals?

Therefore, in the spirit of medical (and governmental) nonabandonment, ongoing efforts to develop biotechnological enhancements must be accompanied by continuity of research to evaluate prospectively the benefits, burdens, and harms incurred to individuals, bystanders, and groups, and clinical care of individuals in whom burdens and harms occur. The DOD should support foundational research to validate human-machine fusion technologies prior to fielding and to track the long-term safety and impact on individuals and groups.

Conclusions

The introduction of augmented, or "cyborg," human beings into the general population, the DOD active-duty population, and those of near-peer competitors will accelerate in the years following 2050. Human-machine fusions will provide significant benefits and will have positive quality-of-life impacts on humankind by restoring functionality lost as a result of illness or injury. Cyborgs will also impact military operations and training and create potential challenges for established legal, security, and ethical frameworks. Each of these technologies will afford some level of performance improvement to end users that widen the performance gap between enhanced and unenhanced individuals and teams. As these technologies evolve, the scientific and engineering communities must move cautiously to maximize potential with a focus on the safety of our society. Commensurate investments in these areas will work to mitigate misuse or unintended consequences of these technologies.

The questions used in these discussions, as exemplified by the case studies, can provide a broader framework assessment for many types of latent cyborg technologies as they emerge. For our case studies, the following are possible recommendations (not in priority order):

- DOD must conduct global assessments of societal awareness and perceptions of human-machine enhancement technologies. General perception exists that our adversaries are more likely to adopt technologies that US populations are reluctant or unwilling to field based on ethical concerns; however, adversary attitudes toward these technologies have never

been verified. Societal apprehension about new technologies can lead to political barriers and slow domestic adoption. By assessing global attitudes, we may be able to predict both where sociopolitical barriers may hamper the introduction of new technologies and when adversarial adoption of offset technologies is likely to be more readily accepted.

- US leadership should use forums (e.g., per requirements with NATO) to discuss impacts to interoperability with allied partners as we approach the year 2050. This will help develop doctrine, policies, and practices to maximize interoperability of military forces.
- The DOD should invest in the development of dynamic legal, security, and ethical frameworks under its control that anticipate emerging cyborg technologies; current frameworks are insufficient given the speed at which these technologies are developing both in the United States and other nations, both allied and adversarial. Forward-leaning policies, both internal and external to the DOD, should protect privacy, sustain security, and manage personal and organizational risk, while maximizing defined benefits to the US and its allies and assets. Because operationalization of technology for national security is at the core of the DOD mission, these frameworks should be structured to be agile and responsive to new technologies whether developed within the United States or elsewhere.
- DOD and others should try to reverse negative cultural narratives of enhancement technologies; popular social and open-source media, literature, and film have often cast the use of machines to enhance human physical conditions in distorted and dystopian lights. A more realistic and balanced (if not more positive) narrative, along with transparency in the government's approach to technology adoption, will serve to better educate the public, mitigate societal apprehensions, and remove barriers to productive adoption of these new technologies. A more informed public will also help illuminate social concerns, such as those surrounding privacy. Although fielding cyborg technology is not intrinsically a DOD mission, defense leadership should understand that, if it intend to field these technologies, it will need to overcome negative public and social perceptions.
- DOD should conduct table-top war games and targeted threat assessments to inform doctrine and tactics of allied and adversarial forces. War games are well-established tools to exercise the impact of asymmetric technologies on tactics, techniques, and procedures. Table-top exercises exploring varied scenarios of the integration and use of human-machine technologies by the United States and/or its adversaries will predict offset advantages, identify NATO and other allied organizational interoperability friction points, and inform senior military strategists and science-and-technology investors. DOD should support these efforts by targeted intelligence assessments on this emerging field.

- The US government should support efforts to establish a whole-of-nation approach to human-machine enhancement technologies versus a whole-of-government approach. Federal and commercial investments in these areas are uncoordinated and are being outpaced by Chinese R&D, which could result in a loss of US dominance in human-machine enhancement technologies. Near-peer dominance in the commercial sector will place US interests in the defense sector at a disadvantage and could lead to an offset disadvantage in the realm of human-machine enhancement by the year 2050. A national effort to sustain US dominance in cyborg technologies is in the best interests of the DOD and the nation.
- The DOD should support foundational research to validate human-machine fusion technologies prior to fielding and to track the long-term safety and impact on individuals and groups. The benefits afforded by human-machine fusions will be significant and will have positive quality-of-life impacts on humankind through the restoration of functionality lost because of illness or injury. The military community will also see capability opportunities that will impact operations and training. As these technologies evolve, the scientific and engineering communities must move cautiously to maximize potential with a focus on the safety of our society. Commensurate investments in these areas will work to mitigate misuse or unintended consequences of these technologies.

Augmentations and enhancements have the potential to impart significant advantages to the individual, we can anticipate costs to national security if DOD fails to pursue these advantages for the warfighter. Enhancements will be intended to produce a competitive edge to an individual's physical and/or cognitive performance. Partly by design and partly as consequence, the use of enhancements will have an impact on individuals and groups other than the enhanced service member. A thorough approach to anticipating, considering, and mitigating ELSI concerns must involve deliberate assessment of impact on other stakeholders, to include bystanders, nonmilitary users, organizations, noncombatants, and other nations. Myriad specific themes or ethical parameters must also be examined systematically, to include unanticipated military uses, changing ethical standards, philosophical and religious beliefs, and opportunity costs.[30] DOD and its partners must commit to advancing ethical precepts and guidelines that account for different stakeholders and ethical parameters, with obligation to care for those in service and who have served at the forefront.[31]

Images created by Jason Gitlin and Brianna McNamara at US Army CCDC CBC

Endnotes

1 Cyborgs and Space, in Astronautics (September 1960), by Manfred E. Clynes and American scientist and researcher Nathan S. Kline.

2 Shook, J. R.; Giordano, J. Neuroethics Beyond Normal: Performance Enablement and Self-Transformative Technologies. Camb Q Health Care Ethics 2016, 25, 121–140.

3 Jumper, J.M. FDA approves world's first artificial retina, American Society of Retina Specialists. https://www.asrs.org/publications/retina-times/details/131/fda-approves-world-firstartificial-retina (accessed 30 September 2018).

4 O'Donnell, F.; Stahlman, S.; Williams, V. Medical Surveillance Monthly Report; (MSMR) Annual Summary Issue. 2017.

5 Dollar, A.; Herr, H. Lower Extremity Exoskeletons and Active Orthoses: Challenges and State-of-the-Art. IEEE Trans. Robot. 2008, 24 (1), 144–158.

6 Yong, J.S.-e., and Wang, D.-Y. Impact of Noise on Hearing in the Military. Mil. Med. Res. 2015, 2, 1–6.

7 Nguyen, C. H.; Karavas, G. K. Artemiadis, P. Inferring Imagined Speech Using EEG Signals: A New Approach Using Riemannian Manifold Features. J. Neural. Eng. 2018, 15 (1), 016002.

8 An Integrated Brain-Machine Interface Platform with Thousands of Channels: http://dx.doi.org/10.1101/703801 (accessed 30 September 2018).

9 Wurzman, R.; Giordano, J. NEURINT and Neuroweapons: Neurotechnology in National Intelligence and Defense. In Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns; Giordano, J., Ed.; CRC Press: Boca Raton, FL, 2015, pp 79–114.

10 Zou, Q., et al. Generation of Gene-Target Dogs Using CRISPR/Cas9 System. J. Mol. Cell Biol. 2015, 7 (6), 580–583; https://doi.org/10.1093/jmcb/mjv061 (accessed 30 September 2018).

11 Cyranoski, R. CRIPSR-baby scientist fails to satisfy critics. Nature 564, 13-14 (2018) doi: 10.1038/d41586-018-07573-w https://www.nature.com/articles/d41586-018-07573-w (accessed 30 September 2018).

12 Cyranoski, R. Russian biologist plans more CRISPR-edited babies. Nature 570, 145-146 (2019) doi: 10.1038/d41586-019-01770-x. https://www.nature.com/articles/d41586-019-01770-x (accessed 30 September 2018).

13 Chen, C.; Andriola, J.; Giordano, J. Biotechnology, Commercial Veiling, and Implications for Strategic Latency: The Exemplar of Neuroscience and Neurotechnology Research and Development in China. In Strategic Latency: Red, White, and Blue. Managing National and International Security Consequences of Disruptive Technologies; Davis, Z., Nacht, M., Eds.; Lawrence Livermore Press: Livermore, CA, 2018, pp 12–32.

14 Garden, H.; Winickoff, D. Issues in Neurotechnology Governance. OECD Science, Technology and Industry Working Papers, 2018/11, OECD Publishing, Paris. https://www.oecd-ilibrary.org/industry-and-services/issues-in-neurotechnologygovernance_c3256cc6-en (accessed 30 September 2018); Palchik, G.; Chen, C.; Giordano, J. Monkey Business? Development, Influence and Ethics of Potentially Dual-Use Brain Science on the World Stage. Neuroethics 2017, 10, 1–4; Coats, D.R. Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community. Report to Senate Select Committee on Intelligence, 29 January 2019, pp 25–26.

15 "US Public Wary of Biomedical Technologies to 'Enhance' Human Abilities," Pew Research Center, Washington, DC, 2016. https://www.pewinternet.org/wpcontent/uploads/sites/9/2016/07/PS_2016.07.26_Human-Enhancement-Survey_FINAL.pdf (accessed 30 September 2018).

16 "US Public Wary of Biomedical Technologies to 'Enhance' Human Abilities," Pew, 2016.

17 Shook, J. R., Giordano, J. Ethics Transplants? Addressing the Risks and Benefits of Guiding International Biomedicine. AJOB-Neurosci 2017, 8 (4), 230–232.

18 Chan, S. More than Cautionary Tales: The Role of Fiction in Bioethics. Journal of Medical Ethics 2009; 35:398-399. https://jme.bmj.com/content/35/7/398.full (accessed 30 September 2018); Clements, J. How Science Fiction Helps Us Reimagine Our Moral Relations with Animals. JSTOR, 2015. https://www.jstor.org/stable/10.5406/janimalethics.5.2.0181?seq=1#page_scan_tab_contents (accessed 30 September 2018); Delgado, A., et al. Imagining High-Tech Bodies: Science Fiction and the Ethics of Enhancement. SAGE journal, Volume: 34 issue: 2, page(s): 200-240. https://doi.org/10.1177/1075547011408928 or https://journals.sagepub.com/doi/abs/10.1177/1075547011408928 (accessed 30 September 2018).

19 Shook, J. R.; Giordano, J. Moral Bioenhancement for Social Welfare: Are Civic Institutions Ready? Front. Sociol. 2017, 2 (21), 1–5;
Kraft, C.; Giordano, J. Integrating Brain Science and Law: Neuroscientific Evidence and Legal Perspectives on Protecting Individual Liberties. Front. Neurosci. 2017, 11, 1–10;
Giordano, J. Battlescape Brain: Engaging Neuroscience in Defense Operations. HDIAC J. 2017, 3 (4), 13–16.

20 Wittes, B.; Chong, J. Our Cyborg Future: Law and Policy Implications; Brookings Center for Technology Innovation, Washington, DC, 2014, p 15.

21 Wittes and Chong. Our Cyborg Future, 15.

22 Wittes and Chong. Our Cyborg Future, 15.

23 Chang, C.-H.; Lane, H.-Y.; Lin, C.-H. Brain Stimulation in Alzheimer's Disease. Front. Psychiatry 2018, 9 (201).

24 Lawson, B.D. Tactile Displays for Cueing Self-Motion and Looming: What Would Gibson Think? In Advances in Cognitive Engineering and Neuroergonomics, AHFE International Conference, Krakow, Poland, 19–23 July 2014; Stanney, K., Hale, K.S., Eds.; Springer International Publishing: Switzerland, 2014; pp 3–13.

25 DeFranco, J.; DiEuliis, D.; Bremseth, L.R.; Snow, J. J.; Giordano, J. Emerging Technologies for Disruptive Effects in Non-Kinetic Engagements. HDIAC J. 2019, 6 (2), 49–55.

26 Tennison, M.N.; Giordano, J.; Moreno, J.D. Security Threat versus Aggregated Truths: Ethical Issues in the Use of Neuroscience and Neurotechnology for National Security. In Neuroethics: Anticipating the Future; Illes, J., Hossain, S., Eds; Oxford University Press: Oxford, UK, 2012; pp 531–553; Gini, A.; Rossi, J.; Giordano, J. Considering Enhancement and Treatment: On the Need to Regard Contingency and Develop Dialectic Evaluation. AJOB Neurosci. 2010, 1 (1), 25–27.

27 Weinberger, A. B.; Cortes, R. A.; Green, A. E.; Giordano, J. Neuroethical and Social Implications of Using Transcranial Electrical Stimulation to Augment Creative Cognition. Creativity Res. J. 2018, 30 (3), 249–255.

28 *The Belmont Report,* US Department of Health and Human Services, https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html.

29 Giordano J. Conditions for Consent to the Use of Neurotechnology: A Preparatory Neuroethical Approach to Risk Assessment and Reduction. AJOB Neurosci. 2015, 6 (4), 12–14.

30 Committee on Ethical and Societal Implications of Advances in Militarily Significant Technologies that Are Rapidly Changing and Increasingly Globally Accessible. In Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues; Chameau, J.L., Ballhaus, W.F., Lin, H.S., Eds; The National Academies Press: Washington, DC, 2014.

31 Lanzilao, E.; Shook, J.; Benedikter, R.; Giordano, J. Advancing Neuroscience on the 21st Century World Stage: The Need for — and Proposed Structure of — an Internationally Relevant Neuroethics. Ethics Biol. Engineer. Med. 2013, 4 (3), 211–229.

CHAPTER 10

Contemporary Global Food Systems as Contested Space: Implications for Special Operations Forces

Molly M. Jahn, Aaron M. Kelly, Gregory F. Treverton, Michael S. Gremillion, LTG (Ret.) Edward Cardon, Matthew A. Rose, Megan Konar, Michael J. Puma, David A. Bray, Joseph Byrum, Anthony L. Nguy-Robertson, Jean-Paul Rodrigue, Thomas L. Creely, Seth C. Murray, William L. Oemichen, and Budhikka "Jay" Jayamaha

> *"The contingency we have not considered seriously looks strange; what looks strange is thought improbable; what is improbable need not be considered seriously."*
>
> ***—Thomas Schelling, in the forward to Pearl Harbor: Warning and Decision[1]***

Introduction

As laid out in both the National Defense Strategy (NDS) and National Security Strategy, the global food system is a complex, active area of operations for great-power competition and conflict, influence, and control. The global food system comprises an unconventional, poorly understood risk surface subject to both intentional and unintentional disruptions. Special operations forces (SOF) are regularly called into action where control of provisioning and information about provisioning are linked to power and freedom to operate. The SOF core activities relevant to this chapter include direct action, special reconnaissance, countering weapons of mass destruction, counterterrorism, unconventional warfare, and foreign humanitarian assistance.[2]

Food Systems in War and Peace

Military control of supply lines and food distribution to civilian populations has always had tactical, operational, and strategic significance in wartime. The power that resides in the control of "food systems" has been wielded by every human civilization in both peace and wartime. Historical evidence underlines the Roman Republic—the longest-lasting democratic government to date (509–27 BCE)—understood this power explicitly; cura annonae, or "care for the grain supply," was revered as the goddess Annona.[3] Outbreaks of civil violence as a result of food shortages in Rome are reported to have occurred 19 times, once compelling the emperor to flee for his life and, on another occasion, forcing the return of Caesar from Egypt.[4] Rome understood military control of shipping lanes was essential for both the application of the domestic rule of law and the Roman ability to mount expeditionary forces.[5]

Over the last millennia, when food distribution systems for expeditionary forces or civilians were interrupted or otherwise failed, history-shaping consequences often followed.[6] Domestic food riots generally dismissed in geopolitics may nonetheless

have regime-shifting consequences.[7] For example, in 2011, the civil unrest known as the Arab Spring was sparked by rising global commodity prices and local drought, resulting in food riots that led to major shifts of military power in several countries of the Middle East.[8] Spurred by droughts and fires in the Ukrainian breadbasket, Russia exploited the civil instability in the Middle East to establish a renewed sphere of influence in the region with long-term, global geopolitical ramifications for warfare and global terrorism.

The need to control agriculturally productive lands directly or indirectly has determined the boundaries of nearly every nation. Some nations—Argentina, for instance[9]—recognize certain agriculturally significant regions as latent strategic national security assets, restricting ownership to citizens. In contrast, the United States has no policy basis to monitor the ownership of agricultural or food system assets or to systematically monitor essential agricultural goods and services or contingencies relevant to national security. Agricultural assets include both direct and indirect requirements such as soil and water resources, seed and seed banks, fertilizer, and agricultural implements.

In the Embargo Act of 1807, Thomas Jefferson threatened curtailment of US agricultural exports to force Britain and France to change their maritime policies toward the United States. During World War II, the US ability to ramp up agricultural production and support its allies strategically, while also continuing to feed its own population, was critical to victory.[10] After the war, the United States built a global agricultural hegemony that remained stable for decades and reduced US trade deficits and led to enormous economic, political, diplomatic and humanitarian benefits. It also resulted in soft-power influence, with unparalleled agricultural abundance, as seen in the green revolution, fueling steep population increases around the world. The Agricultural Trade Development and Assistance Act of 1954 authorized the secretary of agriculture to accept up to $700 million in foreign currency for repayment for commodities shipped to friendly nations.[11] In the 1960s, the John F. Kennedy administration used its Food for Peace program to counter communism in Asia while opening export markets to American farmers.

While the idea of food influence has been crucial in building US alliances, especially in Asia and Latin America, the United States does not aggressively protect strategic use of agricultural exports for foreign policy or security agendas today. Most Americans are unaware that during the past several decades, foreign states or private companies have acquired US agricultural resources and companies. This is occurring as US farmers are in their worst economic position since the early 1980s as a result of sustained low commodity prices, extreme weather, and a prolonged trade war followed by a global pandemic. Farm exits in some states were at all-time highs in 2019. Financial stress and credit policies are resulting in fewer, further consolidated, and larger operations. In 2019, a polar vortex caused widespread heavy rains, early freezes, delayed harvest, spoiled crops, propane shortages as a result of grain drying, stalled shipping, and full bins. US farmers have suicide

rates five times the US average (2017), although statistics are likely skewed to underestimate the actual rates.[12] Some US counties are depleting their aquifers—strategic groundwater reserves—as a result of poor water-management practices and agricultural and trade policies that encourage the export of US fossil water in the form of agricultural commodities.[13]

Moreover, China, Saudi Arabia, and other foreign interests are purchasing US agricultural lands and water rights, often in the absence of legally required notice or complete record keeping, despite the 1978 Agricultural Foreign Investment Disclosure Act. In 2017, ChemChina acquired Syngenta—one of the three primary US seed and chemical input suppliers—the largest Chinese acquisition of a US-owned company to that date, while German multinational Bayer purchased Monsanto. Sufficient seed supplies take years of planning, and these genetic resources are unique and invaluable. If, for any reason, these companies either refused or were unable to serve US markets, there would not be enough seed to plant, with no effective recourse or alternative in place. In short, previous assumptions about the resilience, stability, and productivity of the US food system may not hold, especially under duress, such as biological, artificial intelligence (AI), or other attack. Indirect stressors such as pandemics, market shocks, long-term power-grid failure, or failure of Global Positioning Systems could result in major disruption of the US food system.

Historically, when great powers have mounted an attack, they have anticipated the dynamics of provisioning both their military and civilian populations through either acquired influence (e.g., legal ownership, default technological dominion) or physical control of supply sources and supply lines. For example, in World War II, motivated in part by a vision of agricultural empire, Nazi Germany mounted the blitz through Poland, Norway, Belgium, Holland, and France and attacked the Soviet Union in Operation Barbarossa to meet the Axis need for food and resources.[14] As control of energy sources is often a cause of conflict, food as human energy is likewise a necessity of war.[15] For the modern-day United States, fragility in supply chains, masked by peacetime, presents a serious challenge.

Throughout most of human history, widespread precedent exists for the weaponization of food systems against a belligerent or civilian population as a means of control or influence. Article 17 of the 1863 US Lieber Code states: "It is lawful to starve the hostile belligerent, armed or unarmed, so that it leads to the speedier subjection of the enemy."[16] Control of food systems has always been key to winning wars. Extraordinary institutional innovations such as the Combined Production and Resource Boards, created by the Allies across national boundaries during World War II, were fundamental to victory and saved tens of millions of lives.[17] These institutions have been entirely dismantled in the years since, with the last vestiges of control removed by the 1996 Federal Agricultural Improvement and Reform Act (P.L. 104-127).

Outside US borders, SOF view control of foodstuffs, energy, and other critical provisions as tactical in kinetic war, considered systematically in military planning,

but are not generally in a position to think about food resources strategically. The weaponization of food to subjugate or starve civilian populations is prohibited by the Geneva Convention Article 54(1) of the 1977 Additional Protocol I and Article 14 of the 1977 Additional Protocol II.[18] Unfortunately, this specific prohibition does not clearly limit the weaponization of food or food systems in offensive military contexts, it also does not address gray-zone attacks in the homeland clearly. US actions in this area, therefore, may serve to define and uphold ethical principles of engagement in food systems.

Food *Systems* as an Area of Operations: Why Think in *Systems*?

We define "food systems" as the highly complex, complicated, and dynamic critical infrastructures that provide every human being with food every day.[19] SOF must consider unconventional attack surfaces in the homeland, and the potential for both offensive and defensive action in the battlespace defined by contemporary US and global food systems. Attacks on systems, per se, have been used to perpetrate and propagate damage through causal chains of relationship since at least the Gulf War.[20] Recent research has demonstrated the interconnectedness and fragility of the logistical networks supporting US food systems.[21] The locations of key railway and roadway networks, cargo shipping routes, reservoirs, water-treatment facilities, fertilizer plants, meatpacking/food-processing facilities, seed companies, and ports are public knowledge and, thus, highly vulnerable to targeting by adversaries. US government policy concerning food supply stems largely from the fact that the United States has not experienced warfare in the continental homeland for a century and a half, during which period, the nation has experienced agricultural abundance unparalleled in human history. Beyond stockpiling Meals, Ready-to-Eat (MREs) for sudden expeditionary requirements—such as attacks or disasters in the homeland—US food-system vulnerabilities have not been a strategic focus of the military since the end of World War II. It was reasonable to assume mid-twentieth-century US and global food systems were extremely stable and could not be easily weaponized. However, this stability is being challenged by the current context.

Since the 1980s, massive shifts in the structure of US food systems have occurred, notably consolidation, duopolization, deregulated algorithmic commodities trading, exponential increases in energy intensity, the advent of embedded "smart" systems and just-in-time delivery. All of these have opened up new attack surfaces in the homeland and ill-understood possibilities for both offense and defense. Recent exercises have focused on cyberattack, military attack, and pandemics, but the implications of these events on national and global food systems have not been explored. President George W. Bush issued a Department of Homeland Security Presidential Directive to classify the US agricultural system as "critical infrastructure," followed by revised directives in 2003 and 2013. These policies, in general, have focused narrowly on intentional contamination of the US food system for economic or political terrorism. They fail to address vulnerabilities affected by the trends of

consolidation, resource depletion, increases in foreign control, and farm insolvency that have occurred since enactment of these policies.[22]

The SOF's lenses must be widened to account for unconventional and potentially convergent attack vectors and events. Biological, cyber, and physical threats or mis/disinformation campaigns could be imposed as unconventional attacks, potentially coincident with collateral disruptions to food systems. For example, an unconventional attack launched during the acute global shortage of refrigerated shipping containers, which resulted when the 30,000 units that China ordinarily unloaded per day was abruptly stopped because of the COVID-19 epidemic, could have been especially crippling. Cyberattacks on the food supply chain could incapacitate machinery and/or computer systems involved with agricultural production, harvest, transport, food manufacturing, inventory control, or market information. Ransomware attacks have increased dramatically in the last few years. The high degree of centralization in the US food systems, coupled with low profit margins and complacency, adds up to potentially consequential interruption from a relatively straightforward act of aggression. Cognitive attacks could result from deepfake proof that food is contaminated. Spoofed or scrambled market or supply information may present particulary difficult challenges because misinformation is formally impossible to disprove. An attack could spur antisocial behavior, such as the 2019 "ice cream licking" incidents or deliberate coughing on produce.

Food systems represent an active area of operations for great-power competition and conflict, which Department of Defense (DOD) or US government policies and military planning do not recognize. Current US military doctrine does not account for food systems in the joint planning process, and arguably hand waves this system as not a military concern (JP 1-0, JP 5-0).[23] A chasm exists between the traditional US concept of "food defense." Food defense explicitly excludes warfare, but contemporary subkinetic warfare exploits any vulnerable or important attack surface. This gap in US policy opens potential threat space and opportunities for both competitors and enemies to take actions with long-term and immediate impacts. China has clearly understood that control of many types of assets in the global and US food system is critical for its future stability and security. As for other threats, the default approach in the United States since the 1990s has been to "harden," by stockpiling foodstuffs and raw materials in the event of an attack or emergency.

There is a comforting but false assumption that the commercial sector has unlimited resilience. This view obscures the range of both vulnerabilities and innovative opportunities in the contemporary global and US food systems specifically pertinent to the DOD as both warfighters and peacekeepers. While US defense planners have focused on stockpiles of military foodstuffs (e.g., MRE caches), the US military has not paid enough attention to the complex network structures and properties (e.g., ownership, physical infrastructure, trade policies, institutions, resilience, stability) that govern the US and global food systems. These structures and properties affect US national security and/or define unconventional attack

surfaces.[24] The DOD excels at intelligence, information, and planning. Still, because military planners do not focus on these elements, the defense intelligence enterprise is not tasked with collecting and analyzing relevant information. Protection of US food systems, or aspects of the global food system of particular relevance to US vulnerabilities, may fall to the SOF OCONUS and the National Guard in CONUS. For this chapter, we further parse out this battlespace and discuss potential implications of our current shortfalls in policy and strategy for both SOF and the DOD as a whole.

Strategic Latency in US Military-Force Food Logistics and Supply

The evolution of contemporary military food logistics and supply processes has been broadly guided by the post–World War II Hoover Commission, which led to the creation of the Defense Logistics Agency (DLA). The subsistence directorate of the defense logistics within the DLA oversees the food sourcing for the armed forces.[25] The Defense Supply Center Philadelphia (DSCP) requires each regulated food-chain member to implement a food defense plan in compliance with the DSCP Food Defense Checklist.[26] The Buy American Act and the Berry Amendment require provisions must be purchased from US companies whenever possible, although this requirement was waived for Middle Eastern operations.[27] Perishable items are generally sourced where they are consumed.[28] Food supply in conflict zones comes from a variety of sources, often only lightly secured (if secured at all). The DLA systems require a high inventory load but may still struggle to fulfill forecasted food requirements.[29] Alternatively, food for forward units is often sourced from DLA-maintained agreements with local and regional networks and acquired ad hoc from local markets.[30] Sourcing may also take advantage of the food systems of the host nation's military.[31] Official USDA Food Defense suggests hardening food facilities.[32] The Army has a framework, used by the other branches, that requires a food defense assessment team (FDAT) at each service location.[33] Improvements have focused on increasing the effectiveness of the DLA system of requisitioning food supplies to conflict zones and improving troop nutrition.[34]

Various reports analyze the effectiveness of and potential improvements to the military food systems. A 2009 National Defense University report, "Defending the Military Food Supply Acquisition, Preparation, and Protection of Food at US Military Installations," details food safety and security in DLA processes and military policies.[35] Consideration of "attack" on the military food system is restricted to material attacks on the food itself by way of contamination, poisoning, or intentional introduction of a food-borne pathogen; threats are classified as biological, chemical, or radioactive. The report concludes it would be "extremely difficult to specifically target food destined for the military this early in the supply chain." It is possible, however, that a determined adversary could exploit other types of strikes or vulnerabilities, for instance, interfering with cyber systems and energy supplies, using even disinformation and influence campaigns, and attacking the soft targets on bases where local food service staff come and go daily.

What Is "Food Security," and Why Is It Important?

The term "food security" originated at the 1974 World Food Conference, reflecting the prevailing idea that hunger resulted from a physical shortage of foodstuffs. Today, food security is a formal economic statistic derived from nationally reported statistics on agricultural production, exports, and imports and the number of impoverished people, who are subject to political and other contrivances. The concept has come into wide use since the 1970s. "Food security" or "food insecurity" are most tightly tied to poverty across the development spectrum and, therefore, are not terms that specifically apply to national security or the SOF. An exception is in the extreme case when the US military is summoned for humanitarian assistance and disaster relief. In such environments, insurgencies regularly divert and exploit control of foodstuffs and funds from aid efforts.[36]

Increased obesity and diabetes among active-duty military and civilian populations are symptoms of an out-of-whack US food system. An unfit military has come to be a greater threat to US national security than undernutrition. Still, food insecurity experienced by some military families on base has been noted as a specific concern for readiness. In a Centers for Disease Control and Prevention study of the impact of diet-related health on the military, 71 percent of service-eligible young people were deemed unfit to serve, partly because overweight and obesity rose 73 percent between 2011 and 2015 among active-duty personnel; obese active-duty soldiers were 33 percent more likely to experience musculoskeletal injury. The study further noted the DOD spends about $1.5 billion annually on obesity-related healthcare costs.[37]

Control and Influence in Global Food Systems and Great-Power Competition

Despite popular usage, the term *food security* does not describe a military food system secured to function during the types of large-scale, compound assaults virtually certain to occur in the near future. The term also does not describe a food system upon which a civilian population or the economy depends that is resilient or protected from assault. Shifts in both structure and function of the highly consolidated, highly efficient systems by which food is produced, manufactured, traded, distributed, and consumed have opened potential massive attack surfaces.[38] Considerable potential exists for malevolent actors to weaponize contemporary "food systems" as an unconventional attack surface, with plausible catastrophic impact.[39]

Nodes, or points of control in food systems where direction could be imposed, particularly with reference to ability to or preparedness for war, are not defined. No government, private, or other entity is responsible for identifying, monitoring, or understanding such control points. Current threat taxonomy is incomplete, leading to difficulties in detecting and understanding problems as they emerge. Furthermore, interlinked critical infrastructures in the homeland and globally, upon which the US force depends, are highly vulnerable. Almost every American living room and communication device has opened up a channel through which weaponized mis/disinformation can be delivered. Any aspect of these complex, interlinked networks

is vulnerable to cyber or other attacks, whether as an act of aggression in a great-power kinetic or subkinetic war or an act either to harm US economic, political, civilian systems or to influence warfare.[40]

One example of a nonkinetic act of aggression could be targeting US water security through large-scale saltwater contamination. Ongoing pumping of water into the ground in certain US regions prevents widespread contamination of agricultural soils. Brackish water can result from either disrupting this pumping or increasing the rate of withdrawal, potentially destroying the productivity of that region permanently. For special operators outside the United States, MREs may be the answer to short-term food supply requirements. But for SOF, it is critical to ensure stable, secure supply lines that recognize the gaps in transfer and the softness of expeditionary bases with regard to food preparation on base. New technologies for "pop up" water, food, and energy sources that can be mainstreamed quickly will improve the stability and security of US forces.

Through its global reach, China is addressing a number of obvious domestic imperatives such as stable long-term food sufficiency, the export of labor and finance, access to critical resources (such as mining), and military and foreign policy objectives. For decades, globalization has driven the development of highly efficient and complex supply networks. The number of companies involved directly with food systems has notably decreased, while their size and relationships in massive conglomerates have increased.[41] Meanwhile, through acquisitions, direct and proxy purchases, financing arrangements and labor export, Chinese and Russian agricultural capacity is increasing.[42] Recent Chinese acquisitions include Smithfield Foods, the world's largest pork producer, and Syngenta, mentioned previously, both by state-owned conglomerates.[43] Collateral effects of globalized consolidation and monopolization are increasing global genetic uniformity of crops and livestock and often poorly secured digitized operations.[44] While China is reportedly outpacing the United States in the development of a number of convergent technologies,[i] the two superpowers are deeply intertwined and interdependent and share exposure to various existential risks.

Conclusions

In summary, as the United States updates its war plans in light of the NDS—taking into consideration the implications of unconventional, complex threats at scale in any operating environment—SOF must prepare for new offensive and defensive postures in both civilian and military food systems. SOF should consider the control and management of food systems in any preparation for operations and war plans. In a world where anything can be weaponized almost instantly, including information about an essential commodity in the homeland or abroad, almost anything,

i AI, genome editing, biometric fintech, the Internet of Things, chips, qubits, rockets, nuclear reactors, surveillance, mass detention, and fake islands, to name a few.

including international stature or influence, can be put into play. The perception of agricultural abundance, engineered by President Abraham Lincoln by the suite of visionary legislation he developed during the US Civil War, has lulled US policy into ideosyncratic, narrow channels of concern. The terms "food defense" or "food security" focus too narrowly on local agricultural production and miss global dynamics that could be leveraged with great impact on or for the DOD.

In 2017, DLA organized a summit to create a partnership for all of their supply-chain stakeholders. Shawn Jones summarized what Army Lt. Col. Abel Young, director of DLA Troop Support's Subsistence supply chain, said during the summit, "the partnership has been effective, but like most complex systems, there is room for improvement. . . . The supply chain is a combination of multiple supply chains with several independent agencies and mutually exclusive contracts which results in 'a breeding ground for stakeholders with potentially different expectations and objectives.'" He stated a need to better integrate internal and external stakeholders into a streamlined process with a continuous flow of data.[45] These data could also be purposed for use by AI to build simulation capabilities and identify key control nodes, decision menus, warnings, and threshold protocols, as well as standing capability to screen in real time for essentially any type of threat or its signature.

AI-driven representation of food networks will only be as good as the data used to train the capabilities, making it important to deliberate on new data gathering and curation missions. A DOD-wide standing capability that can identify geospatially events of concern related to global food systems, specifically relevant to DOD's missions and roles, could usefully reside at the US National Geospatial-Intelligence Agency and in the Joint Staff. SOF thinking must consider outliers and black swan events in the realm of food-security disruptions to maintain competitive military advantage and possess the moral high ground for national security. It is necessary to strengthen decision-making agility in this fast-paced, disruptive, and complex technological landscape of competing values and political and national security priorities. SOF's new applied ethics initiative across its operational spectrum will shore up the shortcomings of DOD and US government policies and help mitigate risks.[46] The SOF should ensure every mission considers both vulnerabilities and potential consequences of shifts in the function of military and civilian food systems in the homeland, in theaters, or on missions as a facet of complex provisioning systems whereby power is created, maintained, and exercised.

Endnotes

1 Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, California: Stanford University Press, 2005).
2 "Joint Publication 3-05, Special Operations," July 16, 2014.
3 Rickman, G.E. (1980). *"The Grain Trade under the Roman Empire." Memoirs of the American Academy in Rome*. 36: 263. Downloaded from JSTOR.
4 NPR, "Roman Banquets, a Calculated Display of Debauchery and Power," May 20, 2019, https://www.npr.org/sections/thesalt/2019/05/20/712772285/the-lavish-roman-banquet-a-calculated-display-of-debauchery-and-power.
5 Geoffrey Rickman, "Plenary Address: Ports, Ships, and Power in the Roman World," *Memoirs of the American Academy in Rome*. Supplementary Volumes 6 (2008): 5–20.
6 E. M Collingham, *The Taste of War: World War II and the Battle for Food*, 2013.
7 Henk-Jan Brinkman and Cullen S. Hendrix, "Food Insecurity and Violent Conflict: Causes, Consequences, and Addressing the Challenges" (World Food Programme, July 2011), https://ucanr.edu/blogs/food2025/blogfiles/14415.pdf.
8 Marco Lagi, Karla Z. Bertrand, and Yaneer Bar-Yam, "The Food Crises and Political Instability in North Africa and the Middle East," *ArXiv:1108.2455 [Physics]*, August 11, 2011, http://arxiv.org/abs/1108.2455; Marco Lagi et al., "The Food Crises: A Quantitative Model of Food Prices Including Speculators and Ethanol Conversion," ArXiv:1109.4859
9 Vinals Blake, Pablo, Sanchez Echague, Ignacio, O'Farrell, Marval, "Agricultural Law in Argentina: Overview," Thomson Reuters Practical Law, Agricultural Law in Argentina: Overview, October 1, 2016, https://uk.practicallaw.thomsonreuters.com/4-607-3045.
10 Collingham, *The Taste of War,* 2013.
11 "The Agricultural Trade Development and Assistance Act of 1954," Pub. L. No. 480, § 1691 nt, 7 454 (1954).
12 Todd Fitchette, "Farmer Suicide: The Topic Few Will Discuss," *Farm Progress*, June 7, 2018, https://www.farmprogress.com/outlook/farmer-suicide-topic-few-will-discuss.
13 Sajani Gumidyala et al., "Groundwater Depletion Embedded in Domestic Transfers and International Exports of the United States," *Water Resources Research* 56, no. 2 (February 2020), https://doi.org/10.1029/2019WR024986.
14 Collingham, *The Taste of War*, 2013.
15 Burton Wright III, "Deep Attack—And I Do Mean Deep," *Army Logistician*, no. July-August 2001 (n.d.): 44.
16 Francis Lieber, "Instructions for the Government of Armies of the United States in the Field" (Abraham Lincoln, April 24, 1863), https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule53.
17 Eric Roll, *The Combined Food Board: A Study in Wartime International Planning, Food, Agriculture, and World War II* (Stanford, CA: Stanford University Press, 1956).
18 "Protocol Additional to the Geneva Convention of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), Article 53(1)." (Official Records, June 8, 1977).
19 Polly J. Ericksen, "Conceptualizing Food Systems for Global Environmental Change Research," Global Environmental Change 18, no. 1 (February 2008): 234–45, https://doi.org/10.1016/j.gloenvcha.2007.09.002.
20 John Robb, Brave New War: The next Stage of Terrorism and the End of Globalization (Hoboken, N.J.; Chichester: Wiley; John Wiley [distributor, 2008).
21 Xiaowen Lin, et al., "Food Flows between Counties in the United States," *Environmental Research Letters* 14, no. 8 (July 2019): 084011, https://doi.org/10.1088/1748-9326/ab29ae.
22 "Homeland Security Presidential Directive / HSPD-9" (Department of Homeland Security, January 30, 2004).
23 "JP 1-0, JP 5-0," n.d.
24 Gwen M. Chodur, et al., "Assessing Food System Vulnerabilities: A Fault Tree Modeling Approach," *BMC Public Health* 19, no. 1 (July 3, 2018): N.PAG-N.PAG, https://doi.org/10.1186/s12889-018-5563-x\\uc0\\u8221{} {\\i{}BMC Public Health} 19, no. 1 (July 3, 2018; Agustina Calatayud, John Mangan, and Roberto Palacin, "Vulnerability of International Freight Flows to Shipping Network Disruptions: A Multiplex Network Perspective," Transportation Research Part E: Logistics and Transportation Review 108 (December 1, 2017): 195–208, https://doi.org/10.1016/j.tre.2017.10.015.
25 Valerie Bailey Grasso, "Department of Defense Food Procurement: Background and Status" (Congressional Research Service, January 24, 2013), https://fas.org/sgp/crs/natsec/RS22190.pdf.January 24, 2013
26 Andrew Mara and Lynn McGrath, "Defending the Military Food Supply Acquisition, Preparation, and Protection of Food at US Military Installations," n.d., https://apps.dtic.mil/dtic/tr/fulltext/u2/a506611.pdf.
27 Grasso, "Department of Defense Food Procurement: Background and Status.""plainCitation":"Grasso, "Department of Defense Food Procurement: Background and Status.""","noteIndex":27},"citationItems":[{"id":1626,"uris":["http://zotero.org/groups/2211266/items/XMYI9ZSC"],"uri":["http://zotero.org/groups/2211266/items/XMYI9ZSC"],"itemData":{"id":1626,"type":"report","abstract":"Military food items, also known as subsistence items, are generally procured under the auspices of the Defense Logistics Agency (DLA
28 Mara and McGrath, "Defending the Military Food Supply Acquisition, Preparation, and Protection of Food at US Military Installations."
29 Mark D. Maj. Pike, "BCT Logistics in Al Anbar Province," *Army Logistician* 40, no. 3 (n.d.), https://alu.army.mil/alog/issues/MayJun08/bct_al_anbar.html; James A. Schear, William B. Caldwell, and Frank C. Digiovanni, "Ministerial Advisors: Developing Capacity for an Enduring Security Force," PRISM 2, no. 2 (March 2011): 135–44.

30 Charles R. Brig. Gen. Hamilton, "DLA Troop Support Supplies Army Expeditionary Logistics," Army Sustainment, no. March-April 2016 (n.d.): 42–45; Eyal Ziv, "Logistics in Asymmetric Conflicts," Army Sustainment 44, no. 1 (February 2012), https://alu.army.mil/alog/issues/JanFeb12/Logistics_Asymmetric.html; Alexander F. Barnes and Sara E. Cothren, "Logistics Support for Small Unit Operations: The Marine Corps in the Dominican Republic, 1916–1924," Army Sustainment, no. November-December 2012 (n.d.): 46–52; Mary K. First Lt. Blanchfield, "Transportation Challenges in Afghanistan," *Army Logistician* 37, no. March-April 2005 (n.d.), https://alu.army.mil/alog/issues/MarApr05/afgan.html.

31 Ned C. Lt. Col. Holt, "USAREUR Supports Soldiers Through ACSA Orders," *Army Sustainment*, no. May-June 2018 (n.d.): 56–59."container-title":"Army Sustainment","issue":"May-June 2018","page":"56-59","title":"USAREUR Supports Soldiers Through ACSA Orders","author":[{"family":"Lt. Col. Holt","given":"Ned C."}]}}],"schema":" https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}

32 "Food Defense," USDA.gov, September 24, 2019, https://www.fda.gov/food/food-defense.

33 Mara and McGrath, "Defending the Military Food Supply Acquisition, Preparation, and Protection of Food at US Military Installations."

34 Ann H. Barrett and Armand V. Cardello, *Military Food Engineering and Ration Technology* (Lancaster, Pa: DEStech Publ, 2012); Eric Peltz, "Improving DLA Supply Chain Agility: Lead Times, Order Quantities, and Information Flow," n.d.; Linda C. Maj. Wade et al., "Developing Smarter Logistics Support to Remote Areas," Army Sustainment, no. January-February 2015 (n.d.): 10–17.

35 "Forward DLA Troop Support Food Defense Checklist," March 14, 2018, https://www.dla.mil/Portals/104/Documents/TroopSupport/Subsistence/FoodSafety/FoodQuality/food_defense_check14MAR18.pdf.

36 Jahn, Molly, et al., "Global Food System Stability and Risk," Thomson Reuters Special Report (Washington, DC, 2019).

37 "Unfit to Serve: Obesity Is Impacting National Security" (Center for Disease Control and Prevention, March 2019), https://www.cdc.gov/physicalactivity/downloads/unfit-to-serve.pdf.

38 "Threats to Precision Agriculture" (Department of Homeland Security, Public-Private Analytic Exchange Program, October 3, 2018), https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf.

39 "Food Defense Overview What Is Food Defense and Why Is It Important?" (Food Safety and Inspection Service), accessed January 4, 2020, https://www.fsis.usda.gov/wps/portal/fsis/topics/food-defense-defense-and-emergency-response/food-defense-overview.

40 "Evolving Risks in Global Food Supply. - Lloyds of London," 2019, https://www.lloyds.com/news-and-risk-insight/risk-reports/library/understanding-risk/evolving-risks-in-global-food-supply.

41 Megan Konar et al., "Scaling Properties of Food Flow Networks," ed. Samir Suweis, PLOS ONE 13, no. 7 (July 10, 2018): e0199498, https://doi.org/10.1371/journal.pone.0199498; Bruno Pellegrino, "Product Differentiation, Market Power and Resource Allocation," SSRN Electronic Journal, 2019, https://doi.org/10.2139/ssrn.3329688; Wrigley, "The Consolidation Wave in US Food Retailing"; Hendrickson, et al., "Consolidation in Food Retailing and Dairy"; Wood, "Revisiting the US Food Retail Consolidation Wave"; Howard, "Visualizing Consolidation in the Global Seed Industry."

42 Jingfeng Zhao and Jianmin Tang, "Understanding Agricultural Growth in China: An International Perspective," Structural Change and Economic Dynamics 46 (September 2018): 43–51, https://doi.org/10.1016/j.strueco.2018.03.006; William M Liefert et al., "The Effect of Russia's Economic Crisis and Import Ban on Its Agricultural and Food Sector," Journal of Eurasian Studies 10, no. 2 (July 1, 2019): 119–35, https://doi.org/10.1177/1879366519840185; Ilya Kuzminov et al., "The Current State of the Russian Agricultural Sector," EuroChoices 17, no. 1 (April 2018): 52–57, https://doi.org/10.1111/1746-692X.12184; "Understanding China's Foreign Agriculture Investments in the Developing World | Devex," accessed July 9, 2018, https://www.devex.com/news/understanding-china-s-foreign-agriculture-investments-in-the-developing-world-92639; Cecilie Friis and Jonas Østergaard Nielsen, "Small-Scale Land Acquisitions, Large-Scale Implications: Exploring the Case of Chinese Banana Investments in Northern Laos," Land Use Policy 57 (November 2016): 117–29, https://doi.org/10.1016/j.landusepol.2016.05.028; Bill Oemichen, Molly M. Jahn, and Braeden Rimestad, "Is Agricultural Land Ownership a Food Systems Security Issue?" (Concept Paper, July 2019); Saturnino M. Borras, Jennifer C. Franco, and Chunyu Wang, "The Challenge of Global Governance of Land Grabbing: Changing International Agricultural Context and Competing Political Views and Strategies," Globalizations 10, no. 1 (February 2013): 161–79, https://doi.org/10.1080/14747731.2013.764152; Beth Robertson and Per Pinstrup-Andersen, "Global Land Acquisition: Neo-Colonialism or Development Opportunity?," Food Security 2, no. 3 (September 2010): 271–83, https://doi.org/10.1007/s12571-010-0068-1; Huaichuan Rui and George S. Yip, "Foreign Acquisitions by Chinese Firms: A Strategic Intent Perspective," Journal of World Business 43, no. 2 (March 2008): 213–26, https://doi.org/10.1016/j.jwb.2007.11.006; Rui and Yip, "Foreign Acquisitions by Chinese Firms"; Richard Kamchen, "Just How Much Foreign Ownership of Farmland Is There?," Country Guide (blog), April 4, 2016, https://www.country-guide.ca/guide-business/our-farmland-for-sale/; Keith Schneider, "US, U.K, and China Lead Foreign Land Investments In Agriculture and Finance," Circle of Blue, June 22, 2012, https://www.circleofblue.org/2012/world/u-s-u-k-and-china-lead-foreign-land-investments-in-agriculture-and-finance/.

43 Oemichen, Jahn, and Rimestad, "Is Agricultural Land Ownership a Food Systems Security Issue?"

44 Howard, "Visualizing Consolidation in the Global Seed Industry"; Molly M. Jahn, et al., "Cyber Risk and Security Implications in Smart Agriculture and Food Systems," White Paper (Jahn Research Group, January 2019), https://jahnresearchgroup.webhosting.cals.wisc.edu/wp-content/uploads/sites/223/2019/01/Agricultural-Cyber-Risk-and-Security.pdf.

45 Jones, Shawn J., "DLA Hosts Summit to Strengthen Warfighter Food Supply Chain," *DLA Public Affairs*, January 29, 2018, https://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1423928/dla-hosts-summit-to-strengthen-warfighter-food-supply-chain/.

46 "United States Special Operations Command Comprehensive Review," January 23, 2020, https://sof.news/pubs/USSOCOM-Comprehensive-Ethics-Review-Report-January-2020.pdf.

CHAPTER 11

As the Helix Turns: How New Biology, Biometrics, and DNA Analysis May Forever Prevent Anonymity

Brian Souza and Brad Hart

Advances in biology are driving innovation and discovery in new directions. These advances hold great promise for finding unknown causes of disease and human health. However, they also carry unprecedented risks for the protection of personal identity and privacy. Compounded with these advances are concomitant leaps in technology across multiple domains, such as artificial intelligence (AI), advanced chemical analysis, and biometrics, resulting in a revolution in human identification and tracking. Can the same algorithms that identify complex networks of genes responsible for cancer progression be used to identify people based on their individual biology? Can the methods that track disease be used for multiperson tracking against complex backgrounds found in large crowds? Can the secrets of the genome be unlocked through proteomic analysis? The short answer to these questions is "yes," and when we assess these questions in the framework of the current, real-time pace of discovery from advanced analytics of big data, we can imagine the next "breakthroughs" that challenge the very idea of who we are.

The amount of data available to scientists is vast and growing; discovering and sorting information that accrues at speeds never before imagined requires deep-learning methods. Our ability to predict biological outcomes without having to perform experiments on the bench is changing hypothesis-driven science because new thinking generates testable hypotheses that drive the real-time collection of data as it cycles back into a real-time model. Methods that identify inheritable genetic mutations, genetic damage, or dysregulation (faults in certain cell functions) can be used to identify people by examining small differences in their proteins with a power of discrimination far greater than what has been observed traditionally for complex DNA forensic analysis. These changes represent the beginning of a new era of biology: an era of both great promise and risk.

Commercial at Home Genetic Testing and the Serial Killer in the Family Tree

The advent and surging popularity of direct-to-consumer genetic-testing services such as 23andMe and Ancestry.com have had significant consequences for law enforcement—effectively increasing the pool of available DNA profiles with which to compare forensic evidence.[1] For example, to apprehend the Golden State Killer, Joseph James DeAngelo—who attacked victims in California from 1974 to 1986 and was responsible for at least 12 murders and over 50 rapes—investigators used an ingenious technique that linked DNA from crime scenes to genetic data from DeAngelo's relatives to identify him as a prime suspect. DNA from the crime scene had sat in evidence storage for decades. Its genetic "fingerprint" was absent when

searched against existing criminal DNA databases and, therefore, useless because it had yet to be linked to anyone. If DNA from the crime scene is not in an existing database, then it is essentially orphaned. Frustration with these types of cases is nothing new and has been an issue since the advent of DNA forensics.[2]

What modern forensics lacked, industry developed with home genetic testing and the study of family genealogy. In the case of the Golden State Killer, police used a free service, GEDmatch, to compare the DNA from the crime scene to a database of volunteered genomes in the hopes of finding a match.[3] The suspect's DNA was not in the database; however, a relative's was, and the pool of suspects was reduced to a single family tree. Subsequent law enforcement investigation identified DeAngelo, a former police officer, as a prime suspect. As investigators continued their surveillance, discarded samples containing his DNA were obtained without DeAngelo's knowledge and were a match for DNA recovered from crime scenes decades earlier, resulting in arrest and conviction. "Cold-case" task forces continue to find previously unknown trends or patterns for unsolved crimes originally thought to be unrelated but that were, in fact, the work of a single individual.

While this case highlights the benefits of "crowdsourced" genetic information for identifying criminals, it also presents a dilemma for those who wish to maintain some degree of privacy regarding their genetic makeup. Recently, the Department of Defense (DOD) urged all military personnel to avoid direct-to-consumer DNA testing.[4] This guidance was made in part to ensure that potentially erroneous results from one of the many rapidly growing testing companies would not hamper future opportunities for members of the military. For example, false positives for any number of genetic diseases could disqualify soldiers from a variety of career tracks, especially those requiring particular physical traits. This concern is tied to the fact that members of the military, in contrast to the public, are not protected from discrimination by the Genetic Information Nondiscrimination Act (GINA). However, there is an additional underlying, but less specific, set of risks articulated in the memo.[5]

These risks are associated with contributing one's genetic information to the ever-growing pool of data being generated as millions of individuals seek information about potential health predispositions and ancestral lineage. The DOD memo warns of potential exposure of personal and genetic information that could have "unintended security consequences." While no specific threat or vulnerability is disclosed in the memo, the risk of having the genetic information of personnel with sensitive national security roles—be they members of the law enforcement, military, or intelligence communities—available openly presents several problematic scenarios. While a detailed examination of these issues is beyond the scope of this chapter, one can imagine how rapid DNA analysis combined with large data sets and AI-enabled analysis tools could provide an advantage to an adversary attempting to track, locate, or confirm the identity of either an individual or even members of their family. As analysis methods advance and more is discovered regarding the predictive capacity of genetic information, it will be increasingly possible to isolate and target specific

health-related susceptibilities or even the physical appearance of individuals. The implications of these trends for national security are only now coming to light.

Finding Genetic Differences and Finding People

While DNA is the gold standard for human identification, DNA profiles have real-world limitations. The integrity of DNA is limited because it can degrade quickly under normal environmental conditions. This can mean that, instead of full DNA profiles, typically comprising 18 or more standard markers, limited profiles that are missing some number of markers only provide partial information. Given the relatively small number of markers in a full profile, missing markers impact the overall power of discrimination that can be achieved, reducing the utility of such data significantly. Additionally, samples that contain mixtures of DNA from multiple individuals quickly become intractable as the number of contributors rises and the overall picture becomes less clear.

These issues combine to limit the utility of samples collected from crime scenes, for example, or from items or locations of interest to investigators. However, direct analysis of DNA is not the only way to reveal detailed genetic information. Other biological methodologies for uncovering identifying details of the genetic code have been developed recently. These methods seek to circumvent some of the critical limitations of DNA analysis, allowing for the identification and tracking of individuals based on their genetic code, even in cases where time and/or environmental conditions would have degraded the DNA itself or where multiple individuals contribute to a sample such that a traditional DNA analysis would be confounded.

The most prominent of these approaches involves the application of an area of biological analysis called "proteomics." The rapid advance of instrumentation available for chemical and biological analysis of complex samples has enabled a level of detail to be extracted from even the most complex samples.[6] The combination of high-resolution mass spectrometry and advanced data-analysis tools allows for even single amino-acid mutations to be identified in a complex sea of proteins from a given sample. This has been a key development given that the mechanisms of biology dictate the primary structure of proteins, the actual sequence and identity of each amino acid, is determined directly by the genetic code. Therefore, a sequence-level analysis of protein structure becomes simply another way to understand the genetic sequence of an individual. The protein becomes a high-fidelity echo of the DNA. Importantly, this new source of genetic information is not often subject to the same limitations as DNA. Protein degradation over time or under harsh environmental conditions is much slower than that for DNA because of the nature of differences in their chemical structures, especially for samples such as hair or shed skin cells. Additionally, the nature of the analysis means that, in some cases, a single individual can be identified from a sample containing many contributors. Thus, harsh conditions such as those found on the battlefield or in a crash site would not destroy vital evidence of individual identity.

Exploiting Predisposition to Disease or Stress Response to Better Assess an Opponent

Research efforts are underway to identify the underlying genetic drivers for a host of physical and mental diseases. Some studies have found biological markers that map to stress pathways during auditory processing of language.[7] These data suggest that words, and the way they are delivered, can result in epigenetic and immune responses in the person receiving a verbal message. In other words, "sticks and stones may break your bones, but words may also cause lasting physical damage." The field of human social genomics—as described by work from Steven Cole at the University of California, Los Angeles[i8]—has opened the door to biological-marker analysis for stress response and stress repair in individuals affected by trauma as well as for the identification of factors that may predispose a person to poorer (or more favorable) clinical postevent outcomes. Data that help medical professionals determine risk factors, including those related to stress-related traumatic injury, could be used to vector personnel away from duty that is associated with severe stress from combat. Knowledge of how an adversary uses this information to select individuals either resistant to such stress or that recover rapidly may inform readiness and capability for that opponent. With enough data, it is conceivable that a bigger picture of an adversary fighting force could be formed, highlighting its physical and mental strengths and weaknesses.

Similarly, methods that analyze human DNA for biomarkers related to both susceptibility to and repair from stress could be informative during recruitment and selection of individuals for high-stress roles such as special operations forces. However, the data sets required to make accurate assessments are likely to be enormous. Additionally, advance study of the accuracy of these performance biomarkers requires testing over a period of time for a group of individuals undergoing a selection process to compare both among the group and to a baseline study.

The Death of Anonymity and Its Impact on the Special Operations and Intelligence Communities

Technology convergence across multiple domains has made traditional methods of obfuscating identity obsolete. Obtaining significant levels of anonymity has become an almost impossible task, and it is going to get even harder. When it comes to leveraging technology to maximize authoritarian control, China leads the way. As of 2019, China reportedly had over 350 million surveillance cameras. By 2021, that number is expected to be close to 600 million.[9] Coincident with the rise in the number of cameras is the adoption of AI and related technologies, including facial recognition, on a massive scale. Moreover, China is not limiting its growing network of surveillance to within its borders. For example, in Kampala, the capital of Uganda,

i Scientific literature is growing in human social genomics, and analysis of life experiences that influence gene expression have identified changes that occur in response to adversity. Increase in the expression of proinflammatory genes combined with decreased antiviral responses drive a conserved transcriptional response to adversity (CTRA). (See Cole.)

Chinese companies have installed thousands of cameras equipped with facial-recognition technology, established manned monitoring centers, and provided training and assistance to the Ugandan government ostensibly to help fight crime.[10] The proliferation of such capabilities will support authoritarian governments and make anonymity in such countries extremely difficult. These trends would be amplified if such tracking systems are cross-referenced with genetic databases.

The rapid emergence of applications for AI has been observed across a wide range of public and private domains, including autonomous vehicles, personal electronic assistants, healthcare diagnostics, smart search algorithms, and targeted marketing. The integration of ubiquitous sensing elements—such as positional, movement, audio, video, and health sensors—within AI-driven electronics and other products allows for the concomitant generation and analysis of massive amounts of information. Often these processes are completely opaque to the user. Persistent, ubiquitous connectivity of nearly every kind of consumer electronic device means that integrating and exploiting this data across enormous population sets is a real and active area of exploration for both beneficial and, presumably, nefarious purposes. Societal acceptance of the inherent invasiveness of these technologies speaks to a couple of issues. The first of these is a basic lack of understanding of such systems and just how much of an individual's life and information is captured and shared by the tools themselves. The second is the perception that the benefits of these tools far outweigh the potential risks. In the latter case, the risk potential is not applied uniformly across the population. For special operations forces (SOF), the Internet of Things is a double-edged sword that can reveal key insights about an adversary but also broadcast valuable data about our own strengths and weaknesses.

Implications of the Convergence of Advanced Biology and Technology

The effects of the loss of anonymity on society in general notwithstanding, the implications for national security professionals and warfighters are dramatic. Simply put, it is a challenging time to be a spy. Techniques, tools, and procedures (TTP) that have been the mainstay of intelligence and law enforcement tradecraft over the years should be expected to lose effectiveness as counterintelligence activities become less focused on physical surveillance and more on data fusion, enabled by AI and other data-science-based approaches. Identity is now tied less to superficial appearance and more to behaviors and physical characteristics that are increasingly difficult to mask. When combined with advanced genetic and proteomic analysis methods and a deeper understanding of the underlying genetic drivers for key physical, physiological, and mental predispositions, significant opportunities exist to develop "personalized" approaches to tracking and potentially affecting individuals. Critically, we are entering a phase where previously unrelated technologies and sensing modalities can more easily be integrated autonomously to create rapidly a new type of identity profile that will be nearly impossible to confound.

Like most instances where technology and security intersect, both pros and cons exist regarding the convergence of these technologies. They enable unprecedented ability to reconstruct events and allow perpetrators of egregious attacks to be tracked and apprehended. As SOF and the intelligence community navigate this brave new world, it will be essential to stay on the cutting edge of these techologies both to reap their benefits and counter their use against us.

Endnotes

1 Starinsky-El baz, Sigal, et al. "DNA Kinship Analysis of Unidentified Remains that Led to a Murder Investigation," *Forensic Science International*, 2019. 300: e20-e23.

2 Guerrini, C. J., et al. "Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique." PLoS Biology, 2018. 16(10): p. e2006906; Kolata, G., and H. Murphy, "The Golden State Killer Is Tracked through a Thicket of DNA, and Experts Shudder." *New York Times*, 2018. 27; Phillips, C., "The Golden State Killer Investigation and the Nascent Field of Forensic Genealogy." *Forensic Science International: Genetics*, 2018. 36: p. 186-188.

3 Wickenheiser, Ray A., "Forensic Genealogy, Bioethics, and the Golden State Killer Case," *Forensic Science International: Synergy 1*, July 2019, 114-125.

4 Murphy, Heather, and Mihir Zaveri, "Pentagon Warns Military Personnel against At-Home DNA Tests," New York Times, December 24, 2019.

5 Baruch, Susannah, and Kathy Hudson. "Civilian and Military Genetics: Nondiscrimination Policy in a Post-GINA World" *American Journal of Human Genetics* 83(4), October 10, 2008: 435–444.

6 Parker, G. J. P., et al. "Demonstration of Protein-Based Human Identification Using the Hair Shaft Proteome." PLoS ONE, 2016. 11(9): e0160653.

7 Mehl, M.R., et al. "Natural Language Indicators of Differential Gene Regulation in the Human Immune System." *Proceedings of the National Academy of Sciences USA*, November 2017, 114 (47), 12554-12559.

8 Cole, Steven W., "Human Social Genomics," *PLOS Genetics,* August 2014, Vol. 10, Issue 8, e1004601.

9 Lin, Liza, and Newley Purnell, "A World with a Billion Cameras Watching You Is Just around the Corner," *The Wall Street Journal*, December 6, 2019.

10 Parkinson, Joe, Niholas Bariyo, and Josh Chin, "Huawei Technicians Help African Governments Spy on Political Opponents," *Wall Street Journal*, August 15, 2019.

SECTION 3

THE MATERIALS WORLD: POSSIBLE SOF APPLICATIONS

CHAPTER 12

Additive Adversaries: Enabling and Supporting the Warfighter with Additive Manufacturing

Lawrence E. Bronisz and Dominic S. Peterson

Introduction

During the Apollo 13 mission, an oxygen tank in the service module exploded two days into the lunar journey.[1] This loss of oxygen made the command module cold and dark, forcing the crew to take refuge in the lunar excursion module (LEM) as a "lifeboat." Because three crewmembers were in the LEM, instead of two, the carbon-dioxide scrubbers depleted rapidly. Luckily, the crew had a team in mission control working on the problem and devising a solution to fit the scrubbers from the command module into the LEM machinery (literally fitting a square peg into a round hole). This example demonstrates how a team supporting personnel in the field (or in space) can help solve truly intractable problems, including when supplying a solution directly to a remote operation is impossible.

Similarly, the warfighter is supported by an increasingly large team of people who are not in the field. This assistance allows soldiers to focus on the mission at hand and use their support team to work on solutions to problems that might arise. Additive manufacturing (AM) will play an important part in supporting the warfighter of the future. To begin with, deployed AM resources will bring the supply chain to forward operating bases and possibly into the field. The ability to make replacement parts in the field will reduce (but not eliminate) the need to bring large stores of spare parts with the troops. In addition to regularly used parts, a three-dimensional (3D) printer[i] (or collection of machines) will be able to fabricate the needed spares or unique solutions on demand. This development will disrupt the current thinking about both how to qualify a part for use on an expensive asset and the protocols for inspection and quality assurance required in the field (as opposed to what is required for a major military procurement).

Such a scenario is not entirely futuristic; it bears similarity to the highly skilled medieval blacksmiths and armor bearers, who were critical components of medieval military operations, providing customizations, ergonomic fit, and research and development for the warriors they served. In the medieval period blacksmithing (and metallurgy) was esteemed and known as *metallaria*, one of the seven mechanical arts.[2] Blacksmith shops were the "makerspace"[ii] of society until the Industrial Revolution made them almost obsolete.[3]

i 3D printing, also called additive manufacturing, is a family of processes that produces objects by adding material in layers that correspond to successive cross sections of a 3D model.

ii A makerspace is a collaborative workspace inside a school, library, or separate public and/or private facility for making, learning, exploring, and sharing where participants use high-tech to no-tech tools.

The advent of ubiquitous AM has popularized makerspaces. The digital river of high-bandwidth internet has spread AM and clever design practices to the entire world extremely quickly.Capability constraints of our adversaries (both nation-states and subnational groups) are eroding, putting these groups on a more even technical footing with the United States.[4] Ubiquity of technology availability has leveled the playing field significantly. Geek Youtube channels and a worldwide generation of maker kids is a substantial development.We can expect our adversaries to use modern technologies to offset our superiority, and we must be prepared to presage and counteract them. Using new tools in a distributed network of substantially independent makerspaces is a way both to project force and to counter adversarial agility. AM is substantially changing the "invention factory versus invention factory" arena of modern warfare.

The authors propose that competitive invention factories be promulgated throughout the Department of Defense (DOD) to sharpen leadership and creative skills and to exploit new technologies effectively. Pitting military or contractor red/blue teams[iii] against each other at a professional level (above college robot competitions) will drive both offensive and defensive advancement. Often innovation is "merely" a combination of existing methods or technologies. For example, high-speed arrows were a highly disruptive technology and were quickly enhanced by adding fire and poison.[5] Combining groups of competitors will bring awareness of disparate combinable technologies from different personal experiences and knowledge. Promoting a competitive invention-factory culture will yield new offensive weapons and the defensive means to counter attacks from our adversary's invention factories. As the AM field has evolved, so has the terminology used to describe the technology; "rapid prototyping" has been superceded by term additive manufacturing. However, rapid prototyping is perhaps the most important term with respect to the speed of competitive technology development.

Applying AM successfully to change the status quo will require a substantial overhaul of and transition in the design-and-development approach for modern military equipment. Starting with the worldwide RepRap[iv] hobby AM community, makers used AM to produce a substantial portion of the components comprising AM machines (i.e., machines printing more machines). In the commercial sector, Hewlett Packard's (HP's) Multi Jet Fusion (MJF) ink-jet-based AM machines have been designed with the goal of applying AM intelligently to machine components, resulting in a commercial AM machine with a 50 percent AM part content. The change in the design process was made possible by reducing part count by printing complex "combined-part geometries," thereby replacing a several-part assembly with fewer, more complex AM parts. Change in the supply chain will need to begin by creating designs specifically producible by AM at the start of new projects. In wartime, passion is born of necessity and survival. In

iii Red teams are used against blue teams in war-gaming and software security to find and mitigate weaknesses.

iv RepRap is short for "replicating rapid-prototyper."

peacetime, passion, when it occurs, comes from other sources, such as a personal geek interest, financial gain, and, yes, even patriotism. The challenge leaders and makers face is like building and maintaining a fire: sparking, fueling, feeding, and sustaining AM passion and creative potential to achieve patriotic disruption.

Beyond rapid prototyping in the development and customization laboratory, mass customization and specialization of AM will be of particular value to the soldier of the future. The people who know best what is needed to operate a piece of equipment more efficiently are those who use it daily. By communicating with the home team, the soldier will be able to get a quick turnaround design for a tool to solve their immediate problem or even to make their job just a little easier. The robustness of 3D printers is improving, and the technology will eventually advance to the point that the end user will become an operator, needing only to load part geometry files and change out consumables, much like computer numerical control (CNC) machine operators are not required to be fully trained machinists.

"New Path" Vision

AM has existed for only a few decades. Chuck Hull built the first successful AM machine in 1983 and a commercial unit was sold in 1987. His stereolithography apparatus (SLA) solidified parts layer-by-layer on a stage in a vat filled with ultraviolet (UV) curing resin.[6] This machine brought awareness to the technology and sparked a rapid proliferation of invention. Another method, selective laser sintering (SLS), which fuses parts layer-by-layer in a moving powder bed, became commercial in 1989.[7] Excitement drove investment and more invention.

With a pace similar to the rapid advancement of AM, in the next three decades, monumental disruption of offensive and defensive warfighter realms will be driven by applying AM technology successfully to military applications. Here are some reasons why:

- Tool development and qualification as well as threat response will happen in almost real time.
- AM will upend each aspect of the DOD's entrenched, serial cycle of specification, design, qualification, and modification/requalification (headquartered in the world's largest office building, the Pentagon).
    - An analogy for how AM will affect the military complex is the toy industry, which subsists by a rapid, complete product cycle with repetition and rapid change to hit holiday sales spikes. Currently, much military acquisition "moves" at a glacial pace; fast-track leaps are rare and driven by desperation and necessity, once the need becomes obvious enough to influence change agents.
- The wide availability of AM equipment and expertise will enable practitioners to develop solutions on a short time cycle in conjunction with broader strategic objectives.

3D-printed firearms provide an example for how quickly this technology can advance. The first 3D-printed gun was produced by Defense Distributed in 2012, mostly to show that it could be done.[8] Only five years later, the US Army printed almost every component for a grenade launcher (the RAMBO).[9] In a short time period, the technology advanced from demonstration to something designed for US military use.

Figure 1. Comparison of the first 3D-printed gun (the Liberator, sterolithography [STL] geometry files were released to the public in 2013), left, and a US Army Armament Research, Development, and Engineering Center (ARDEC) 3D-printed grenade launcher (RAMBO) in 2017, right.

Despite the previous example, the upending change expected from AM will probably not happen rapidly unless a number of "killer app," game-changing, fielded successes can be achieved and communicated as "new path" examples for the future. For instance, ubiquitous open and secure high-bandwidth global communications are already available to drive a dynamic specification environment allowing (and requiring) rapid response to emerging threats and opportunities for asymmetric warfare. These technologies will be essential to enabling the warfighter to take full advantage of AM technologies. It may be too much to expect frontline soldiers to design parts, but their ideas should be listened to and their thoughts, requirements, and desires need to be communicated to specialists such as designers. This communication may include teleconferencing, photos, or even scans of what is needed and the ability to design and deploy the solution in the field rapidly. In his work on terrorist innovation, Adam Dolnik observes, "a key determination of innovation success lies in the specificity [specifying] of the problem [to be solved], the solution of which would offer significant advantages."[10] This also applies to nonterrorist organizations.

Such shifts toward rapid action are not without precedent in the military-industrial complex. As World War II loomed, the conceptual design of the Pentagon was completed in 4 days, including a weekend (14 days before Congress authorized it), under the driving leadership style of General Brehon Somervell.[11] With minimal documentation, groundbreaking occurred September 11, 1941, only four and a half weeks after drawings were started. It was estimated that the design alone would take at least one and a half years. Designed in conjunction with its construction, the

Pentagon became what is still the world's largest office building in a mere 16 months. The budget was blown by a factor of four to six, but it got done. Somervell's man on the ground was General Leslie Groves. Many rules were bent, broken, or ignored to achieve a rapid result.[12] In contrast, One World Trade Center took over eight years to design and build with only half the square footage.[13] Groves learned much from Somervell, who stated:

> *Successful management depends on five factors. The first factor is a precise understanding of the job to be done. The second is qualified and capable men in key positions. The third is a workable organization properly adapted to the job to be done. The fourth is a simple, direct system for carrying on the activities involved in the job. The fifth is a positive method for checking on the results. Given any three of these five, a business or agency can probably function with fair success. Four of them operating together will result in much better than average efficiency. However, it requires all five to create the best management obtainable.*[14]

Ironically, the rapidly built Pentagon now houses residents who primarily plod toward military modernization in a slow serial approach, with some notable, recent exceptions. The entire November-December 2016 issue of *Defense Acquisition, Technology, and Logistic*s magazine, a publication of the Defense Acquisition University, detailed many of the pilot programs, studies, and efforts underway to embrace AM. Secretary of the Navy Ray Mabus is quoted stating:

> *Too many new assets are mired in outdated bureaucratic practices that were developed for another era. As we enter the age of cyber, unmanned systems, and advanced manufacturing, we cannot allow these overly complex, form-over-substance, often useless, and too often harmful, practices to slow or prevent development of some game changers, while simultaneously giving our potential adversaries the competitive advantage.*[15]

As a result, the Joint Advanced Manufacturing Region (JAMR) effort, via an integrated project team, produced the prototype TB-100 Expeditionary Manufacturing Mobile Testbed (EXMAN) for modular fieldable AM technologies.[16]

The US Army's Rapid Equipping Force (REF) was created in 2002 after US soldiers realized the need for nonstandard equipment to meet the demands of new terrain, warfare tactics, and their assigned missions.[17] Since then, the REF has met challenges as diverse as enhancing soldier mobility, providing improved surveillance in austere locations, equipping operational energy sources, and enhancing communications. The REF is the Army's quick reaction capability for getting urgent

matériel solutions into the hands of soldiers. The organization is able to do this both through unique authorities and by maintaining a presence near the point of need.

New AM Technologies

New AM technologies are emerging with key development loci. Practioners focused early AM technologies on process technologies that could print 3D parts without much concern for structural properties. Developers of the earliest AM technologies concerned themselves with form and almost never with function (which is why early AM was known as rapid prototyping).In reality, most 3D processes are capable of producing "near-net-shaped" parts. The next leap in AM development is to make parts with engineering properties similar to those that can be produced via traditional manufacturing methodologies. A number of new 3D technologies extend two-dimensional (2D) lithographic technologies.

Digital light processing (DLP) technology, which came from optical projection, has revolutionized and greatly expanded the original AM technology segment of stereolithography. It began with rastering a laser over a vat of UV curing resin. DLP optical resolution provides feature detail at increments of tens of microns[v] in combination with much higher volumetric build rates. These technologies have traditionally relied on acrylate[vi] chemistry, which enables high write speeds but produces relatively weak and poorly aging parts. More recently, additional materials have been explored, substantially broadening the types of materials that can be printed using DLP, including printing ceramics (postprocessed by sintering) and making composites by mixing chopped carbon fiber, and even graphene, into the resin. In addition, DLP technologies are evolving to enable much more rapid part production. The very limits of speed have been explored by Carbon 3D, which can produce a full-size part in a matter of a few minutes by controlling the quenching layer of the polymerization region.[18] The disadvantage of this approach is that it still requires extensive postprocessing to complete the cure of the polymer.

HP's MJF technology has leveraged 2D ink-jet printheads to apply picoliter droplets[vii] to powdered polymers delivering rapid build rates, which are ten times faster than fused deposition modeling (FDM) and SLS (at half the cost of SLS), in tough, useful, strong polymers including nylon and polyurethanes and with detailed features.[19]

In additional developments, the Polyjet UV curable 600 dots-per-inch (dpi) ink-jet technology from Objet Geometries of Israel, now merged with Stratasys, has been able since 2008 to mix two feedstreams in variable ratios, resulting in graded polymer part fabrication.[20] New technology from X-Jet with finer 1600 dpi ink-jet-applied nanoparticle-loaded polymers has demonstrated production of metal and ceramic

v For comparison, a human hair is about 90 microns in diameter.

vi An acrylate is a compound derived from acrylic acid, a colorless, corrosive liquid that readily forms polymers and used to make plastics, paints, synthetic rubbers, and textiles.

vii A picoliter is one-trillionth of a liter. It is so small that the eye cannot see it, and a raindrop can hold thousands of picoliters.

parts with fine detail.[21] A similar feedstream mixing will likely be able to produce graded and cermet composite materials with unusual and useful material properties. Evolve Additive is commercializing electrostatic transfer printing, which first came about with the Xerox machine in 1959.[22] Evolve Additive Solutions has developed an AM system that uses electrostatic transfer printing to build layers of 3D parts in fine detail with standard polymers at high volumetric build rates reportedly 50 times faster than other technologies.[23] Based on preliminary reports, the technology can deposit 28 micron polymer layers in four seconds, implying a peak volumetric build rate of over 600 cubic centimeters per hour (cm^3/h) over their large build envelope.[24] The company debuted the technology publicly at FomNext in Frankfurt, Germany in 2019.

Postprocessing

Postprocessing of AM parts, the lethal "rhinoceros in the cubicle," is often glossed over and perilously ignored. This oversight has stunted or killed many otherwise successful AM applications. The novel ability to produce complex geometries rapidly, unachievable by conventional subtractive fabrication, often mesmerizes the beholder, while the removal of support material and postfinishing are not taken into account. Currently, the postprocessing steps for many AM technologies are labor intensive. In order to realize the promise of AM, these operations must become fully automated. The type of postprocessing required depends on three factors: the material,[viii] types of support structures,[ix] and surface finish.[x]

Material Advances: Making Functional Parts Possible

Ultimately, the utility of additive manufacturing to produce parts for soldiers in the field will depend on the material. Three basic classes of materials are available for printing: metals, polymers, and composites (including ceramics). The greatest improvements in AM technology have been made when utilizing robust materials that fulfill engineering requirements. Progress will continue along the same lines, but there will likely always be some trade-off between the material that can be fabricated by AM and the ideal material for an application. For instance, some stainless steels can be printed, but not all are readily available in powder form. The AM processes, especially laser sintering, cause much more rapid heating and cooling rates than conventional casting, forging, and heat-treating processes. These rapid heating rates cause significant vaporization of some alloy constituents, while rapid cooling greatly affects grain morphology, sometimes resulting in better (but certainly different) material performance.

Printing aluminum parts is possible, but the raw material can be explosively hazardous because of its affinity for oxygen. Also, there will likely be some limitations to the number of printing materials taken into the field, and the military may need to

viii For example, does it require heat treating or a postcure step? What type of excess material needs to be removed?

ix As well as how they need to be removed.

x That is, if a machining or polishing step is required.

decide what subset of materials will be used in forward operating environments. In particular, metal printing has the largest hurdles before being deployed closer to the end user, partly because the metal powders must be melted to be fused together, usually by using a laser or electron beam. Both of these methods are power intensive, and the raw material is heavy.[xi] These limitations mean that metal AM will require significant logistical support. Finally, metal AM instruments require fastidious cleaning before changing between materials; this fact will likely lead to a subset of materials being available in forward operating bases compared to a more complete set available to and strategically stockpiled by the home team.

The second major class of materials available for AM, polymers are perhaps the most versatile class of materials and can be produced by every AM technique. Of the different AM materials, primary polymer has easily modified chemical properties, which opens up a wide range of existing polymers that can be used for AM. The synthesis of new polymers is occurring as a result of the "new production step" of photocuring. The greatest drawbacks to polymer AM parts is they may not meet engineering requirements. Polymers are softer and weaker than metals and are often susceptible to aging, especially in oxidative environments or when exposed to UV light. However, polymer AM will be the most useful in the field as it can be deployed with minimal power and can be used readily with different materials. In 2016, the utility of polymer AM was demonstrated by the first 3D printer installed on the International Space Station, which has since been used to print wrenches, sensor covers, and airflow monitor holders.[25]

In addition to basic metals and polymers currently used for additive manufacturing, there is both great interest in and a need for producing composite materials, which are made from multiple constituent materials that when combined create a material with far superior properties than either material individually.[26] The promise of these materials lies in their high strength and stiffness coupled with reduced weight. The specific materials that could be formed are broad, including ceramics and carbon fiber reinforced and infused with nanoparticles (including metals and semiconductors). Using these materials will enable technicians to tune the final part to have specific material and physical properties and, possibly, multifunctionality designed into them.

A range of researchers across the world are studying composite materials intensely. Glass, carbon, and aramid[xii] fiber reinforcment of injection-molded parts has become common in structural applications, and fiber-reinforced polymers have been demonstrated in laser-sintered AM components. The pace of filled composite materials in fused deposition modeling (FDM) is already demonstrating usefulness. Axially disposed long fibers in FDM are allowing directional "layup" for focused

xi The density of steels is about 8 grams per cubic centimeter (g/cm^3), compared to about 1 g/cm^3 for polymers.

xii Aramid fiber is the generic name of a group of synthetic fibers. Commonly known commercial brands include Kevlar, Twaron, and Nomex.

strength in FDM[xiii] parts. In 2019,Desktop Metal Corporation introduced a hybrid flat fiber combined with FDM high-temperature thermoplastics (PEEK and PEK).[27] This brings tape-layup composites into the AM realm. The trick to employing composite materials for AM is developing a method to enable printing of the two phases while ensuring the loading material can be incorporated in sufficiently high concentrations. This can be done by either adjusting the rheological conditions of the material being printed or modifying the loading material to ensure it can be cross-linked with the polymerization mixture.

Parts designed to be built with different material properties at the voxel-by-voxel[xiv] level are starting to be realized. HP is developing and has demonstrated some voxel customization with their MJF technology.[28] Tailoring modulus (stiffness) and even electrical conductivity are part of this development, which is determined by custom ink-jet applied chemistry individually applied to each voxel of a printed part. The Massachusetts Institute of Technology has demonstrated a voxel-by-voxel AM machine, which switches dynamically between multiple polymer feedstreams to enable adjacent voxels in a layer to be different materials.[29]

One of the most exciting areas in additive manufacturing (and perhaps the most difficult to predict) is the ability to make parts with multiple materials, including materials with graded structures, which can have significant advantages in designing parts with highly tuned functionality.[30] In addition, composite materials can be produced that behave differently in different environments. The new area of "four-dimensional (4D) printing" focuses on making materials that will behave differently over time depending on the environment. This "programmable matter" produces a product that reacts with environmental parameters (e.g., humidity, temperature, light). The current results are academically focused and demonstrate behaviors such as folding/unfolding depending on the temperature and/or relative humidity.[31] This nascent technology already has some exciting potential applications, including self-assembling structures, integrated sensing, and actuating systems for aircraft, soft robotics, self-deployable antenna arrays, valves, and active springs. The composite structures that will be available by 2050 will provide additional tools and capabilities to the warfighter, although printing for this type of technology may not be available in forward deployable environments.

The use of additively manufactured parts will require some change in thinking about how materials are produced, inspected, qualified, and put into service. The current process for putting a new material into service is quite lengthy, especially on major assets or parts critical to the operation of a piece of hardware. AM parts have initially been used in areas considered less critical, such as certified AM toilet seat covers.[32] Although the amount of inspection and qualification applied to these parts is

xiii FDM AM technology deposits extruded roads of thermoplastic polymer (now with embedded reinforcements) like a hot-glue gun in layers.

xiv A voxel is a volumetric (three-dimensional) element for visualization, like a pixel is a two-dimensional element for an image.

still high. As the military community and services become more comfortable with the technology, the process for using new AM materials will likely continue to relax, which will eventually enable most replacement parts to be created, inspected, and qualified as needed in the field. Currently, AM parts are inspected for dimension, surface finish, and internal composition, using techniques such as X-ray computed tomography (CT). X-ray CT inspection of AM parts will likely be fieldable over the next several decades (just as medical-imaging techniques have become mobile).

More than a Change in Technology, a Change in Thinking to Enable Agile Operations

For much of human history, customized equipment has been reserved for the rich and powerful (such as officers and royalty). Rank-and-file military personnel have made do with mass-produced, standard equipment. Additive manufacturing will enable "mass customization" to be rolled out to all military personnel. This will fundamentally change how the military can operate to become a more agile organization. Throughout the history of armed conflict, significant advantages have belonged to the side that can innovate and develop novel solutions, possibly to problems that were not identified as ones before the solution. Things like the invention of the stirrup, short swords, shields, armor, gunpowder, and rifling have had profound effects on the outcome of conflicts.[33]

Mass customization enabled by additive manufacturing will enable equipment users to have customized tools they need to be successful in their mission. This will lead them to think further about other useful equipment. Soldiers will need to be tied to AM practitioners who can make their visions a reality. These "makerspaces" will be staffed with an interdisciplinary group able to take ideas, design a solution, identify material needs, and rapidly iterate the idea to produce a high-quality solution. However, centralized power and control tends to affect innovation negatively.[34] Therefore, to operate more creatively and to ensure AM is a useful technology for the future, these units must be staffed properly. The personnel selected will need to be highly collaborative, be able to operate at a high tempo, and understand a wide range of AM technologies, limitations, and constraints. Depending on the development of these units over the next few decades, they could be staffed with military personnel or civilian contractors.

Leadership and Innovation

For AM to fulfill its potential, the right leadership must be in place. Thomas Edison's Menlo Park, Bell Labs, and the Manhattan Project provide examples of leaders applying innovative solutions to pressing problems. Consider for a moment a plethora of mini-Manhattan projects enabled by AM, but without a blank check and during peacetime, and, therefore, a lack of wartime mentality.

Edison's Menlo Park

Edison has been described as the greatest US inventor, substantially because of his early investment in the infrastructure that enabled routine invention. His Menlo Park laboratory became the first institution set up with the specific purpose of producing constant technological innovation and improvement. It produced the carbon button microphone (making the telephone practical), the phonograph, the incandescent light bulb, and power-generation and -distribution components, including generators, switches, plugs, and sockets.[35] Edison stated purpose for his Menlo Park laboratory was to "invent some minor thing every ten days and some big thing every six months."[36]

In his biography of Edison, Quincy Shaw gives a synopsis of the Menlo Park invention factory:

> *What Edison created was not the stereotypical factory of the Industrial Revolution, with workers performing repetitive actions designed to lower costs and raise efficiency—it was a bustling hub of creativity and shared intent. Edison hired proud and skillful craftspeople and opened up his lab to them. In return, he expected them to dedicate themselves to the projects to which they were assigned. Anyone who did not would soon leave, usually of his own volition.*
>
> *The atmosphere in the Edison machine shop was open and congenial. When a new employee asked about rules, Edison told him, "Hell, there ain't no rules here! We're trying to accomplish something." The men were given freedom to experiment on their own, testing new ideas, materials, and work methods.*
>
> *This is not to say that Edison was a pushover or that he spoiled his staff. He was a tough and demanding employer. . . .*
>
> *When it came to hiring craftsmen, Edison put more stock in their manual skills and their perseverance in solving real-life problems than he did in their formal education. He had little respect for college degrees and even less for the standard curriculum of the time. He denounced traditional schooling for "taking up too much time teaching things that don't count. Latin and Greek—what good are they? They say they train the mind. But I don't think they train the mind half as much as working out practical problems." As he told an interviewer late in life, "Doing the thing itself is what counts."*[37]

He and his men invented many big things to fulfill his original intent by doing what counted.

Bell Labs

If there is a formula to creating technical innovations, Bell Labs had solved it, especially in the second half of the twentieth century.[38] Bell Labs is a premier industrial research laboratory with innovations and contributions in a wide range of fields.[39] Indeed, Bell Labs invented not only new things but also new ways to invent them.

One of the key leaders of Bell Labs was Mervin Kelly, director of research from 1936 to 1944 (during which time Bell contributed to several critical military advancements, including radar), executive vice president from 1944 to 1951 (when the transistor was invented), and president from 1951 to 1959. The overall research structure of Bell Labs under Kelly's leadership focused efforts in three areas: basic research, systems engineering, and the design and development of new devices. However, Bell Labs'real innovation was in bringing together a critical mass of talent and building a "living organism" structure in which social and professional exchanges encouraged back-and-forth discussions in order to refine ideas. One of Bell Lab's official policies was that anyone (even the most junior staff members) could approach an expert in the field with questions and the expert was expected to interface with the junior staff member.

In addition to the structural interactions enabled by the scientific and engineering staff, Bell Labs enabled a parallel subculture of technical assistants, who were the keepers of technical secrets and tricks and maintained the lore of how things got done at Bell Labs. These personnel may have been less educated than the scientific and engineering staff (often having a high school education), but they were highly valued for their technical intuition. They were often the types of people who could take apart and put back together an engine or watch.[40] Bell Labs also had the ability to provide resources, the foresight to hire talent (even if there was not a current business need), and the culture to enable collaboration and to encourage long-term thinking.

Bell Labs provides an example of how additive manufacturing can have the highest impact for the military; a structure will need to be instituted to enable the highest level of performance. This culture must enable designers and engineers to have a free-flowing transfer of information and ideas to solve problems, while also enabling the print technicians to have a significant role in contributing to how parts are made and ensuring the success of the final products. In addition, some resources should be provided to explore solutions for more intractable problems that may not have immediate payoff.

General Groves

As a final example of the importance of leadership to the proper implemetation of AM for SOF, the Manhattan Project relied on extraordinary technical innovation and also on equally extraordinary leadership abilities. When the War Department wanted a leader for the Manhattan Project, General Somervell pointed to General Groves, his subordinate on the War Department general staff, and then left to lead military supply for WWII. General Groves was the right leader. Perhaps his strongest skill was

detecting and selecting leaders to whom he could reliably delegate critical tasks.[41] Groves superintended over the $2 billion (World War II dollars) Manhattan Project and spent an additional $6 billion during the war on other construction projects. The only larger World War II procurement line item was $3 billion for the B-29 bomber development and production.

Groves had a virtually a blank checkbook but was extremely focused. He mitigated risk with parallel paths. He chose Robert Oppenheimer to herd the "crackpots" at Los Alamos, who did so with aplomb and ultimate technical success. Examining Groves's leadership style, Oppenheimer commented:

> *First, General Groves is the biggest S.O.B. I have ever worked for. He is most demanding. He is most critical. He is always a driver, never a praiser. He is abrasive and sarcastic. He disregards all normal organizational channels. He is extremely intelligent. He has the guts to make difficult, timely decisions. He is the most egotistical man I know. He knows he is right and so sticks by his decision. He abounds with energy and expects everyone to work as hard or even harder than he does. Although he gave me great responsibility and adequate authority to carry out his mission-type orders, he constantly meddled with my subordinates. However, to compensate for that he had a small staff, which meant that we were not subject to the usual staff-type heckling. He ruthlessly protected the overall project from other government agency interference, which made my task easier. He seldom accepted other agency cooperation and then only on his own terms. During the war and since I have had the opportunity to meet many of our most outstanding leaders in the Army, Navy, and Air Force as well as many of our outstanding scientific, engineering, and industrial leaders. And in summary, if I had to do my part of the atomic bomb project over again and had the privilege of picking my boss I would pick General Groves.*[42]

Conclusions and Vision for the Future

The ultimate goal of any organization is to ignite the passion and drive to deliver the best possible solutions to problems. At their essence, the motivations are an inner individual drive. As our previous examples show, multiple sources exist for this motivation. One is the necessity and the essential nature of the work, as was the case with the Apollo 13 mission, building the Pentagon, and executing the Manhattan Project. While this type of motivation is strong, it can also be driven by fear of negative consequences; therefore, it may not be sustainable over a long period of time or with large numbers of people. Another major motivation may be based on a particular reward (e.g., pay, promotion, recognition, or overarching personal enjoyment). Identifying people who are driven by the love of something and not an external reward is difficult, but doing so yields excellent results over the long term.

Opportunities to identify and recruit these types of people can include competitions or events where people design and implement ideas—such as with robot battles, drone racing, or car racing—and are committed, creative, and technically savvy. SOFWERX—a platform that helps solve challenging warfighter problems at scale through collaboration, ideation, events, and rapid prototyping—represents a substantial functioning example of this approach.[43]

Additive manufacturing will lead to some fundamental shifts in parts procurement. AM will facilitate the ability to build parts on an as-needed and just-in-time (JIT) basis, which will reduce the need to perform life-of-program buys for critical spare parts and rapid turnaround for a small-volume part. Early military applications of AM have already been realized. While this could have an adverse effect in some of the procurement practices, one could also envision a range of AM shops near major military installations to service the major, routine needs for military AM parts. Such a system might enable a broad manufacturing base across the country, which would, in turn, enable innovation and be available to service other industries. Such a manufacturing base would also tie into more robust quality-acceptance and testing requirements.

Finally, as aforementioned, proper leadership is the key to obtaining the full disruptive value of AM. To enable mass customization, to empower front-line units to envision what they need, and for makerspaces to produce needed equipment, the highest levels of leadership will need to trust lower levels of the organization. This may include delegating some the decision-making authority; however, it also includes ensuring expectations are clear and all levels understand their responsibilities for overall mission success. Quoting George S. Patton, "Never tell people *how* to do things. Tell them *what* to do and they will surprise you with their ingenuity."[44]

Endnotes

1 Lovell, J., Kluger, J., *Lost Moon: The Perilous Voyage of Apollo 13*, Houghton Mifflin Company, 1994.

2 Johannes Scotus Eriugena (ninth century) in his commentary on Martianus Capella's early-fifth-century work, *The Marriage of Philology and Mercury*.

3 Walton, S. A., *An Introduction to the Mechanical Arts in the Middle Ages*. 2003: University of Toronto.

4 Dolnik, A., *Understanding Terrorist Innovation: Technology, Tactics and Global Trends*, New York: Routledge, 2007 1.

5 Levy, J., *Fifty Weapons that Changed the Course of History*, London, Apple Press, 2014, 18.

6 Hull, C. W., US Patent 4,575, 330, *Apparatus for Production of Three-Dimensional Objects by Stereolithography*, Filed August 8, 1984, Published March 11, 1986.

7 Deckard, C. R., US Patent 4,863,538, *Method and Apparatus for Producing Parts by Selective Sintering*, Filed October 17, 1986, Published September 5, 1989.

8 Daly, A., *Socio-Legal Aspects of the 3D Printing Revolution*, London: Palgrave, 2016, 54.

9 Burns, Seung-kook "Sunny," and James Zunino. "RAMBO'S Premiere," Army ALT Magazine, Science and Technology, sMarch 1, 2017, https://asc.army.mil/web/news-alt-amj17-rambos-premiere/, accessed 23 December 2019.

10 Dolnik, A., *Understanding Terrorist Innovation*, 15.

11 Vogel, S. *The Pentagon*, Random House, 2007, 37, 48.

12 Vogel, *The Pentagon*, 124, 316.

13 Greene, E and Salo, E., *Buildings and Landmarks of 20th and 21st Century*, Santa Barbara: Greenwood, 2018, 260; Dupré, Judith, One World Trade Center: Biography of the Building, New York: Little, Brown, 2016, 69.

14 Ohl, John Kennedy. *Supplying the Troops: General Somervell and American Logistics in World War II*. DeKalb, Illinois: Northern Illinois Press, 1994, 67.

15 Remarks by the Honorable Ray Mabus, Sea-Air-Space Exposition, April 15, 2015; https://www.navy.mil/navydata/people/secnav/Mabus/Speech/SAS_Final%20AS%20PREPARED%20(2).pdf, accessed on 2/27/2020.

16 Greene, D., Holzworth, K. "Great Expectations in the Joint Advanced Manufacturing Region," Defense Acquisition Magazine, https://www.dau.edu/library/defense-atl/p/Defense-ATandL---November-December_2016, 54, accessed 23 December 2019.

17 "Army REF: About Us," US Army, https://www.ref.army.mil/AboutUs, accessed 23 December 2019.

18 Tumbelston, J. R., et al., *Continuous Liquid Interface Production of 3D Objects*, Science, 2015, 347, 1349-1352.

19 Varotsis, Alkaios Bournias, "HP MJF vs. SLS: A 3D Printing Technology Comparison," 3D Hubs, https://www.3dhubs.com/knowledge-base/hp-mjf-vs-sls-3d-printing-technology-comparison/, accessed February 27, 2020.

20 Wohlers Report 3D Printing and Additive Manufacturing Worldwide Progress Report, Wohlers Associates, Inc., 2014, 29, 78.

21 "XJet Introduces Updated Product Line," *Intercam—Int. Ceramic Rev.*, 68, 16 (2019).

22 "Happy Birthday, Copy Machine! Happy Birthday, Copy Machine!" Morning Edition, October 23, 2013, accessed February 13, 2020, https://www.npr.org/2013/10/23/239241106/happy-birthday-copy-machine-happy-birthday-copy-machine.

23 Sweeney, M. A., Mang, M. E., LaFica, S., US Patent 10,557,056, Filed December 31, 2015, Published July 6, 2017.

24 Arnold, Katelyn, "AM 101: Selective Thermoplastic Electrophotographic Process (STEP)," Additive Manufacturing, December 6 2019, https://www.additivemanufacturing.media/blog/post/am-101-selective-thermoplastic-electrophotographic-process-step retrieved 27 Feb. 2020.

25 Hurley, B., "3D Printing and Space Exploration: How NASA Will Use Additive Manufacturing," NASA Tech Briefs, Jan. 17, 2020.

26 Ohl, *Supplying the Troops*, 67.

27 Press Release: "Desktop Metal Set to Transform Continuous Fiber 3D Printing," Lynda McKinney (press contact), 1 November 2019. https://www.desktopmetal.com/news/desktop-metal-set-to-transform-continuous-fiber-3d-printing/.

28 Dignan, L., "HP Launches 3D Multi Jet Printers That Aim to Deliver Fully Functional, Color Parts with Systems in $50,000 range," ZDNet 2/5/2018: https://www.zdnet.com/article/hp-launches-3d-multi-jet-printers-that-aim-to-deliver-fully-functional-color-parts-with-systems-in/ accessed 2/27/2020.

29 Doubrovski, E. L., et al., *Voxel-Based Fabrication Through Material Property Mapping: A Design Method for Bitmap Printing,* Computer Aided Design, 60, 2015, 3-13.

30 Toursangsaraki, M., *A Review of Multi-Material and Composite Parts Production by Modified Additive Manufacturing Methods*. arXiv.org, e-Print Arch., Phys., 2018: p. 1-25; Yang, L., et al., Functionally Graded Ceramic Based Materials Using Additive Manufacturing: Review And Progress. Ceram. Trans., 2016. 258 (Additive Manufacturing and Strategic Technologies in Advanced Ceramics): 43-55.

31 Kuang, X., et al., "Advances in 4D Printing: Materials & Applications," Adv. Funct. Mater., 2019, 1805290, 1-23.

32 Vialva, Tia. "$10,000 Air Force Toilet Seat Covers Reduced to $300 Thanks to 3D Printing." 3D Printing Industry, July 12, 2018, https://3dprintingindustry.com/news/10000-air-force-toilet-seat-covers-reduced-to-300-thanks-to-3d-printing-136102.

33 Levy, *Fifty Weapons that Changed the Course of History*, 2014.

34 Dolnik, A., *Understanding Terrorist Innovation: Technology, Tactics and Global Trends*, New York: Routledge, 2007 p. 17.

35 Jehl, Frances, *Menlo Park Reminiscences* Vol 1, Dearborn, MI: Edison Institute, 1936, 33.

36 Jehl, *Menlo Park Reminiscences*, 105.

37 Shaw, Quincy, *Edison*, New York: New Word City, 2016, pp. 56-57.

38 Gertner, J., *The Idea Factory: Bell Labs and the Great Age of American Innovation*. 2012, New York: Penguin Press, 149-152

39 Gertner, *The Idea Factory*, 1-3.

40 Gertner, *The Idea Factory*, 153-155.

41 Norris, Robert, *Racing for the Bomb*, Hanover, NH: Steerforth Press, 2002, p. 541-542.

42 Nichols, Kenneth D., *The Road to Trinity,* New York: William Morrow, 1987), 108.

43 "Welcome to SOFWERX," SOFWERX, 2020, https://www.sofwerx.org/.

44 Patton, George S., *War as I Knew It*, 1947, 357.

CHAPTER 13

Nanotechnology and SOF: Is Smaller Really Better?

P. Randall Schunk

Introduction—Smaller Is Better!

In *Shadow Warriors: Inside the Special Forces* (2002), Tom Clancy describes vividly the challenges special operations forces (SOF) faced during the Vietnam War, which were mostly related to excessive equipment weight and the lack of military intelligence in forward operations.[1] Numerous challenges Clancy describes had high-technology solutions that had not yet been invented in the 1960s. Simply put, SOF needed technology that was smaller, lighter, and higher-performing.

Fast forward 50 years: It is remarkable how many of these challenges have been surmounted, largely because of high-tech materials and devices that make objects small and light, enhance performance, and provide better real-time intelligence. Interestingly, the human dimension that dominated SOF operations in Vietnam remains paramount to maintaining advantage.[2] Perhaps somewhat surprisingly, nanotechnology (NT) underpins most human intelligence technologies. NT enables artificial intelligence (AI), the Internet of Things (IoT), sensing, radio-frequency and infrared (IR) communications, and other technologies that enhance the sense-think-act paradigm of "autonomy." NT can impact warfighter performance and preservation in still unimagined ways that present tremendous, but still latent, threat and advantage. Take for example the advances in body-armor technology enabled by NT.[3] Perhaps Tony Stark's (also known as Iron Man's) "nanite suit," in the *Avengers: Infinity War* (2018), will someday soon move beyond science fiction.

"Where did that come from?"

Bruce Banner (The Hulk)

"It's nanotech. Like it?"

Tony Stark (Iron Man)

Avengers: Infinity War

This chapter makes plain the current state of NT, its hype and overhype, its latency, and even its history, largely as it relates to challenges, needs, and gaps in special operations forces. In the field of NT, SOF need to be innovators, not problem solvers.4 In an environment of battlefield uncertainty, situations often devolve into disorder and chaos, weakening human performance; NT can aid in these situations. The benefits of NT in the human dimension are not fully realized, and perhaps represent a latency that can be used to gain strategic advantage.

Nanotechnology Hype: Real or Imaginary?

At lengths small enough to be considered "nanoscale," which has been widely accepted as less than about 100 nanometers (nm), physical phenomena are dominated by forces still relatively mysterious to humans. Even though these length scales are large compared to atoms or molecules, molecular forces control how matter behaves and interacts in a way that dominates material microstructure, thermodynamics, and motion. Successful nanotechnologies result when macroengineering tools, such as a microscope or laser, tame these forces, resulting in macroscale systems that benefit the warfighter. By controlling the chemistry of material structures, scientists can create other successful nanotechnologies, enabling materials design functionality. Some nanotechnologies are built simply on the integration of nanomaterials (particles of <100 nm dimension) into composites to enhance thermophysical properties or optical/electromagnetic properties. Though rarely a means to an end, NT enables and improves technology. Engineering at the nanoscale has created legions of technological possibilities, and society has already enjoyed the benefits.[5] However, technology developers must overcome challenges at the molecular scale to realize all that nanotechnology has to offer.

Nanotechnology is such a broad category it defies simple definition. NT started with wide-scale materials-science advances such as the electron microscrope in the 1960s; these advances brought fundamental molecular-scale chemistry and physics to "life" in the 1980s and 1990s. As a result, companies touting the "nano" brand began to pop up in the late 1990s and early 2000s. In 2000, President Bill Clinton championed the National Nanotechnology Initiative, providing a $225M budget. Numerous government agencies restructured their discretionary research and development (R&D) portfolios to include nanoscience and engineering. Nanotechnology exploded in popularity, with numerous start-up and multinational companies including NT as a core discipline or even a "product." However, in the early 2000s, many of the surviving start-up companies that flaunted their nanotech credentials rebranded themselves as materials or semiconductor companies, realzing nanoscience and the fundamental discipline known as *materials science* were synonomous.[6] NT enabled broader technologies that are realized at the macroscale. In the end, NT never had its "Facebook" moment or blockbuster debut in the stock market.

The chronological history of nanotechnology has been constructed in numerous locations.[7] Norio Taniguchi coined the term "nanotechnology" in 1974, in reference to the explosive growth of the nascent semiconductor industries,[8] but some argue the word stems from Richard Feynman's "vision" in 1959 that resulted from the advent of electron microscopy (EM) and the ability to "see" atoms and molecules for the first time.[9] Davis Baird provides a compelling case that the real tools of nanotechnology were those based on scanning tunneling microscopy (STM) and its relatives (e.g., atomic force microscopy).[10] EM was just an imager, but STM enabled atomic manipulation. John Randall, et al., assert that "nanotechnology" circa 2018 has failed to live up to its potential and claim that while nanoscience flourishes and

has led to some exciting applications, nanoscale devices with proven reliability are still nonexistent beyond prototypes.[11] However, nanotechnology products enabled by nanomaterials—such as nanocomposites and nanoparticles for medicine—have become commonplace and can be credited for many technology improvements and breakthroughs. Randall, et al., base their assertion on simple sematics, as NT is much broader than he describes. Nonetheless, the assertion is worth further consideration, especially from a manufacturing viewpoint.

George Whitesides and J. Christopher Love were the first to review relatively nascent nanofabrication techniques and expose the plethora of possibilities and challenges.[12] They categorized process routes as either bottom-up—building up structures with nano building blocks or particles—or stamping, molding, or forming structures from the top down. One early conclusion emerged from this work: top-down soft lithography and optical lithography, the workhorses of the semiconductor industry, are the only scalable routes to nanodevices. Soft-lithogaphy has since achieved commercial scale, even though fabricating 3D logic devices like transitors remains challenging.[13]

The modern semiconductor industry is really a nanotechnology industry. It can control fabrication of the building blocks of transitors to scales of less than 20 nm using light and interferometric patterning tricks, and has done so while maintaining remarkable throughput. It has also created microdevices that provide platforms to study phenomena at the nanoscale.[14] Optical lithography is at its limit, however, and even with numerous tricks, the semiconductor industry is at the "end of silicon scaling."[15] Soft lithography will be critical in attempts to overcome this limit.

To build a nanoscale "system," or an object engineered at the sub-100 nm scale to achieve a certain function, one can do so best with the so-called nanoparticle. STM and related technologies prove an "atomic assembler" is not as far fetched as some have claimed.[16] Whether one will ever be practical is another matter. Nonetheless, bottom-up fabrication with nanoparticles may be a future and impactful latency. In fact, most nanoscale technologies revolve around nanoparticles with specific functionality. Readily manufactured carbon nanotubes (CNTs) have unique electronic properties that can improve electrochemical sensing and enable molecular-scale transistors.

Scientists can engineer nanoparticles with nearly any extraordinary property; examples include photoluminescence/quantum dots, tunable cargo-carrying porous particles for drug delivery, core-shell shape for dual functionality, and nanosheets for composite strengthening and lightweighting.[17] Nanomaterials can also be engineering to serve as sensors or taggants for trust technologies, such as tamper indicators and system authentication.[18] Essentially, nanoparticles can be made with chemical elements across the periodic chart, which can become a scientist's "palette" to create custom NT function and form (see Figure 1). The beauty of nanoparticles is that, unlike other forms of nanomanufacturing, such as silicon-CMOS, they can be dispersed as colloids into inks and processed with solution-deposition schemes and related digitally based additive-manufacturing approaches, such as ink-jet printing and liquid film coating, at much larger scales.

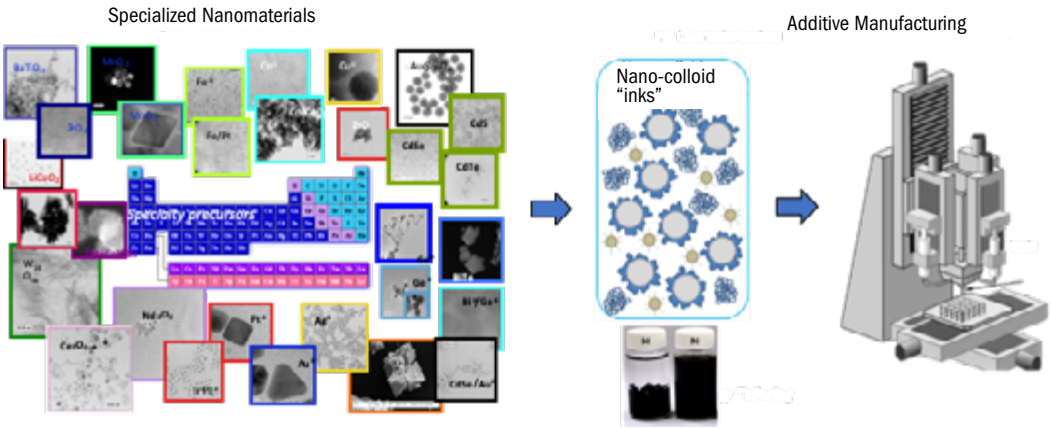


Figure 1 (acknowledgement: T. J. Boyle, A. Cook, N. Bell, Sandia National Laboratories).

Governments and private industry continue to invest in developing low-cost, scalable process technology at the nanoscale to meet consumer demands for electronic devices. National Science Foundation–sponsored engineering research centers at the University of Texas at Austin (www.nascent-erc.org) and the University of Massachusetts Amherst (umass.edu/chm/) provide examples of R&D efforts underpinning the integration of nanomaterials such as graphene and nanopatterning at scale. Department of Defense (DoD) investments, under the auspices of Manufacturing USA hubs,19 in packaging of Si-CMOS in functional-hybrid electronics stand to intersect with nanotechnology to meet the needs of IoT. These large-scale efforts attest to the plethora of remaining challenges of bringing nanotechnology to market. The primary challenge remains achieving practical fabrication for reliable devices and materials.

Nanotechnology and SOCOM/SOF

Nanotechnology is ubiquitous in today's military technology and impacts nearly all enabling technologies in SOCOM's primary mission. NT is most prevalent in mobile electronic devices—smartphones, global positioning system (GPS) units, and wearable electronics. Size-weight-and-power (SWaP) improvements, power-requirement reductions, and integrated sensors (e.g., cameras) all exemplify the benefits of NT. These devices serve many needs for SOF, as they can enable person-to-person and centralized communication, as well as numerous other functions. The central processing units of smart devices have transitors as small as 40nm, and their nonvolatile and universal memory can hold gigabytes of information because of nanoscale magnetic bits. The power source and display of smart devices are high density and fidelity because of small pixel sizes and integrated nanomaterials. Figure 2 illustrates the essential components of a smartphone/device and the underpinning technologies NT enhances.[20]

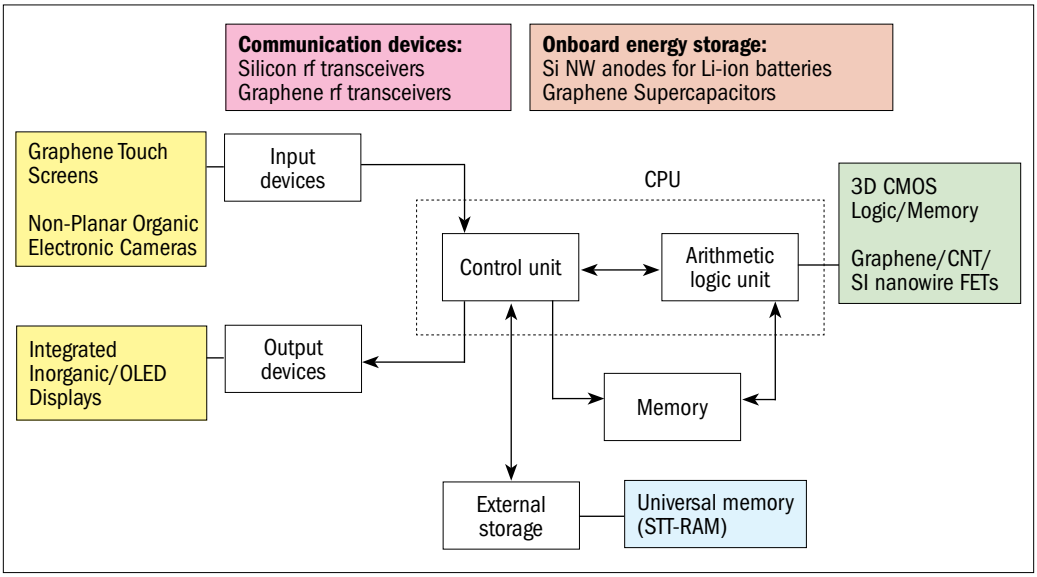


Figure 2. Essential components of a smartphone or other smart device and the underpinning technologies nanotechnology enhances.

Note that many of these NT enhancements involve the integration of nanomaterials (e.g., graphene, CNTs, nanowires) or pattenerning with printing/imprinting. Until about 2015, most nanoscience-device R&D efforts relied on slow and inflexible fabrication processes such as electron-beam patterning or thermodynamically defective (self-assembly) processes with limited capability for pattern complexity or high levels of process integration. Transformative nanomanufacturing systems and processes that enable mass production of economically competitive mobile computing are overcoming these challenges.[21]

Beyond electronics, many other NT benefits for SOF have already been realized. NT has made inroads in biometrics/chem-bio detection/mitigation, lightweight nanocomposite materials, and energy and environment technologies; many of these can be used for military applications. Extensive reviews exist on how nanomaterials have impacted these sectors, as well as other forms of nanotechnology and nanomanufacturing.[22] The Institute for Soldier Nanotechnologies at the Massachusetts Institute of Technology represents an excellent source of topical research and technology information.[23] For broader DoD-level applications of nanotechnology, readers can consult other reports.[24] For the warfighter, nontechnology benefits have been in play since the early twenty-first century, mostly in the realm of clothing, communications, blast protection, and navigation.[25]

A few other NTs deserve mention in this piece, as they have not been fully realized in the SOF community. Specifically, NT greatly enhances device performance in power generation, energy storage, and climate control by harnessing the sun[26] as well as in food technology, water resourse detection, and water desalination and purification.[27]

The burgeoning industry of "nanomedicine" benefits from NT, and, of note for the purposes of this book, includes gene editing as countermeasures for biological attack.[28] Human performance monitoring and enhancement with wearable detectors and controlled therapeutic delivery are already readily available in lightweight forms, and communication for real-time control and chem/bio sensitivity/selectivity are poised for ongoing investments. And, how about IR vision with implanted NPs in your eyes? It has already been proven to work in mice.[29] On the topic of light management, 3M, for example, has manufactured an all-polymer (no metal), 98 percent reflective (in the visible range) flexible film.[30] All these technologies are currently impacting, or will impact, the warfighter, enhancing battlefield performance through weight reduction, portable power, medical diagnostics and therapuetics, and overall survivability in difficult environments. Finally, in the area of lethality, researchers have realized breakthroughs in controlled morphology of energetic nanoparticles (explosives such as CL-20).[31]

Nanotechnology and Strategic Latency

In terms of strategic latency, four developing nanotechnologies will likely provide advantages to SOF. These include 1) fifth generation (5G) wireless communications, 2) chip-scale atomic clocks (CSAC), 3) sensorizing everything (i.e., IoT) and 4) graphene. Note that all, even graphene, amplify human-in-the-loop capabilities (e.g., communication, data analytics) and enable problem-solving in chaotic situations.

5G: Fast and Furious

5G cellular communications technology uses much higher radio frequences and enables data transfer at exponentially higher speeds than fourth-generation technology (4G). More important, 5G reduces latency, or the delay before data transfer begins, drastically. 5G also enables far more devices to be used within the same geographic area.[32] In short, 5G will enable up to three orders of magnitude improvement in data rates, bandwidth, and supported devices.

The impact of 5G on military operations has been covered extensively in the context of drone-to-drone unmanned aerial vehicle communication and battlefield uses.[33] The connectivity from operator to operator in the field, and with command and control, would be instaneous because of the high-speed data transfer and low-latency of a 5G network. Devices that might be networked for autonomous vehicles or drones will be able to commuincate in "real-time." Instantaneous, high-bandwidth communication enables the IoT more than any other technology does or can. So what role does NT play in maximizing the benefits of 5G? Look no further than portable electronic devices. Beyond mobile computing, 5G enhances a plethora of IoT devices (e.g., sensors, energy harvestors, central computing) because of the rapid communication not possible with 4G. In short, 5G will greatly amplify the benefits of any technology that enables SWaP improvements in devices.

Nonetheless, barriers can thwart any potential technology. For 5G networks, barriers include security and power consumption. In 5G, devices are identified in a

"flat" internet protocol vulnerable to cyber threats.[34] Ironically, the real benefit of 5G to SOF will be a reduction in computing-at-the-edge needs, and, hence, electrical power consumption. 5G greatly enables networking SOF with a central server for real-time decision analytics. Also, wearable devices do not require as much computing power; overall power needs decrease, as will the size and weight of devices.

Atomic Clocks: The Test of Time

Atomic clocks are the most accurate timekeeping devices and serve as reference clocks both domestically and globally.[35] They use the oscillation of single atoms or ions induced by an electromagnetic field as the frequency standard for timekeeping. Certainly, atomic clocks epitomize "nanotechnology." Precision timekeeping, as it pertains to global positioning and, hence, battlefield situational awareness in the absence of GPS, are indispensable to an SOF operation. As a side benefit, they can be used for ultrasensitive electromagnetic field detection (in, for example, hydrology, geology, and underground weapons storage). The National Institute of Standards and Technology (NIST) and the Defense Advanced Research Projects Agency (DARPA) have invested heavily in atomic-clock technology, and DARPA has funded the CSAC program,[36] which aims to condense such systems to small units that can be deployed easily on a warfighter.[37] While atomic clocks are being developed for both CONOPs for military operations and commercial production, rapid communication from asset-to-asset and person-to-person would only amplify the benefits of atomic clocks for soldiers. Perhaps the 5G breakthrough is the missing link for battlefield use of CSACs because the nanotechnology underpinning lightweight portable devices that thrive on rapid communication is already established.

Internet of Things: Sensorizing Everything

5G antennas and CSACs for eletromagnetic field detection are two forms of sensors. Nanotechnology has greatly enabled the "sensing" aspect of the sense-think-act triad of autonomy. Ubiquitous sensing enables capturing environmental signatures of any type, uploading and processing to determine a course of action to assess current states of operations, and gaining adversarial intelligence. Tunable nanomaterials, nanowires, and other nanostructures are instrumental in the development of highly selective and sensitive sensors for biologicals,[38] chemicals and explosives,[39] radiological materials (from scintillators and carbon nanotubes)[40] as well as for local temperature, biometrics from soldiers, and temperature of hard assets.[41] More sensors means more data and, therefore, the need for more processing. However, anticipatory analytics could be greatly enhanced if coupled with 5G and centralized computing. NT sensing devices enable AI and its deployment in real-time battlefield situations. NT has made sensors more sensitive, selective, and lower power, which amplifies the benefits of IoT.

Graphene: The Magic Material

The ubiquitous applications of graphene and related "2D" materials, together with close nanotube relatives (e.g., CNTs), should be evident in this piece. Graphene has extrodinary properties and has been called a "magic" material because it can be used for all sorts of technology applications. Basically, graphene is a monolayer of carbon atoms arranged in an hexagonal structure that possesses remarkable structural integrity. In fact, graphene is the lightest and strongest known material and also conducts heat and electricity better than most metals. Moreover, its chemical and thermal structures remain stable in extreme environments. Its unique "thinness" and structural flexibility mean it can be processed into useful devices and other performance-enhancing technologies . As a semiconductor, it can make light-energy devices, such as photovoltaics, thinner and more flexible. It can be used as an ultrathin antenna or a chemsorption surface to detect chemical and biological species. In flake form, it can be integrated into structural composites to strengthen and for lightweighting. It can even be used as a highly selective membrane for water purification.

Despite the challenges of growing graphene and related sheetlike materials in chemical vapor deposition (CVD) reactors and transferring them onto polymer substrates for integration into devices, many successes have already been realized.[42] Graphene has enabled many breakthrough technologies in electronics—including radio-frequency identification tags, low-cost sensors, and large-area, lightweight displays—that are difficult or impossible to realize with standard silicon or semiconductor integrated circuits. Plastic GHz/THz devices would provide unparalleled advantages to SOF, such as unbreakable platforms with arbitrary form factors that have favorable SWaP attributes. Graphene-based photovoltaics show remarkable efficiences[43] and could lead to an all-graphene flexible photovoltaic, which would be of great use in forward-base operations. In summary, the production and integration of graphene to useful devices in SOF are just beginning, so stay tuned.

Conclusion

Has nanotechnology lived up to the hype it received in the early 2000s? Absolutely. However, NT is rarely cited as a core-technology enabler. "NT inside" prevades numerous current and future technologies, including those of keen interest to SOF. This chapter only highlights a field that stems from centuries of materials-science, chemistry, physics, and engineering research and development.

Any reliable technology pursuit that can reduce size, weight, and power consumption, harvest energy, improve communication speed and bandwidth, provide data analytics, and improve human performance, endurance, and decision-making is paramount to advancing SOCOM's capabilities. NT has clearly been a key part of currrent technology advantage, and will be crucial to maintaining advantage. Some combination of all these capabilities culminate in the most important one: human performance and decision-making. NT with the human-in-the-loop is a force multiplier.

The United States is making significant investments to help accelerate nanotechnology, both in the government and private sectors; however, numerous challenges remain, most pertaining to manufacturing. The NT patent rates in Asia[44] have surpassed those in the United States, probably because countries in the region have increased research expenditures in high technology. Gary Pisano and Willy Shih predicted and provided evidence that the erosion of high-tech innovation leadership in the United States is a result of a decline in manufacturing.[45]

In the 1990s, US companies outsourced manufacturing to Asia and beyond, partly for economic reasons and partly to improve their images as innovators. Without a trained manufacturing workforce and manufacturing commons in the United States, innovation slowly eroded, particular in high-profit-margin high-tech industries, including nanotechnology. In recent decades, a number of US industries have lost their lead to Asia, and other regions, in manufaturing such products as flat-panel displays, advanced batteries, and other electronic and energy technologies. Industry is faced with the problem of determining when manufacturing is critical to innovation and when it can be safely outsourced to lower costs and reduce capital outlays. Currently, companies pursue the production of NT through low-cost processing routes such as roll-to-roll and additive manufacturing. Nanotechnology is likely to suffer the same fate as other sectors of the high-tech industry have.

Finally, quantum technologies are conspicuously missing from this piece. "Quantum" seems "nano," but it implies technology that relies on particles much *smaller* than nanometer scales (hence, the lack of attention given to it in this essay). Nonetheless, some quantum topics are worthy of discussion in the NT context. Atomic clocks represent technology clearly in this category, but what about quantum computing? Because of operating systems and software challenges, quantum computing will likely not be a game changer for forward operations until 2025 or beyond.[46] That said, quantum computing will be a key to AI advancement because of the power limitations that currently hamper high-performance computing technology. This piece also used "quantum" in another context. Breaking and reforming chemical bonds in a way that machines can control over large areas or in large volumes will be the basis for "nanomachines and nanopattering" at scales far smaller than current semiconductor or nanoimprint technologies. Atomic bonds are at the quantized state of matter, e.g. the particles that make up the atom. This author believes the new devices and form factors created by subnanotechnology, such as controlling bond breakage and formation precisely, will be revolutionary.

Endnotes

1 Clancy, Tom, with Carl Stiner and Tony Koltz. *Shadow Warriors: Inside the Special Forces*, Penguin, 2002.

2 Spulak Jr, R. G., *Innovate or Die: Innovation and Technology for Special Operations*. 2010, Joint Special Operations Univ Hurlburt Field FL.

3 Halsey, T. C., "*Electrorheological Fluids.*" Science, 1992. 258(5083): p. 761-766; Wagner, N. J. and E. D. Wetzel, Advanced Body Armor. 2010, Google Patents.

4 Spulak Jr, R. G., *Innovate or Die: Innovation and Technology for Special Operations*. 2010, Joint Special Operations Univ Hurlburt Field FL.

5 Paragon, H., "*7 Nanotechnology Examples That Already Exist,*" Aug. 9 2017, https://humanparagon.com/nanotechnology-examples.

6 Kelleher, K., "*Here's Why Nobody's Talking about NanoTech Anymore.*" Time Oct. 9 2015, http://time.com/4068125/nanotech-sector.

7 For one example, see www.nano.gov.

8 Taniguchi, N., "*Current status in, and Future Trends of, Ultraprecision Machining and Ultrafine Materials Processing.*" CIRP annals, 1983. 32(2): p. 573-582.

9 Feynman, R. P., *"There's Plenty of Room at the Bottom,"* California Institute of Technology, Engineering and Science magazine, 1960.

10 Baird, D., and A. Shew, "*Probing the History of Scanning Tunneling Microscopy.*" Discovering the Nanoscale, 2004. 2: p. 145-156.

11 Randall, J. N., et al., "*Digital Atomic Scale Fabrication an Inverse Moore's Law–A Path to Atomically Precise Manufacturing*. Micro and Nano Engineering," 2018. 1: p. 1-14.

12 Whitesides, G. M. and J. C. Love, "*The Art of Building Small*. Scientific American, 2001. 285(3): p. 38-47.

13 Willson, C. G., and M. E. Colburn, "*Step and Flash Imprint Lithography.*" 2002, Google Patents.

14 Schena, M., et al., "*Microarrays: Biotechnology's Discovery Platform for Functional Genomics.*" Trends in Biotechnology, 1998. 16(7): p. 301-306.

15 Segars, S. "*ARM Wrestles with Silicon, Battery Hurdles,*" August 19, 2011.

16 Drexler, K. E., *Nanosystems: Molecular Machinery, Manufacturing, and Computation*. 1992: John Wiley.

17 Purcell-Milton, F., et al., "Impact of Shell Thickness on Photoluminescence and Optical Activity in Chiral CdSe/CdS Core/Shell Quantum Dots." *ACS Nano*, 2017. 11(9): p. 9207-9214; P. Dogra, et al., "Establishing the Effects of Mesoporous Silica Nanoparticle Properties on In-Vivo Disposition Using Imaging-Based Pharmacokinetics." Nature Communications, 2018; Ghosh Chaudhuri, R. and S. Paria, "Core/Shell Nanoparticles: Classes, Properties, Synthesis Mechanisms, Characterization, and Applications." Chemical Reviews, 2011. 112(4): p. 2373-2433; University, N. "Stronger Graphene Oxide 'Paper' Made with Weaker Units," August 15, 2019, https://phys.org/news/2019-08-stronger-graphene-oxide-paper-weaker.html.

18 Cummings, E. B., et al., "Tamper-Indicating Barcode and Method," 2005, Google Patents; Carnicer, A., et al., "Security Authentication Using Phase-Encoded Nanoparticle Structures and Polarized Light," *Optics Letters*, 2015. 40(2): p. 135-138.

19 https://www.manufacturingusa.com.

20 www.nascent-erc.org.

21 Cooper, K., "NSF Nanomanufacturing Programs, DOE Workshop on Integrated Nanosystems for Atomically Precise Manufacturing," Berkeley, 2015.

22 Stavis, S. M., et al., "Nanoparticle Manufacturing–Heterogeneity through Processes to Products." *ACS Applied Nano Materials,* 2018. 1(9): p. 4358-4385; Nayfeh, M. H., Fundamentals and Applications of Nano Silicon in Plasmonics and Fullerines: Current and Future Trends. 2018: Elsevier.

23 lsn.mit.edu.

24 https://www.nano.gov/node/621.

25 "Military Nanotechnology—How Worried Should We Be?" Nanowerk, November 13, 2006, https://www.nanowerk.com/spotlight/spotid=1015.php.

26 Abdel-Motaleb, I.M. and S.M. Qadri, |Thermoelectric Devices: Principles and Future Trends." arXiv preprint arXiv:1704.07742, 2017; Kim, T.K., et al., "Tandem Structured Spectrally Selective Coating Layer of Copper Oxide Nanowires Combined with Cobalt Oxide Nanoparticles." *Nano Energy*, 2015. 11: p. 247-259.

27 Stavis, S.M., et al., "Nanoparticle Manufacturing–Heterogeneity through Processes to Products." ACS Applied Nano Materials, 2018. 1(9): p. 4358-4385; "Military Nanotechnology—How Worried Should We Be?" Nanowerk, November 13, 2006, https://www.nanowerk.com/spotlight/spotid=1015.php.; Cygan, R.T., et al., "A Molecular Basis for Advanced Materials in Water Treatment." *MRS Bulletin*, 2008. 33(1): p. 42-47.

28 Rappe, M., Sandia Research, 2017; Mirza, A. Z., and F.A. Siddiqui, "Nanomedicine and Drug Delivery: A Mini Review." *International Nano Letters*, 2014. 4(1): p. 94.

29 Gabbatiss, J., *Nanotechnology could grant humans 'super vision' after mice given power to see infrared*. 2019.

30 Hebrink, T., *Durable polymeric films for increasing the performance of concentrators*. Third Generation Photovoltaics, 2012. 39.

31 Bian, K., et al., "Exploration of Processing Parameters of Vacuum Assisted Micelle Confinement Synthesis of Spherical CL-20 Microparticles." *MRS Advances,* 2018. 3(11): p. 553-561.

32 Browne, J. *How 5G Could Impact the Military*. 2018; Mar 08, 2019, https://www.mwrf.com/defense/how-5g-could-impact-military.

33 Browne, J. *How 5G Could Impact the Military*. 2018; Mar 08, 2019, https://www.mwrf.com/defense/how-5g-could-impact-military; Campion, M., P. Ranganathan, and S. Faruque, "UAV Swarm Communication and Control Architectures: A Review. *Journal of Unmanned Vehicle Systems*, 2018. 7(2): p. 93-106.

34 Mohamed, A. F. and A. Mustafa, "Nanotechnology for 5G," *International Journal of Science and Research (IJSR)*, 2016. 5(2): p. 1044-1047.

35 NIST. A New Era for Atomic Clocks. February 04, 2014, https://www.nist.gov/pml/time-and-frequency-division/new-era-atomic-clocks-page-3.

36 DARPA. *Chip-Scale Atomic Clock*. 2017, https://www.darpa.mil/about-us/timeline/chip-scale-atomic-clock.

37 Knappe, S., et al., "A Microfabricated Atomic Clock." *Applied Physics Letters,* 2004. 85(9): p. 1460-1462; Hollberg, L. and J. Kitching, "Miniature Frequency Standard Based on All-Optical Excitation and a Micro-Machined Containment Vessel." 2004, Google Patents.

38 Pumera, M., "Graphene in Biosensing." *Materials Today*, 2011. 14(7-8): p. 308-315.

39 Soutter, W. "Nanotechnology in Explosive Detection." AZoNano; 2019, May 24, https://www.azonano.com/article.aspx?ArticleID=3089.

40 Hassan, T.A. *Development of nanosensors in nuclear technology*. in *AIP Conference Proceedings*. 2017. AIP Publishing.

41 Segev-Bar, M. and H. Haick, "Flexible Sensors Based on Nanoparticles." *ACS Nano*, 2013. 7(10): p. 8366-8378.

42 Wang, G., et al., "Direct Growth of Graphene Film on Germanium Substrate." *Scientific Reports*, 2013. 3: p. 2465.

43 Yong, V. and J.M. Tour, "Theoretical Efficiency of Nanostructured Graphene-Based Photovoltaics." *Small*, 2010. 6(2): p. 313-318.

44 Davis, Z. and M. Nacht, eds., *Strategic Latency Red, White, and Blue: Managing the National and International Security Consequences of Disruptive Technologies*. 2017, Lawrence Livermore National Lab (LLNL), Livermore, CA.

45 Pisano, G.P., and Shih, W., "Restoring American Competitiveness." *Harvard Business Review*, July-August 2009.

46 Chilton, A. Sept 17 2014, https://www.azanano.com/article.aspx?ArticleID=3251.

CHAPTER 14

The Disruptive Potential of Advanced Energetics

Bryce C. Tappan and Patrick R. Bowden

Introduction to Energetic Materials: Propellants, Explosives, and Pyrotechnics

As we introduce the concepts associated with advanced energetics for special operations forces (SOF), it is important to have a brief understanding of energetic materials and their historical relevance and advances before exploring related emerging technologies and their strategic latency. The "energetic materials" family consists of three categories: propellants, explosives, and pyrotechnics. The first two categories, propellants and explosives, rely on many of the same basic ingredients and design techniques and differ primarily on whether the charge is ignited via a thermal ignition to induce deflagration (burning) or a strong shock to initiate detonation. Meanwhile, pyrotechnics encompass thermites, intermetallics, fireworks, gas generators, and delay compositions, to name a few.

To a large degree, the chemical design of propellants and explosive relies on the elements carbon, hydrogen, nitrogen, and oxygen (CHNO), with chlorine present in oxidizers that have the perchlorate anion (as with ammonium perchlorate). Metals can be added to increase the overall heat of reaction; most often, this metal is aluminum (Al) but can also be other elements such as silicon (Si), magnesium, or titanium. On the other hand, pyrotechnics utilize a vast number of elements to provide different effects, such as heat, color, light, burning rate, or desired metal formation.

Through the years, research in explosives chemistry has led to advances in energetic materials, including materials that have nearly twice the energy density of 2,4,6-trinitrotoluene (TNT)—such as hexanitrohexaazaisowurtzitane (CL-20)—or have greater power than TNT but are extremely insensitive to accidental initiation—such as 5-nitro-1,2-dihydro-1,2,4-triazol-3-one (NTO) or 1,3,5-triamino-2,4,6-trinitrobenzene (TATB). NTO and TATB find use in insensitive munitions and insensitive high-explosive (HE) formulations. However, research continues in the development new HE materials that perform as well or better than 1,3,5,7-tetranitro-1,3,5,7-tetrazocine (HMX) but are also insensitive to shock, impact, and friction, like TATB. One method to achieve this goal has focused on the preparation of high nitrogen heteroaromatics because they tend to have high enthalpy of formation values; the higher nitrogen content often leads to slightly higher densities, which has led to outlier explosives such as 4,4'-dinitro-3,3'-diazofuroxan (DAAF), with roughly the power of the explosive Composition B (Comp B) but little response to impact, spark, or friction.[1] Explosive performance depends on density, but, to date, researchers investigating CHNO-type explosives have been able to achieve maximum densities of only 2 grams per cubic centimeter (g/cc), which is likely the physical limit.[2]

Adding metals, particularly aluminum, to explosives is a well-known practice, dating back to 1899 and 1900 in Germany with the first suggested use of Al as an

explosives additive.[3] Metals are added simply to realize greater energy densities in one of several regimes of the explosive process. Explosive regimes can be divided into three basic temporal stages: prompt reaction in the detonation (nanosecond to microsecond [ns-μs], i.e., within the Chapman-Jouguet [C-J] chemical reaction zone); reaction in the postdetonation early-expansion phase (4-10 μs); and late reaction contributing to blast effects (1-100s of milliseconds [ms]).

Work on mixtures of TNT and Al, termed tritonals, began as early as 1914 and was extensive by World War II, when the United States and British researchers discovered great effects in the third temporal regime of blast without detrimental effects to the prompt detonation regime.[4] Because of a lack of acceleration in detonation wave speed, the energetics community commonly believes no Al participation exists at the C-J plane. However, work by Melvin Cook *et al.* in the 1950s demonstrated that replacement of Al with an inert surrogate, like sodium chloride (NaCl), actually increased detonation velocity. Therefore, he postulated Al *does* react in the C-J plane; however, it is kinetically limited to endothermic reactions.[5] In contrast, later work by Gert Bjarnholt *et al.* did not see as significant a difference in detonation velocity when Al was substituted for the inert surrogate lithium fluoride (LiF) in TNT/RDX (cyclotrimethylenetrinitramine) admixtures.[6] However, this work showed a 55 percent increase in cylinder-wall velocity for late-time expansion for Al-added formulations versus an inert surrogate, with Al contribution roughly 4 μs after the passage of the C-J plane.[7] This observation correlated well with the work of Milton Finger *et al.* as well as others, given a small enough particle size of Al.[8]

Modern high-performance munitions applications typically contain explosives designed to provide short-lived high-pressure pulses for prompt structural damage or metal pushing, such as the HMX-based materials PBXN-14 or PBX 9501. Another important class of explosives, however, includes those designed for longer-lived blast output (enhanced blast) via late-time metal-air or metal-detonation-product reactions. An example of an enhanced blast explosive, PBXN-109, contains only 64 weight percent (wt%) RDX and includes Al particles as a fuel, bound by 16 wt% rubbery polymeric binder. The low wt% RDX results in diminished detonation performance, but later-time Al/binder burning produces increased air blast. To the extreme of metal reaction-based energetic materials are a separate class of fuel rich energetic materials referred to as "thermobaric" explosives, in which the metal loading can range from 30 wt% to as high as 90 wt%.[9] These explosives are fundamentally different from other enhanced-blast HE. As with such high metal loading, they are far from stoichiometric in terms of metal oxidation with detonation products; additionally, they have considerably lower detonation temperature and pressure, which also affect metal oxidation rates.[10] Therefore, such materials are well suited for late-time blast and thermal effects but not for metal acceleration.

A rare but fundamentally important class of materials that has only recently been exploited, known as "combined-effects" explosives, combine the favorable initial work output from the early pressure profile of a detonation wave with late-time

burning or blast and rely on specific ratios of metal to explosive as well as metal type/morphology and binder type. Preliminary results by the US Army Research, Development and Engineering Laboratory at Picatinny demonstrate both high metal-pushing capability *and* high blast ability are achieved by combining small size Al particles, conventional high-explosive crystals, and reactive polymer binders.[11] Researchers believe this combination is effective because the small particles of Al enhance the kinetic rates associated with diffusion-controlled chemistry; additionally, the ratio of Al to explosive was found to be of utmost importance. It was determined that at levels of ≥ 20 wt% Al, the metal reactions did not contribute to cylinder-wall velocity.[12] This result is not only counterintuitive but also an indication that for metal-acceleration applications, the bulk of current military explosives containing Al are far from optimal. To fully optimize combined-effects explosive, scientists would have to develop a system in which the binder is either all energetic/reactive or completely replaced with a high-performance explosive. Furthermore, while a fair amount of research has been performed on Al reactions in explosives, little is understood about the reaction of Si and boron (B) in postdetonation environments.

The Limits of Chemical Energy

To understand the disruptive potential of advanced energetics we must take a realistic approach to understanding what limitations we face from energy storage in chemical bonding. Explosive power is derived from three simple concepts held within their molecular structure: how much energy is held within the chemical bonds,[i] how much energy can be derived from the oxidization of the fuel molecules carbon and hydrogen,[ii] and how densely packed all of these molecules are.[iii]

TNT is the benchmark explosive to which we compare others, not because of its performance, but because of historical usage, ability to be melt-cast, relative insensitivity, and high chemical stability. Those qualities combined with a simple synthesis from cheap commodity chemicals enabled TNT to be produced at massive scales and used as a single component explosive or as a base in materials such as Comp B (60 wt% TNT + 40 wt% RDX), pentolite (50 wt% TNT + 50 wt% PETN) or tritonal (80 wt% TNT + 20 wt% Al powder), to name a few. Fast-forward 100 years or more after the first use of TNT as an explosive, and the most state-of-the-art explosive available is CL-20, which has less than 2 times the energy per unit volume as TNT and resides near the limit of practical chemical energy for a CHNO molecule. Other examples exist that may be slightly higher in energy than CL-20, such as hexanitrobenzene or octanitrocubane (1.999 and 2.35 times TNT, respectively), but their difficult and expensive synthesis make them more expensive than gold by weight, and their sensitivity and stability would likely limit their utility to explosives of only academic interest.

i Referred to as *enthalpy,* or heat of formation.

ii Referred to as the oxygen balance of the molecule.

iii Referred to as the theoretical maximum density or TMD.

These facts lead us to a simple thought exercise: if we have HMX that is 1.54 times TNT, why not just use 25 percent more in a munition to achieve the same lethality as CL-20 for a fraction of the cost? This thought exercise has merits in many circumstances but is actually flawed in some, which leads us to more in-depth consideration of the effects of energetic materials, entire system consideration, and the economics of lethality, discussed below.

In other approaches discussed in this chapter, the addition of reactive metals is applied to enhance the energy of explosives. In Figure 1, we see the energetic potential of some elements based on their heat of combustion with oxygen.[13]

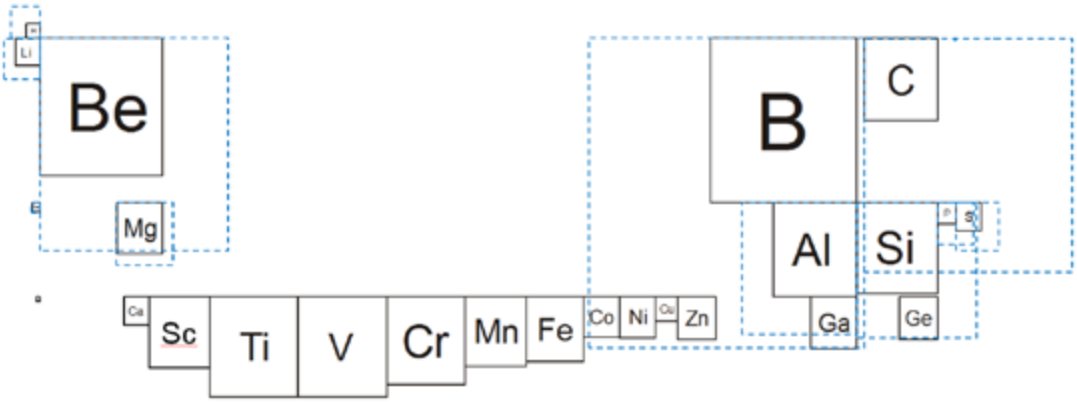


Figure 1. From Lindsay-Fajardo: "The Pyromaniac's Periodic Table," where the length of a side of each element's box (black) is proportional to the energy of oxidation per unit volume from the element's standard state. The dashed blue boxes indicate the energy of oxidation relative to the "free-atom limit," or the available energy if no bonding existed between individual elements.[14]

Figure 1 is an excellent visual aid from seminal work by Lindsay and Fajardo,[15] for indicating how much chemical energy is available for the combustion of elements in the first three rows of the periodic table. It also illustrates the "free-atom limit"—which is the energy tied up in the covalent or metallic bonding of the standard material—for oxidizing beryllium, B, and carbon atoms. However, no strategies exist to exploit this potential energy because of the physical constraints in chemical bonding. In other words, like single people, free atoms do not like to hang around with one another without seriously bonding.

Sensitivity Constraints of Energetic Materials

All explosives have geometric constraints on their functionality in detonation. Referred to as critical diameter/thickness or failure diameter/thickness, energetic materials can only sustain a detonation above a threshold condition. These conditions are dictated primarily by energetic functionality sensitivity, but also by structure, chemistry, proximity of oxidizer and fuel, and density factor in substantially. As a general rule

of thumb, materials that are more sensitive to stimuli—be it shock, impact, or friction—tend to have weaker bonds that are more prone to breaking. Thus, molecular explosives containing azido or peroxy bonds are most susceptible to initiation, followed by nitrate esters, nitramines, and nitroaliphatics.

When a material is "below its critical diameter," a detonation will fail because the size is too small. As a detonation propagates through a cylindrical explosive rate stick, curvature of the shock front develops as a result of edge effects (the boundary between the explosive and the confiner—for example, air, plastic, metal). The detonation is always driven orthogonally to the shock front. Thus, when curvature develops, less energy transmits axisymmetrically. As the diameter decreases, curvature becomes more pronounced, and eventually, too much energy is "lost" by the shock front being driven outward (instead of in the direction of propagation) and the rate stick will fail; hence, critical diameter has been reached. Since energy is required to drive the chemical-decomposition reaction of a detonation, the quicker the bonds break and reform into oxidized gaseous products (CO, CO_2, H_2O, N_2), the smaller the critical diameter will be. Thus, weaker bonds have smaller activation energies, thus allowing explosives to have smaller critical diameters, see Table 1 for additional information.

TABLE 1. BOND DISSOCIATION ENERGIES

Family	Energetic Functionality	Activation Energy (kcal/mol)
Nitroaliphatics	$C\text{-}NO_2$	70
Nitramines	$N\text{-}NO_2$	47
Nitrate Esters	$O\text{-}NO_2$	40
Peroxy	O-O	35
Azido	$M\text{-}N_3$	30
High Nitrogen Compounds	N-O-N; N-O-N-O	20-50

Energy Release in Energetic Materials

The measure of energy in an explosive is not an absolute quantity that can be used to compare all explosives; rather, the type of energy release must be considered. For example, simple black powder, the first explosive material formulated by humans, is a low explosive and does not detonate. However, it gets used in pipe bombs, where it certainly can deliver lethal effect. If one were to try to measure its explosive equivalency via a "plate dent" test, which measures the detonation pressure of an explosive, it would not dent the plate and therefore register as zero. Thus, other tests, such as ballistic pendulum, must be used to obtain a measure of performance in which that material can compete. The same goes for fuel-air explosive devices, possibly the most powerful explosives available when considering weight of material delivered to target. However, unless one measures air blast within or near the detonating gas cloud, it would be difficult to quantify explosive energy. So, let us consider where the lethal effects of an explosive are experienced.

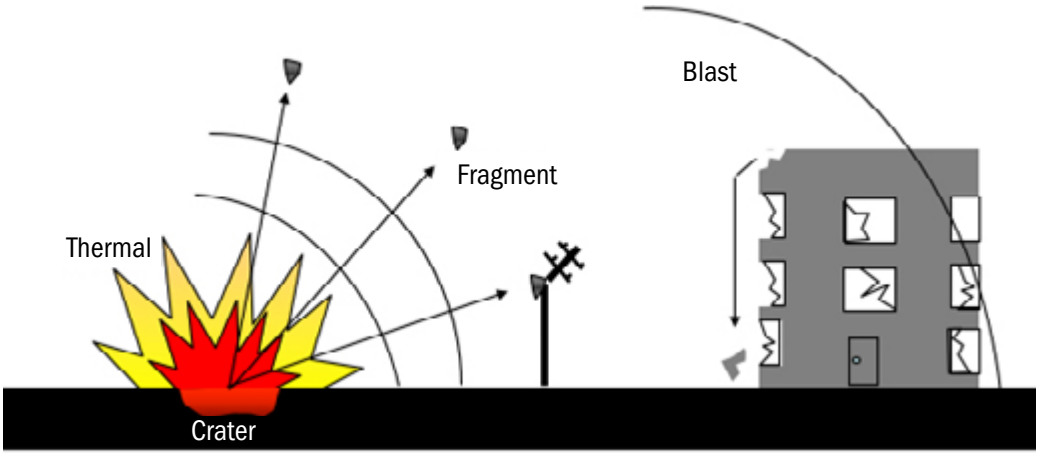


Figure 2. Graphical depiction of the basic effects of an explosion, with near-, mid- and far-field damage occurring from direct-pressure effects, thermal radiation within the fireball, fragmentation, and blast-wave damage.

Aerobic-Phase Energetic Materials

A general class of explosives for enhanced energy release can be thought of as aerobic, or air-breathing, materials. The conceptual function of these materials is that if you utilize ambient air as an oxidizer for the fuel contained within the explosive device, then you can carry more energy to the target. Most explosives carry there own oxygen to detonate (exceptions are materials like the azides, acetylides, and high-nitrogen molecules that rely only on highly positive heats of formation to decompose), and those with the greatest detonation pressure are able to burn all the the hydrogen to water and the carbon to either carbon monoxide or carbon dioxide. To put this in perspective, if you had to carry all of the air (23 percent oxygen by weight) to burn a gallon of fuel, you would have to carry over 100 pounds in addition to that gallon of fuel! Generally speaking, aerobic materials fit into the categories of thermobarics, enhanced blast explosives, combined effects explosives and fuel-air explosives.

Thermobaric explosives can be thought of as weakly detonating or even nondetonable materials often distributed with a strong, high-explosive center booster. Enhanced blast explosives are fuel-rich metal-containing detonable explosives. Combined-effect explosives are metallized explosives formulated in such a way that metal reaction will not only enhance blast but also accelerate metal. Finally, fuel-air explosives consist of a explosively distributed fuel with a second explosive event that will initiate a detonation in the mixed fuel-air cloud. Figure 3 illustrates the basic philosophy of when and how much blast pressure releases in the general categories of explosives. For simplicity, the TBX:EBX and CEX peak pressures are depicted as equal, but, in reality, the pressures should increase in the order listed.

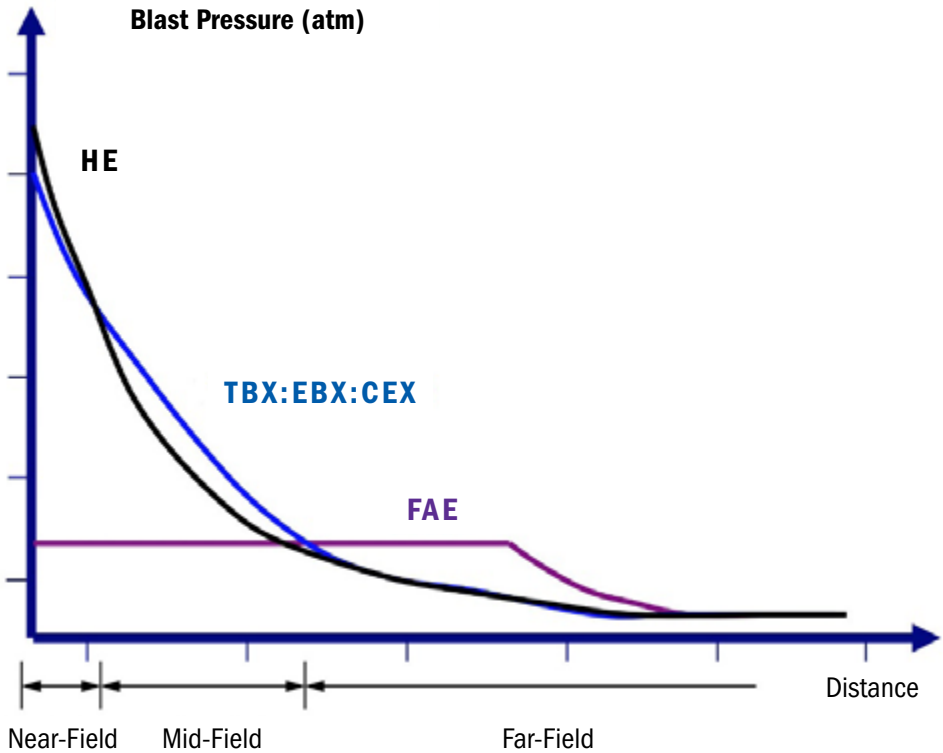


Figure 3. Idealized graphic on blast function of HE, TBXs, and FAEs, modified from David Frost and Fan Zhang. Primarily, HE will always provide a higher peak pressure, while TBX materials and FAEs will each have lower peak pressure but longer sustained pressure, leading to higher impulse. Most US and Canadian research, however, has indicated that ideal TBX performance is rarely or never achieved.

Fuel air explosives (FAEs) are a distinct category in which a fuel is distributed with an explosive and a secondary explosive charge will initiate a gas-phase detonation once fuel is mixed as optimally as possible with air. In terms of actual energy delivered per weight of munition, FAEs are the highest-energy explosive system, but they have a limited target set because of the type of impulse possible, with low peak pressures, as seen in Figure 3. However, they do have certain applications that produce devastating effects to large-area soft targets, such as exposed troops and unhardened structures, as in the iconic China Lake test seen in Figure 4. While large area targets may not be common for SOF, it is worth noting that developing nation-states may master this technology for use against US SOF. Often, FAEs are referred to as the "poor-man's nuke," based on the idea that the energy release is between that of a conventional HE and a nuclear weapon. While in some respects this may be true, in reality, the energy released is astronomically closer to a standard explosive than even the smallest tactical nuclear weapon.

Figure 4. FAE munition testing China Lake, circa 1970

Despite not being widely adopted by the military, FAEs have captured the imagination of cinema and state-level propaganda. In Figures 5 and 6, we see the examples in the movies *Outbreak* (1995) and *The Incredible Hulk* (2003).

Figure 5. Fictional FAE munition attack for viral outbreak area decontamination, *Outbreak* (1995).

Perhaps one of the more accurate fictional depictions of a FAE is shown in Figure 6 in *The Incredible Hulk*, which was clearly adapted from the China Lake test shown in Figure 4. As one would expect, Hulk, representing the hard target, sustains little damage.

Figure 6. Fictional FAE munition attack on the Hulk. Ironically, the frames display the ineffectiveness of FAEs against hard targets.

In 2007, a FAE device used in Russia propaganda straddles fact and fiction (Figure 7). While it is not impossible that such a device was developed, the comparison of the Russia "Father of All Bombs" and the American "Massive Ordnance Air Blast" is not accurate, and lethality mechanisms will differ.

Figure 7. Russian Television coverage of FAE munition deemed "Father of All Bombs."

Reactive Materials and Structural Composites

Efforts to obtain greater energy output from explosives have largely plateaued since the 1980s with the synthesis of dense nitramine explosives and optimization in metallized formulations to provide enhanced metal pushing and blast effects. Therefore, to deliver more energy to target, scientists and engineers have turned to replacing normally inert components with reactive materials, thus imparting greater blast energy from either anaerobic or aerobic reactions.

In fiscal year 2015, Los Alamos National Laboratory (LANL) successfully developed and tested a new reactive case concept using a simple, affordable, and effective design based on aluminum foil rolled and bound with either an energetic binder or epoxy. Figure 8 shows a scanning electron microscopy (SEM) image of a case cross section. The authors hypothesized the shock from the detonating HE would fragment the foil into extra fine Al particulates, free of a protective oxide layer (inherent to Al that is exposed to air), that would oxidize with air following an observable delay in ignition. The high-speed video records collected during testing showed better-than-expected results, with extremely prompt ignition of Al foil material and no perceivable delay. Reactive cases, were produced and filled with a high-energy cast-cure plastic-bonded explosive developed at LANL, which is based on HMX and micron-sized Al

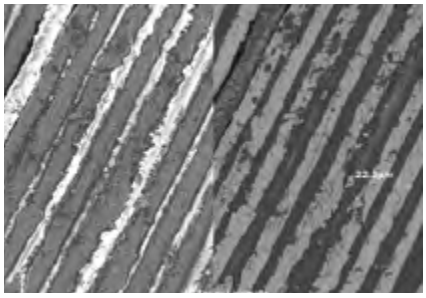


Figure 8. Cross section of Al foil epoxy-rolled case, showing Al thickness of ~22 μm.

bound with a glycidyl azide polymer (GAP) binder system. As shown in Figure 9 (right image), the combination of reactive case, bound by an inert epoxy, and LANL explosive substantially outperformed the baseline steel case, during blast overpressure testing.

Figure 9. Testing of reactive cases: Baseline in steel case (left) and LANL Al-Foil reactive case (right).

Such devices that provide dramatic enhancement in blast can produce a significant advantage in targets such as cave structures and bunkers where fragmentation devices are ineffective because of the lack of line of sight. This is of particular utility in battlefield scenarios that SOF's may encounter such as cave networks seen in Afghanistan, utilized in part by adversaries such as the Taliban. In fact, much of the historical development of these and other anerobic munitions has been driven by this need, first by the Soviet Union, and later the United States. Because the reactive material also displaces structural materials, weight gains can be realized over existing munitions. The same philosophy can be applied in reactive fragmentation, as discussed in the following section.

Reactive Fragmentation—Bringing Energy to Target

Reactive fragmentation cases are similar to reactive cases, but unlike the cases described above designed for prompt reaction, reactive fragmentation cases are designed to create large, fragments that will react upon impact with a target, essentially delivering more energy at the site of impact. These materials have significant utility against thin-skinned targets such as automobiles, aircraft, or missiles. Various Department of Defense (DoD) branches have funded this line of research, namely the Defense Threat Reduction Agency and the Office of Naval Research. The reactive chemistry applied is typically the same as that used for thermites and intermetallics or fuel-oxidizer mixtures with a highly electropositive metal (e.g., Al, Mg, Ti) mixed with a fluorocarbon binder system. While much of this technology will find antimissile or anti-aircraft applications, the utility for SOF is in enhanced energy delivery to automobiles both in standoff and emplaced munitions.

The primary challenges of reactive fragmentation are obtaining a fragment density that comes close to the steel being replaced as a munition casing, providing sufficient strength to survive detonation and fragment launch, and still provide reaction upon target impact. This criteria, while difficult to achieve, provides significant

advantages when performed correctly. In roughly 2011, Dahlgren Naval Support Facility demonstrated that High-Density Reactive Material (HDRM), a material with "the strength of aluminum, density of steel, and more than one and a half times the energy of TNT" could have dramatic effects for delivery of energy on target, and produce an enabling technology (Figure 10).[16] Efforts to commericalize such technologies are still ongoing, as is the case with companies suchs as MATSYS Inc., as also is illustated in Figure 10.[17]

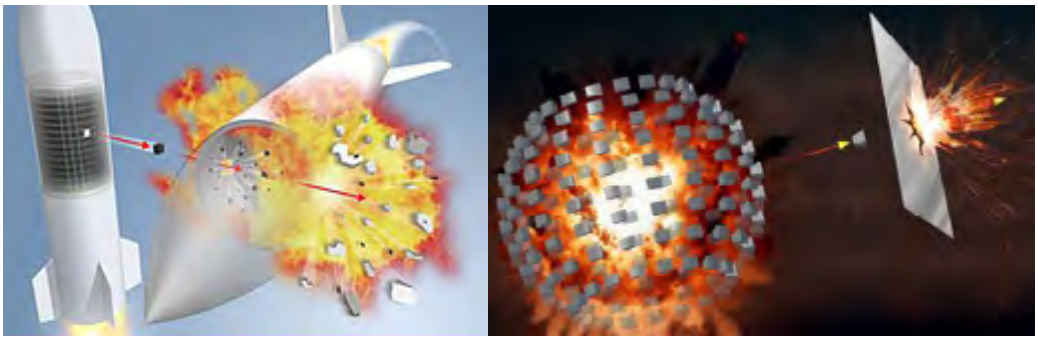


Figure 10. Graphical depictions of reactive fragments releasing energy upon impact with thin-skinned targets, photo credit ONR Press Release 2011,[18] left, and MATSYS Inc., right.[19]

It is not hard to imagine the advantages this technology could bring SOF, both in defense of position and against offensive targets. Like many technologies, if a greater effect can be produced from less material, then a lower weight will be required in a munition. Thus, a missile can be made to fly farther and give a range advantage over an adversary, or, likewise, an operator will have less weight to carry for the same delivered effects on target.

Nanomaterials: Enabling New Reaction Pathways

Like in any technical community, new discoveries or advancements will lead to trends or temporary excitement and, sometimes, even advancement of the field as a whole. The overall excitement in the wider scientific community about nanomaterials that gained momentum in the 1990s also made a significant impact in the energetics research community. From this, many new discoveries were made, primarily utilizing nanoparticulate aluminum metal (nAl), most notably in materials such as nanothermites, which enabled reaction rates up to 1000 times faster than conventionally sized counterparts.[20] However, this does not also equate to higher energy release, a point commonly misconstrued. As discussed previously, hard limits exist to energy content stored within chemicals, and no changes in physical form will alter that. Despite this, no shortage of researchers have made erroneous claims based on either perfidy or simple lack of understanding of the basic physical chemistry of the processes at hand. Many claims were introduced that because of the small particle size, an enhanced surface energy was produced, exceeding that of the available chemical energy. While

there is theoretical basis for the hypothesis that surface energy increases as particle size decreases, the realization of these claims was quickly debunked. As a general approach, without detailed information about particle size and surface energy, the surface energy of the bulk material should be considered.[21]

Advances in energetic materials, like in all technology fields, are perpetual (for now). There are always properties to enhance, whether through increased performance or insensitivity or optically switchable, optically initiable, melt-castable, more environmentally friendly, or higher-energy-per-unit-volume technology. As such, the field of energetics, although stagnant in certain realms, continues to thrive in others. Additionally, by enabling new reaction pathways, nanoenergetics have the ability to allow materials not typically recognized as explosive ingredients to be used, opening up use in hybrid and gray-zone conflicts.

Special Applications of Explosives

When we consider the opportunity to interject an explosive material into an ordinary object, we must consider critical diameter of the chosen energetic-material formulation. For small items, explosives that have large critical diameters would not be effective. Formulations also must be considered for their ability to maintain a small critical diameter. Typically, for a formulation to flow and be castable (into a shape), solids loading typically maxes out at ~80 wt%; thus, 20 wt% is binder. For any explosive, the more diluent (i.e., inert binder) added, the larger the critical diameter becomes. As such, emphasis on creating detonable binder systems is of great importance for maintaining critical diameters close to those of neat crystalline high explosives.

Common cast-cure explosives can be similar to rocket propellants, utilizing hydroxy-terminated polybutadiene (HTPB) as the primary binder component, along with isocyanates and plasticizers. Energetic polymers, such as GAP, 3,3-bis(azidomethyl)

Figure 11. Chess pieces cast with explosives.

oxetane (BAMO), and 3-azidomethyl-1,3,-methyl oxetane (AMMO) have become more popular for developing cast-cure formulations (albeit, mostly rocket propellants). Typically, these polymers are not detonable on their own, nor are they merely "dead weight" to keep an energetic formulation together. However, the substitution of inert binders (e.g., HTPB, epoxy), with energetic polymers, such as GAP, can have realized effects on critical diameter. As a result, objects with fine, small features can be cast or printed (via additive manufacturing) with fidelity such that all material will be consumed in a detonation of the object.

Producing cast replicas of everyday objects is easy, as evidenced by Figure 11. First, the inert article was cast into a relatively rubbery material (e.g., Shore Hardness 20, 40, or 60). Once a two-part mold is obtained, the HE/binder system is cast into the mold(s) and allowed to cure; curing times depend on the binder: epoxy takes minutes, whereas most GAP-based systems requires hours or days. The color associated with items can be changed easily; chemists refer to this as "a little bit of color goes a long way," meaning < 0.1 wt% of added coloring agent will cause drastic changes in color without altering performance, resulting in an item innocuous in appearance but capable of sustaining a detonation if a detonator were placed on it.

Other methods of introducing explosives into items include printing the material or spray casting explosives onto parts. Recent advances in additive manufacturing have resulted in explosive formulations that can be used in either direct-ink write (DIW) or fused deposition modeling (FDM) printing. Both of these allow internal structure to be printed, resulting in control of detonation propagation or reduction of part weight, and even printing of open access files, such as the Stanford Bunny (Figure 12).[22] Spray casting can be used to coat structural components, increasing their flammability and/or creating a detonable layer. Spray casting requires the explosive to be soluble in a given solvent (e.g., PETN in acetone) and also the explosive to be detonable in thin layers (i.e., critical thickness must be very small).

Figure 12. An example of using open-access print files in energetic printing. The Stanford Bunny produced from an FDM-based explosive material.[23]

Machine Learning/Artificial Intelligence

A machine learning/artificial intelligence (ML/AI) system to develop synthetic pathways for explosives with all the desired traits would be one of the most powerful and disruptive technologies ever developed. In such a system, a supercomputer with ML/AI algorithms,[24] perhaps coupled with an automated chemical synthesis machine, could quickly run through candidate molecules and provide a means to produce them quickly and safely. Desired properties might be selected as high-power/high-density, high-power/low sensitivity, high-power/cheap, melt-castable TNT replacements, or environmentally friendly synthetic pathways, to name a few. To be able to circumvent

the need to train chemists and other scientists and technicians, run costly labs with huge infrastructure costs, eliminate environmental effects (quickly becoming the cost drivers in most countries), and perform long-term research in mere hours would enable the country that developed the technology to dominate energetic materials. However, thankfully for us explosives scientists still consisting of flesh and blood, the input data to produce such ML/AI algorithms simply does not exist yet. Of the world's known explosives, few have been studied at the level of detail needed to populate such a system, and much of the literature includes dubious or misleading information, which would spoil the ML/AI algorithm. While this may not be something we see in the near term, because such a concept does not defy first principles, it will be part of humanity's future, as long as we do not suffer a great social collapse by other means first. Future SOF applications of such technologies, along with additive manufacturing, could be miniature custom munition factories on forward operating bases or on off shore factory ships.

Concluding Remarks

This chapter, to paraphrase Lindsay-Fajardo, intends to ground expectations in the ability for obtaining greater chemical energy storage in energetic materials and to provide a realistic lens in which we view possible strategic latency in energetic materials. With the advent of molecules such as CL-20 that have densities around 2 g/cc, and more exotic molecules such as hexanitrobenzene or octanitrocubane, we can still only achieve around 2 times TNT equivalence. Exotic means of energy storage might include free-radical stabilization, metastable helium, metallic hydrogen, polynitrogens, extended molecular solids,[25] or even matter-antimatter annihilation. However, research efforts in the United States and worldwide have resulted in only some validation of theoretical concepts or experiment confirmations at extreme financial cost and enormous energy input.

Therefore, strategies for disruptive energetic production have turned to the more physically obtainable concepts such as insensitive explosives with power near high-energy explosives—this would allow more ordnance closer to front lines in major conflicts as well as open up trade space in powerful armor penetrating munitions. Because they use ambient air, fuel-air explosives/thermobarics have a higher theoretical energy to target than standard high explosives; however, work output is different and not directly comparable. Reactive cases could provide up to four times blast energy over a steel-cased munition of equal size, but no lethal fragments, so uses would likely be in caves or structures in which fragments are easily blocked. Reactive fragments could provide much greater energy on target and could prove effective against soft-skinned targets like missiles, aircraft, and automobiles.

Special applications of explosives is another area that could provide disruptive advances in energetics (for SOF), with the ability to produce quickly special shapes or configurations of tools or devices that would be able to hide in plain sight, be difficult to detect, or utilize energetics where inert plastics otherwise would have been used.

Finally, machine learning/artificial intelligence is a far-future concept that could provide a nation-state with a quantum advancement in energetic-materials chemistry. As we look to the future of explosives, propellants, and pyrotechnics, we must not fail to observe how they will be coupled with other disruptive technologies in development, such as autonomous weapon systems, unmanned aerial systems, and advanced guidance systems. As computational power increases and electronics become more and more miniaturized, perhaps the danger on the horizon is not how big an explosive effect will become but how well we can use a small amount in a specific and targeted fashion. The continued development of these smart energetic systems will enable the special operations forces of the future to continue to be the fastest, lightest, and most lethal known to the world.

Approved for Public Release- LA-UR-20-28868

Endnotes

1 D. Chavez, et al., Preparation and explosive properties of azo- and azoxyfurazans. *J. Energ. Mater.* 2000, 18, 219-236.

2 P. E. Eaton, et al., Octanitrocubane: A New Nitrocarbon *Propellants, Explosives, Pyrotechnics* 2002, 27, 1-6.

3 B. Fedoroff, T., in *Encyclopedia of Explosives and Related Items*, Vol. 1, US Army Research and Development Command TACOM, ARDEC, Picatinny Arsenal, New Jersey, 1960, pp. A146-A152; G. Roth, (Ed. K. Patentamt), Germany, 1900.

4 S. M. Kaye, in *Encyclopedia of Explosives and Related Items*, Vol. 9, US Army Research and Development Command TACOM, ARDEC, Picatinny Arsenal, New Jersey, 1980.

5 M. A. Cook, *The Science of High Explosives*, second ed., Robert E. Krieger Publishing Co., Huntington, N.Y., 1958; M. A. Cook,et al., Thermo-Hydrodynamics and Reaction Kinetics in Some Metalized Explosives in *Second Symposia on Detonation*, Office of Naval Research, National Academy of Sciences, Washington, DC, 1955, p. 733.

6 G. Bjarnholt, Effects of Aluminum and Lithium Flouride Admixtures on Metal Acceleration Ability of Comp B, in 6th International Symposium on Detonation, Office of Naval Research-Department of the Navy, Coronado, California, 1976, p. 510.

7 Bjarnholt, *6th International Symposium on Detonation*, 510.

8 R. R. McGuire, M. Finger, Composite explosives for metal acceleration-The effect of detonation temperature in *8th International Symposium on Detonation*, Office of Naval Research, Albuquerque, NM, 1985, pp. 1018-1024; R. R. McGuire, et al., Detonation chemistry: An investigation of fluorine as an oxidizing moiety in explosives in *Seventh International Symposium on Detonation*, Office of Naval Research, Annapolis, MD, 1981; W. C. Tao, C. M. Tarver, D. R. Breithaupt, Fundamental Chemical Interactions in Metal-Filled Composite Explosives (Ed.: LLNL), Livermore, CA, 1991; W. C. Tao, et al, Understanding Composite Explosive Energetics: IV. Reactive Flow Modeling of Aluminum Reaction Kinetics in PETN and TNT Using Normalized Product Equation of State, in *10th International Detonation Symposium*, Office of Naval Research, Boston, Massachusetts, 1993, pp. 628-636; P. Brousseau, et al., Detonation Properties of Explosives Containing Nanometric Aluminum Powder, in *Twelfth International Detonation Symposium*, Office of Naval Research, San Diego, 2003, p. 11; V. Y. Davydov, et al., Effect of additions of powdered aluminum on the energy of an explosive transmitted in the axial and radial directions, *Combustion, Explosion, and Shock Waves* 1988, 24.

9 D. L. Frost, et al. "Effect of Scale on the Blast Wave from a Metalized Explosive," in *13th International Symposium on Detonation*, Office of Naval Research, Norfolk, VA, 2006, pp. 97-109; F. Zhang, "Detonation in Reactive Solid Particle-Gas Flow," *Journal of Propulsion and Power* 2006, 22, 1289-1309; F Zhang, K. Gerrard, and R. C. Ripley, "Reaction Mechanism Of Aluminum-Particle—Air Detonation," *Journal of Propulsion and Power* 2009, 25, 845-858; F. Zhang and W. H. Wilson, "The Effect of Charge Reactive Metal Cases on Air Blast," *AIP Conference Proceedings* 2009, 1195, 149-152; Y. Kato, K. Murata, and S. Itoh, "Detonation Characteristics of Packed Beds of Aluminum Saturated with Nitromethane," in 13th International Symposium on Detonation, Office of Naval Research, Norfolk, VA, 2006, pp. 187-195.

10 R. R. McGuire, M. Finger, in *8th International Symposium on Detonation*, Office of Naval Research, Albuquerque, NM, 1985, pp. 1018-1024; T. Bazyn, H. Krier, N. Glumac, Oxidizer and pressure effects on the combustion of 10-micro m aluminum particles *Journal of Propulsion and Power* 2005, 21, 577-582; N. Glumac, et al., *Chemical and Physical Processes in Combustion* 2003, 105-108; N. Glumac, et al., Combustion burn time and temperature measurements of ultra-fine metal particles in a shock tube, *Combustion Science and Technology* 2005, 177, 485-511; R. E. McClean, H. H. Nelson, M. L. Campbell, Kinetics of the reaction aluminum(2P0) + water over an extended temperature range, *Journal of Physical Chemistry* 1993, 97, 9673-9676.

11 E. L. Baker, C. Capellos, L. I. Stiel, Stable detonation velocities for aluminized explosives *Science and Technology of Energetic Materials* 2006, 67, 134-138; E. L. Baker, et al., Combined effects aluminized explosives, *International Symposium on Ballistics, Proceedings, 24th, New Orleans, LA, United States, Sept. 22-26, 2008* 2008, 2, 1135-1143.

12 W. Balas, et al., Development, Optimization, and Application of Combined Effects Explosives in *8th International Symposium on Special Topics in Chemical Propulsion*, Cape Town, South Africa, 2009.

13 C. M. Lindsay, M. E. Fajardo, The quest for greater chemical energy storage in energetic materials: Grounding expectations *AIP Conference Proceedings* 2017, 1793, 040023.

14 Lindsay and Fajardo, *AIP Conference Proceedings* 2017.

15 Lindsay and Fajardo, *AIP Conference Proceedings* 2017.

16 Revolutionary Material Dramatically Increases Explosive Force of Weapons. https://www.onr.navy.mil/en/Media-Center/Press-Releases/2011/High-Density-Reactive-Material-Explosive Vol. 2011, Office of Naval Research, Corporate Strategic Communications, Arlington, Va.

17 Structural Reactive Materials., *Vol. 2019*, MATSYS Inc.

18 Revolutionary Material Dramatically Increases Explosive Force of Weapons, Office of Naval Research,.

19 Structural Reactive Materials., *Vol. 2019*, MATSYS Inc.

20 V. E. Sanders, et al., Reaction propagation of four nanoscale energetic composites (Al/MoO3, Al/WO3, Al/CuO, and Bi2O3) *Journal of Propulsion and Power* 2007, 23, 707-714.

21 D. Vollath, F. D. Fischer, D. Holec, Surface energy of nanoparticles—influence of particle size and structure *Beilstein Journal of Nanotechnology* 2018, 9, 2265-2276.

22 Schmalzer, A. et al., Controlled Detonation Dynamics in Additively Manufactured High Explosives APS SCCM July 14, 2017 Saint Louis, MO.

23 Schmalzer, Controlled Detonation Dynamics in Additively Manufactured High Explosives, 2017.

24 D. C. Elton, et al., Applying machine learning techniques to predict the properties of energetic materials, *Scientific Reports* 2018, 8, 9059.

25 Lindsay and Fajardo, *AIP Conference Proceedings* 2017.

CHAPTER 15

Metamaterials: How Close Are We to a Klingon Cloaking Device or Harry Potter Invisibility Cloak?

Michael Valley

Introduction

Life conditions us to believe and react to what we see, hear, and feel; however, metamaterials may one day challenge our reliance on senses, as scientists mold material behaviors with alchemy-like outcomes to get the edge on nature. Such advances inspire dreams of invisibility cloaks, realizing fictional technologies from the universes of Harry Potter and Star Trek. Then again, this sleight of hand would require us to bend light and energy to our will. Clearly this is not possible—or is it? This chapter examines the burgeoning field of metamaterials and implications for special operations forces (SOF).

The United States is not alone in its pursuit of metamaterials. Both rapid strides in global technology and dynamic adversary posture shifts contribute to future mission environment uncertainties. Preserving our national security advantage, deterring foreign actions, mitigating countermeasures, and ensuring adversaries share our confidence in SOF capabilities dictate we possess disruptive technologies. The United States holds unrivaled responsive alternatives, but technological superiority is perishable. Metamaterials have the potential to provide asymmetric advantages to erode the value of foreign technology advances. We must understand how to use them to our advantage and how to diminish their effectiveness when employed against us. Metamaterials may drive us to rethink everything about battlespace technologies.

When metamaterials emerged is debatable, since mankind has long worked to improve materials, though the term's use has been prevalent for only a few decades. What is clear is the accelerating pace of metamaterial developments and the promise they hold. Pioneering work by Victor Veselago and others stirred beliefs about the possibility of creating materials to control electromagnetic waves, providing the foundation for visions of metamaterial-enabled devices with tailored optical and energy-wave control abilities.[1] Since the turn of the twenty-first century, progress in the ability to study metamaterial behavior down to atomic size scales has contributed scientific insights that led to the creation of powerful design tools.

Parallel advances in the synthesis of new materials and advanced manufacturing helped material designers translate their concepts into amazing fabricated parts. This rapid progress has excited researchers far and wide. Indeed, metamaterials is a dynamic, worldwide research topic with over 25,000 publications since 2000. Unfortunately, the greatest metamaterial research growth is outside the United States, with 80 percent of publications coming from China since 2015. Breakthroughs are being incorporated into national security applications. What is already achievable is noteworthy but nothing compared to what is on the horizon for this materials

revolution. Our fascination with metamaterials has just begun and will grow as their use becomes more common.

Herein, we do not review metamaterial literature, which go back a century. Many publications summarize key breakthroughs in topical areas within the metamaterials genre. Representative overviews can be found in "The Century of Metamaterials," "Mechanical Metamaterials Associated with Stiffness, Rigidity and Compressibility: A Brief Review," and "3D Metamaterials."[2]

Unraveling the Metamaterial Mystery: Magical, Mythical, or Simply Marvelous?

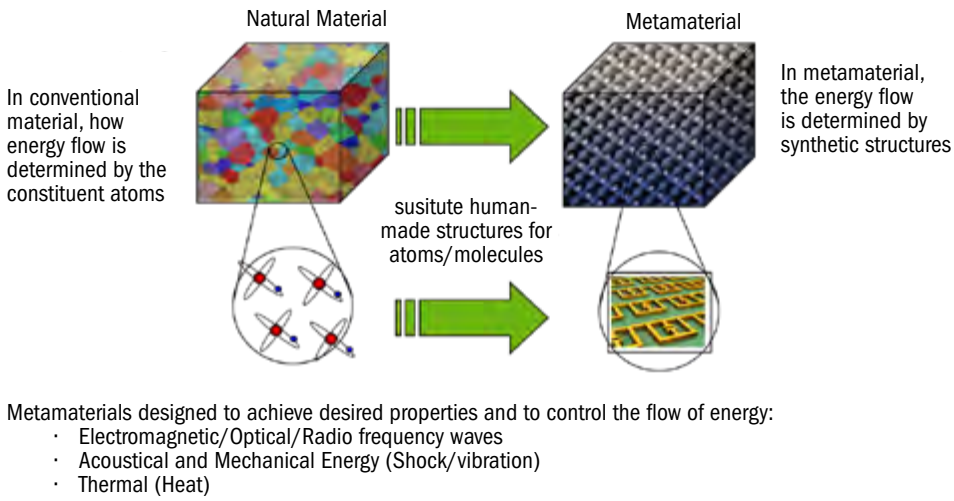


Figure 1. Metamaterial versus a natural material.

The definition of what constitutes a metamaterial continues to evolve as creative researchers push the boundaries of science and manufacturing, allowing us to translate the art of the possible to field what has long seemed impossible. Essentially, as shown in figure 1, metamaterials are natural materials fashioned to deliver unconventional properties through the integration of small engineered structures—often called meta-atoms—whose feature size can approach dimensions thousands of times smaller than the width of a human hair. The achievable material properties and behaviors resulting from the atomic and microstructural additions and rearrangements depends on the blend of the constituent materials and the small-scale structural arrangement of those materials achieved through precise manufacturing methods. The possible combinations are limitless! Today's metamaterials demonstrate tunable, reconfigurable, and spatially variable behaviors that go far beyond the well-recognized characteristics of even the most advanced "smart" materials.

Indeed, progress in design tools and manufacturing sciences enables us to translate our imagination into fabricated structures with unprecedented precision,

including the ability to adjust individual atoms. Though manipulating atoms can be a powerful method for creating some materials, we are not limited to fabricating devices with molecular-scale structures. Additive manufacturing can assemble metamaterial products with features from grain scales (100-200 nanometer [nm] building-block size using a Nanoscribe three-dimensional [3D] printer) to centimeters or larger as manufacturing build volumes expand to meter scales. These larger sizes still manifest amazing properties, as has been demonstrated in reinforced composites, printed lattices, compression pads, optics, and more.

Though the ability to manufacture ultralarge metamaterial structures has been elusive, developers will achieve this capability within the foreseeable future. Even today, metamaterial-based technologies are making it to the marketplace within the defense and national security, telecommunications, consumer electronics, medical, environmental, and energy industries (e.g., solar, batteries, energy storage).

A desirable and well-recognized metamaterial characteristic is their ability to be designed to control energy flow—how much energy is reflected, absorbed or dampened, transmitted, redirected through steering or focusing, or filtered as a function of wavelength or frequency. Energy-flow control is achievable across the electromagnetic regime, providing utility in the optical, infrared (IR), microwave, radio-frequency (RF), and radar domains. Similarly, energy-flow control is possible for mechanical, acoustic, and thermal energy. Imagine if we could capture energy of interest and regulate what happens to the undesirable energy. It is this aspect of metamaterials that inspires hope for invisibility cloaks. Though large-scale cloaking has not yet materialized, the practical value of energy-flow control provides new functionalities that govern device behaviors, as well as material signatures and observables. The energy manipulation attributes of metamaterials holds the promise of delivering capabilities to strengthen SOF technology options in an uncertain and rapidly changing global environment.

Metamorphic Manufacturing

Metamaterial characterization capabilities, combined with state-of-the-art testing systems, elucidate relationships between engineered microstructures and their resulting material performance, helping design mature modeling software that captures the phenomenology that drives material behavior. It is important to understand the underlying physics to use these materials confidently. The ability to capture small-scale attributes is particularly important, because metamaterial properties are governed by their constituents' fundamental material physical properties, inclusions and defects, shape, and the characteristics of integrated engineered material substructures.

Early on, researchers chiefly fabricated metamaterials using particle-beam lithography (e.g., electron-beam, focused-ion-beam lithography). Lithography remains an important fabrication method as developments overcome its historic limitations. Today, there are more than a dozen lithography options, each addressing

a specific fabrication need. Unfortunately, the size of what can be made is only a few centimeters. This is not to infer lithography is not viable for creating disruptive technologies. Consider, for example, the Defense Advanced Research Projects Agency (DARPA) EXTREME project that uses membrane projection lithography to construct 3D metamaterial structures with the intent of developing compact conformal, hyperspectral, and night-vision technologies.[3] The utility would be immense for a reconfigurable, small, low-power, lightweight device that provides simultaneous multispectral, polarimetric, and classical imaging.

Additive manufacturing is poised to fabricate products orders of magnitude larger than what lithography can produce. For example, though not using a metamaterial, Oak Ridge National Laboratory printed an entire car body in a day. Additive-manufacturing systems provide controlled fabrication of 3D structures using polymers, metals, ceramics, and multimaterial combinations, as well as metamaterials. These machines provide submicron resolution or large build volumes, but typically not both at the same time; however, the pace of innovation in additive manufacturing, driven by a worldwide market exceeding $20 billion annually, will rapidly advance metamaterial manufacturing in the 2020s.[4] Forecasted systems will fabricate metamaterials measured in meters with improved fabrication tolerances.

Additive-manufacturing systems fabricate parts not achievable through conventional methods. They take advantage of design concepts such as topological optimization[5] to construct components customized for the mission need while increasing strength, decreasing size and weight, and providing shape agility for novel packaging and form factors. Considerable efforts are underway to expand additive-manufacturing material-feedstock choices, which will extend technology development options. For example, chemists are synthesizing novel additive-manufacturing printer inks to create materials with unusual attributes to advance products such as flexible electronics. Further, state-of-the-art system controls are improving part quality and reducing the achievable feature size, which can be smaller than a micron. Nevertheless, fabricating large parts for defense and national security uses is still difficult.

To overcome metal part size limits, researchers are crafting additive-manufacturing concepts that use multiple high-powered lasers to better control heating at increased fabrication speeds. Early tests show heating control reduces defect formation and controls the metal grain structure to achieve desired properties. Another advance is the Fraunhofer Institute for Laser Technology's hybrid system, which combines conventional and additive-manufacturing processes to take advantage of each technologies' best attributes. This system's fabrication process chain increases manufacturing speed and achievable part size while ensuring consistent part quality and not compromising control of small features.

For fabricating flexible electronics, roll-to-roll methods such Metamaterial Technologies Inc.'s Rolling Mask Lithography method and MICROGRAVURE printing are proving effective. These production-scale printing systems are cost-effective, flexible, and avoid chemical-etching issues. Active research in roll-to-roll printing

of metasurfaces continues.[6] With breakthroughs in self-assembled nanomaterial synthesis methods and the invention of printable inks that fully embrace the periodic table, the roll-to-roll manufacturing methods will likely become a future workhorse for fabricating metamaterial surfaces.

As demonstrated by the University of Delaware and the US Army Communications-Electronics Research, Development and Engineering Center, roll-to-roll systems can insert electromagnetic materials into large structural composites. This ability may prove impactful for building microwave devices and radomes with integrated, high-end antennas. Alternately, electromagnetic structures, including microwave metamaterials that integrate metals and dielectrics, can be fabricated with multimaterial additive-manufacturing systems. For example, fused deposition modeling 3D printing can now generate high-quality gigahertz (GHz) microwave metamaterials, overcoming the need for metallization after printing.

Similarly, metamaterials can be spun into fabric textiles using screen printing combined with standard composite processing methods. Lightweight metamaterial devices (e.g., communications, sensors, self-cooling) woven into uniforms could enhance soldier capabilities and reduce carried-gear weight.[7]

Metamaterials by Design

Until recently, exploiting the promise of metamaterials has challenged engineers and designers. Classical design methods require solving complex equations governing the multiscale, multiphysics behavior of the devices and materials of interest—a daunting task requiring high-powered computers and expertise in corresponding fields of science. Fortunately, tremendous progress in solution methods are easing design burdens. Technical-skill requirements are partially mitigated by commercial software that aids the design process. Examples include the ANSYS High Frequency Structure Simulator and COMSOL Multiphysics software, which use finite element methods to solve 3D-device design problems; however, some expertise and model iterations are needed to optimize device designs with these tools.

An effective approach applied to lessen computational burdens and problem-solving complexity in metamaterials design uses reduced-order models that simplify approximations to real-life processes while still capturing the core physics of the material phenomena being modeled. An example is the perturbative metamaterial method used to maximize dynamic metamaterial performance, such as dampening vibrations.[8]

Other design approaches overcoming metamaterial design challenges come from the field of artificial intelligence (AI). For example, a Tel Aviv University team demonstrated an AI deep-learning approach to nanophotonic metamaterials design.[9] Similarly, a team from Pohang University of Science and Technology used a deep-learning-assisted inverse design method to improve the efficiency of designing photonic structures.[10] These data-driven artificial neural-network approaches reduce the number of iterations required to optimize a design. They are well suited to designs where the metamaterial devices will be quasi-static and where data is available to train the neural network.

Determining how energy will flow in a structure is straightforward if you understand the governing equations or use a commercial design code. Regrettably, the possible design variations are innumerable, often requiring countless iterations to achieve an acceptable design. To overcome this challenge, developers have examined a new design paradigm called *metamaterials-by-design* (MBD).[11] MBD considers the design process from an application-oriented perspective driven by the device's performance requirements. In other words, MBD methods solve the inverse problem, starting with the end in mind and working backward. While this would seem logical, it is far from easy.

Working metamaterial designs backward requires the use of optimization methods to find the best solution, given a myriad of design choices. Imagine finding the deepest dimple on a rough surface without measuring each one. This search challenge is similar to solving an inverse design problem. Many methods such as topological optimization tackle this hunt for the best design, though they still require many trials.[12] Fortunately, a strategy called "modified error in constitutive equations," together with an adjoint optimization solver for sensitivity calculations independent of the number of design variables, has proven efficient at finding the best solution without the need for either a supercomputer or many iterations.[13] This approach has been validated under harsh mechanical test conditions. For example, a metamaterial designed with this approach and implemented with 3D additive manufacturing demonstrated three to five orders of magnitude reduction in shock and vibration wave-energy transmission and tunable frequency transmission across a 10 kilohertz (kHz) frequency range.[14]

The aforementioned approaches, though powerful, require technical expertise for proper use. It is well-known that metamaterial properties are tightly associated with the size, shape, composition, and internal distribution of the material constituents. Change the material's internal structure slightly, and you are apt to create a different material response. This places a burden on the metamaterial's design and manufacturing. To realize the potential of metamaterials requires we have practical, easy-to-use design tools, which is the goal of the DARPA Mirage program. As explained by Ihab El-Kady, the Mirage project lead:

Mirage is shifting the burden of design from the subject-matter expert to the practitioner. Emerging software users design science fiction–like materials with the same ease and efficiency that architects use when they draft building plans, speeding up metamaterials research and development (R&D). No longer is a large cross-disciplinary team of experts required—you just need your imagination, and the new tool will do the rest. These nascent tools are driving a perspective shift in material selection and conventional design approaches.[15]

This design software achievement is exactly the breakthrough needed to accelerate the development and adoption of metamaterial-enabled devices. Currently, Mirage software is applied to electromagnetic metamaterial device designs, but efforts are underway to extend this software to acoustic and mechanical device design applications.

Anticipating the Surprise and Realizing the Dream

Continued progress coupling material physics into user-friendly design tools and fabrication methods for metamaterials is enabling extraordinary control of the flow of energy to create lightweight, damage-tolerant, high-performance materials with attributes that have long been unreachable. The way creative designers are taking advantage of energy control mechanisms is making us reimagine what is possible. As illustrated in figure 2, and discussed below, the ways metamaterials can transform and augment SOF operations are steadily growing.

GRAPHICS CREATED BY DANIEL THOMPSON (DSTHOMP@SANDIA.GOV), SANDIA NATIONAL LABORATORIES.

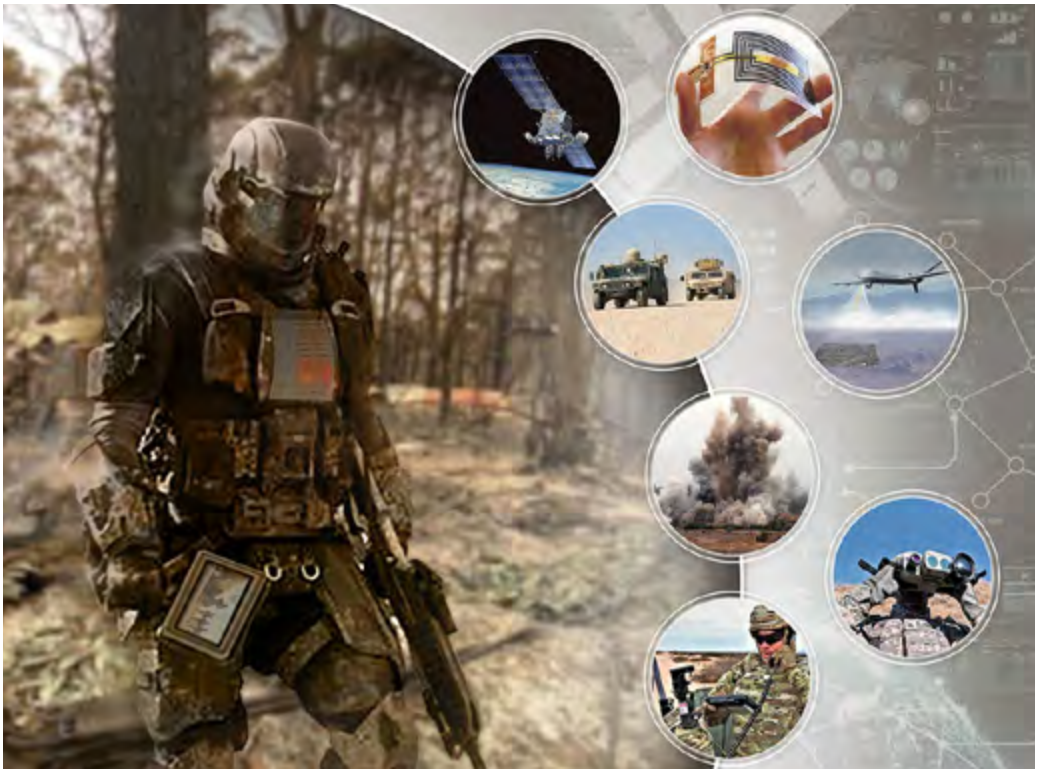


Figure 2. Metamaterials for diverse SOF applications.

While the greatest near-term use of metamaterials may be communications and radar systems, early signs indicate metamaterials will soon broadly proliferate into commercial and military products. For example, metamaterial super lenses may someday image details beyond diffraction limits for higher-resolution microscopes to study basic material sciences, as well as the physics of metamaterials themselves. With these lenses, we may push past manufacturing barriers to fabricate more capable microelectronics processors with smaller feature sizes, particularly if matched with materials such as phononic metamaterials that control thermal conduction attributes for heat management. Already, progress has been made with making thin, super-

lightweight flat optics for cameras and viewfinders. Researchers have demonstrated metamaterial optical resolution above 80 percent of diffraction limits, and products are making it to market. For example, firms such as Metalenz Inc., Phoebus Optoelectronics LLC, Nano-Meta Technologies, Inc., and Multiwave Technologies are incubating optical metamaterial technologies from lab to market at an increasing rate.

For microelectronics and electronic packaging, researchers at the Toyota Research Institute are developing thermal composite metamaterials for thermal energy cloaking and shielding, printed circuit-board temperature control, energy harvesting, and electrothermal power conversion for next-generation electronics, optoelectronics, and photonic devices.[16] Also for microelectronics, magnetic metamaterials are helping developers move past silicon to field a new class of low-power transistors and superconductors for next-generation electronics and high-performance computers. These same electromagnetic metamaterials could lead to extreme magnetic field sensing for ground-penetrating radars, space-based and underwater magnetometers, and improved antiship missile-defense radar.

Though we currently cannot upsize metamaterial optical systems to larger scales, ongoing work will someday field more capable military reconnaissance systems, including agile spectral and polarization filters, and light-weight flat lenses. Possibly, designers will soon couple sparse array metamaterials with computational imaging software to field larger airborne and space optics. Already, metamaterials show promise in adaptive optics, laser-tracking antiglare, and laser protection coatings (e.g., Metamaterials Technologies Inc.); it is a matter of time before they expand into larger optical systems.

Research is yielding improved resolution and measurement sensitivity in commercially available sensors. Examples including strain sensors, biomedical sensors (e.g., MRI, glucose sensors), optical gas sensors, ultrasonic imagers, and thermal imagers such as nanoantenna-enabled cameras that can boost the signal by up to three times and improve image quality by reducing dark current by up to 100 times. Evolv Technology employs metamaterials for imaging and high-speed walkthrough firearm and explosive detection portals, which might enable portable entry control systems for gray-zone urban environments. Firms such as TeraView use metamaterials in a terahertz inspection system that is so sensitive it can determine paint thickness or find small defects at semiconductor device scales, possibly providing a process control or supply-chain trust-assurance tool. TeraView's terahertz and millimeter-wave imaging systems extend from explosives detection and vehicle collision avoidance to higher-resolution radar and sonar systems. Also, for autonomous vehicle collision avoidance, Lumotive is developing solid-state Light Detection and Ranging (LIDAR) systems with a metamaterial beam-steering technology.

Visualize what is possible with responsive sensors attuned to their surroundings. Environmentally activated passive sensors can indicate package tampering (e.g., food, microelectronics, medical) to improve safety and trust in the international supply

chain. This capability could also activate remote devices autonomously when exposed to a targeted signal (e.g., heat, humidity, shock, vibration, RF).

Metamaterials can control mechanical energy, which is the energy source for what we feel from shocks, vibrations, impacts, and blast waves. Consider a woodpecker's beak that impacts a tree about 20 times per second with a deceleration of 1200 g's ("g" is acceleration due to gravity) without hurting itself.[17] Metamaterials seek similar protective capabilities. The same principles that allow us to regulate sound can be employed to control how we absorb, reflect, focus, or redirect mechanical waves.

Indeed, mechanical metamaterials have proved effective in rocket flights, isolating sensitive parts from dynamic flight loads. These same materials may reduce the jostling from a bumpy road by blocking the energy as it passes through tires, allowing military vehicles to speed through undeveloped regions safely and comfortably. Focusing mechanical energy would enhance shape-charge effectiveness, placing more energy on a small spot. Metamaterials for absorbing and redirecting incoming shocks or blast waves could improve shielding, be used for safety equipment, cushion falls, and improve footgear. Further, we can design intentional failure mechanisms to control energy absorption, such as a crumple zone in a car, thereby protecting something precious, such as a human life or a delicate instrument.

Because we can control metamaterial constituents and their distribution in what we build, we can design stiffness and load response variations in devices and structures. Uses for this include actuators that can be tuned to respond to specific forces, such as strain or loads. SOF applications could include better exoskeletons to enhance soldier performance and improved prosthetics and artificial muscles needed when serious injuries are sustained.

In the arena of battlefield sound management and aeroacoustics, research is underway to develop lightweight tunable metamaterials for acoustics and vibration control. One intriguing effort uses resonant metamaterials for aerodynamic flow control to delay the onset of turbulent flow transition, thereby reducing skin friction drag and reducing power usage.[18] Similarly, a research team from the Italian University of Niccolo Cusano and the Chinese Academy of Aerospace Aerodynamics is studying a porous metamaterial, ultrasonically absorptive coating to delay the turbulent flow transition to reduce the boundary-layer drag and heat-transfer rates for a hypersonic vehicle.[19]

One intriguing class of metamaterials is auxetic materials. They exhibit high-energy absorption and fracture resistance through the material microstructure, which can flex and stretch in phenomenal ways. These materials have a negative Poisson's ratio, which means they expand in all directions when stretched and contract in all directions when compressed. Possible uses for auxetic metamaterials include materials for engines and thermal protection, stronger ropes, foams and packaging materials to protect parts from shocks, and blast-protection applications. For example, Auxetix Ltd. demonstrated an auxetic material called Zetic that can survive a car bomb. They suggest Zetic could provide superior body armor and protective clothing, blast-resilient ultralight ultrastrong stretchable backpacks and military tents, and

strong flexible medical sutures compatible with body tissues. Further, a team from the Massachusetts Institute of Technology's Self-Assembly Lab demonstrated heat-activated auxetic materials, adding a new dimension to what is possible. It is likely these magic materials will one day find their way into military applications.

Metamaterial adoption has been greatest in communications, antennas, and radar systems, with related RFID applications for tagging, tracking, and locating. The move to 5G communications and extraordinary radar capabilities will push developments even faster, with commercial sales forecasted to exceed $10 billion annually by 2030.[20] Metamaterials are integral to future high-performance, high-impedance, low-profile, conformal, and fractal antennas for communications and radar systems. Immense potential exists for game-changing shifts in military communications and radar systems through metamaterials. Indeed, as metamaterials become more fully integrated into antenna technologies, they will reduce system costs, enable smaller devices with reduced power requirements, facilitate novel shapes and form factors, and deliver more agile beam forming and shaping capabilities.

It is now feasible to produce dramatically smaller electric and magnetic dipole antennas with boosted radiating power and patch antennas with increased directivity, enhanced gain, and reduced return loss. This size reduction does not mean performance is compromised. For example, tiny metamaterial antennas can be tuned across entire communications bands, overcoming narrow operating bandwidths to make smaller radios possible. Also possible are remarkable frequency and polarization agility and improved multiband operations with reconfigurability for microwave devices and custom antennas.

The push for smaller antenna sizes will continue. With it will come operational resilience. For noisy RF environments, metamaterial mobile-communications smart antennas can adjust to their environment to strengthen communications of interest while mitigating competing signals. Further, Pivotal Commware sells a wireless system that reuses the same spectrum bands, possibly providing a means to ensure communications are sustained in congested and contested RF environments.

Many companies already take advantage of the special attributes only metamaterials can provide for RF devices. For example, Fractal Antenna Systems, Inc. employs metamaterials for RFID tags, smart sensors, novel antennas, and flat-lens technologies for microwave applications for telecommunications and surveillance systems. Their metamaterials allow for multiband and wide bandwidth fractal antennas that can be positioned in nontypical locations. For example, they claim their recessed antennas can even be located next to metal without disrupting antenna operations. These antennas are small, thin, lightweight, have no electrical connections and reduced circuitry, and offer increased gain.

Another firm, Kymeta, uses metamaterials in thin, lightweight broadband systems for vehicle-to-vehicle communications, enabling a new secure-communications paradigm for military forces in remote areas. Well known for their satellite communications systems for land and sea, Kymeta now produces a thin, lightweight

flat-panel satellite antenna. They use electronically activated metamaterials to steer their Ku-band communications beam to a satellite. Together with satellite constellations under development, such as the DARPA Blackjack program, this could support direct satellite-to-soldier communications.[21]

Metamaterial advances are also transforming radar systems. For instance, Echodyne makes a handheld radar able to track people, cars, and even a small plane at a distance of a few miles. Likewise, Metawave has combined artificial intelligence with metamaterials to create radar for autonomous driving vehicles, including an ability to see around corners, which could be powerful in contested urban environments.

Metamaterial adeptness in redirecting and sensing energy flow has opened an exciting research path, exploring "compute by feel," to sense an environment dynamically, assess conditions, react autonomously, or respond without a human in the loop. Such a reflexive ability to enable functions at the speed of battle should increase survivability and weapon-system effectiveness dramatically, especially if it simplifies multi-input data analysis needed to deliver situational awareness. These metamaterials might obviate computer-based feedback loops to reduce power and system complexity. Triggering autonomous action, including system reconfiguration, could protect systems from damage and soldiers from harm, or improve performance, such as communications-link optimization through origami-like structure-change methods.[22] Autonomous navigation and maneuvering will be achieved when "compute by feel" metamaterials prove capable of discerning normal loads from hostile conditions. This will create marked advantages in contested environments with mobile targets, particularly for unmanned aerial, underwater, and hypersonic vehicles seeking to avoid countermeasures or adverse flight conditions.

The concept of "compute-by-feel" metamaterials operating like a nervous system in a cybernetic mode to drive complex actions is not far-fetched. Classic examples exist through smart materials, self-assembly fabrication and material synthesis methods, and biomimicry, in which we learn from nature. Many have suggested nature produces the best materials adapted over time to deliver exquisite attributes. For example, a spiderweb is a distributed sensor platform where the web strands capture vibrations and interpret and communicate them to the spider using only mechanoreceptors on their legs. Such concepts can now be translated to complex metamaterials.[23] Metamaterials may be a key building block that allows us to borrow from nature and create functionalities that heretofore have been limited to plants, animals, and insects. Imagine if we could replicate chameleon capabilities!

Metamaterials are also finding a home in advanced computing. For example, professor Nader Engheta and his team at the University of Pennsylvania used metamaterials to demonstrate an analog computer that could someday result in low-power computers that operate by light instead of electricity.[24] Also, the DARPA Defense Sciences Office has sponsored brain-inspired neuromorphic computing research that uses metamaterials and will take advantage of the revolutionary breakthroughs in machine learning and artificial intelligence. Indeed, as described by the project

lead, Francois Leonard, "imagine a window that turns blue if a bear walks by but turns red if it's a giraffe. Even better, this window could learn to respond to different stimuli by repeated exposure to a training dataset, much like the human brain."[25] By showing metamaterials themselves can extract useful information from optical fields without the need to process optical signals with electronics, this project will create neuromorphic optical-media building blocks to increase processing speed and reduce power requirements. This could also transform optical sensing, image processing, and recognition for national security applications.

Metamaterials will someday provide SOF forces with robust, effective, and flexible technologies to assure mission success across the full detect-deter-deny-destroy mission spectrum. However, cloaking may be the most impactful for irregular warfare—but what is possible?

Metamaterial Stealth—A Vanishing Advantage

The same class of metamaterials that improves our communications and radar systems can absorb energy. Of interest is the ability of these materials to deliver low radar cross-section and IR stealth characteristics. Narrow-band, multiband, and broadband high-absorption metamaterials have been demonstrated from the optical to microwave spectral regions. For example, a team led out of the University of Electronic Science and Technology of China has demonstrated a metamaterial with 98 percent absorption for discrete wavelengths that can be designed within the 600–1500 nm wavelength range. Applications for this capability range from improved sensing, spectral filtering, reduced thermal emissions, and night-vision goggles.[26] Similarly, metamaterials can be designed to control the direction in which thermal energy is emitted. Beyond providing metasurfaces for thermal management on satellites, such a capability is valuable in tailoring IR signatures for stealth and camouflage uses.

As another example, a research team at Zhejiang University published results for an optically transparent, broadband radar stealth material with a frequency-selective microwave-transmission window and low IR emissivity.[27] Their test results showed strong broadband performance from 1.5 GHz to 9 GHz, with a radar transmission window at 3.8 GHz. This radar transparent metasurface simultaneously demonstrated low surface IR emissivity, which would make systems fabricated with this material hard to detect with radar or IR imagers. Further, emerging research in polymeric photonic crystals indicates chameleon-like tunability in the RF range may also be achievable. In general, by manipulating a surface's energy-scattering properties using a metasurface, the signal return can be manipulated to alter an object's appearance or make it disappear completely.[28] These attributes seem like what we might expect from a military digital radio frequency memory (DRFM) system, where we seek to obfuscate electromagnetic signatures, but without the need for power and software.

When considering metamaterial invisibility, discussions frequently focus on inanimate objects like tanks, planes, and ships; however, using metamaterial invisibility to provide protection for our forces on the ground would be equally compelling. The proven capability to weave metamaterials, microelectronics, and micropower systems (including solar power) into clothing provides the tools for an adjustable camouflage and concealment capability that could be fine-tuned in real-time to a soldier's environment. Combine such a uniform with creams and face paints with nanometamaterial additives to reduce visible and IR signatures, and we would be one step closer to having a Predator outfit right out of the movies.

Invisibility cloaking drew excitement in the early days of metamaterials research, and a similar sound-masking technology is on the horizon. Acoustic metamaterials were first demonstrated by Zhengyou Liu and others in 2000, laying the foundation for sound attenuation and control through metamaterials.[29] Today we find acoustics and sound control in consumer audio systems, and signature management is now possible, to some extent. Indeed, companies such as Metasonics control sound without impeding air flow, and the Acoustic Metamaterials Group creates high-performance noise-dampening metamaterials. Many research teams worldwide have demonstrated an ability to control which acoustic frequencies can penetrate through metamaterials, as well as which acoustic signals will be released. Complete noise silencing has been demonstrated, offering the hope that one day any vehicle, engine, or noise source can be completely silenced, whether operating on the ground, in the air, or in marine domains. Also, by manipulating sound we can alter emissions from audio to ultrasound and sonar frequencies, potentially creating an ability to replicate the noise signatures of anything we choose to emulate.

Considering proven capabilities to control energy flow into and out of surfaces, it is logical to anticipate advanced stealth, camouflage, and signature-management technologies will become commonplace in arenas where concealments, deception, and subversion may be employed. By bending light and energy with space-age metamaterials, we may also be able to further reduce visibility by removing shadows. What we do with the incident energy—be it light, heat, mechanical, or electromagnetic—will be important for enabling stealth. One possibility might be to harvest energy intended to harm and reapply it for useful purposes, like storable power.

Stealthy metamaterials may prove to be both a blessing and a curse for intelligence, surveillance, and reconnaissance (ISR) systems as innovations provide more capable sensing systems, as well as the ability to reduce signals from what we wish to sense. We will be driven to consider a wider range of measurements of potential observables to achieve ISR mission goals against the use of metamaterials for static signature management. For materials that provide tunable or autonomous chameleon adaptations, we will be challenged to develop countermeasures that can discriminate signals and targets from background clutter. This may prove to be a pivotal technology where the United States must sustain an advantage and be the first to field robust capabilities to shape the future battlespace.

Conclusions—Making a Material Difference in National Security

Today's global landscape reflects an unprecedented mix of conflicts, stress points, and potential threats. Threats are evolving, and US policy has not constrained adversaries. The SOF community remains an essential component of our response options to protect US and ally interests in these times of growing uncertainty. SOF capabilities, training, skills, motivation, and effectiveness remain high; but as strong as they are, they must adapt continually to disrupt the actions of adversaries. In fact, US rivals are actively researching and developing technologies to nullify the US advantage at a pace exceeding US development-to-deployment cycles. In the face of these aggressive foreign efforts, the US may need to expand its research, production capabilities, and supplier base to meet this national security and domestic economy need. Indeed, metamaterials may become a critical base technology and pivotal enabler to engineer capabilities that keep SOF on the forefront of international technologies. If so, the United States will need to accelerate its cycles of learning and rate of insertion into mission toolkits.

In the coming years, we will gaze in awe at the incredible revolution made possible by the science of metamaterials and abilities to design and shape them into asymmetric technology advantages. By 2025 we expect controllable metamaterials will contribute to SOF capabilities through advanced radar and communications systems, enhanced tagging-tracking-locating and targeting devices with greater geolocating accuracy and operating ranges, compact highly capable electronics and sensors, "smart uniforms," and lightweight materials and armored vehicles resilient to shocks, blasts, projectiles, lasers, radiation, and electromagnetic attacks. So too can we see the day when cloaking and stealth become mainstream capabilities, realized through cutting-edge camouflages, concealments, and surface materials that manage radar, RF, and IR signatures and observables, as well as noise emanations.

While we must be on guard to avoid the hype, we must also be open to the new realm of metamaterial possibilities. Achieving the metamaterial dream requires we nurture and advance national capability-based science and engineering foundations. If we do so, through remarkable innovations we will deliver more agile and effective tools to SOF forces and avoid adversary surprises in future warfare. Our quest to design materials that can be fabricated with predictable and controllable qualities remains, but design tools like Mirage and additive-manufacturing advances put metamaterials within our grasp, adding radical new dimensions to what is possible.[30] Indeed, metamaterials hold the promise of delivering strengthened SOF technology options in an uncertain and rapidly changing battlespace.

Acknowledgement

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the US Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Endnotes

1 Veselago, Victor G. 1968. "The Electrodynamics of Substances with Simultaneously Negative Vaues of e and μ." *Sov Phys Uspekhi* 10 (4): 509–14.

2 Tretyakov, Sergei, Augustine Urbas, and Nikolay Zheludev. 2017. "The Century of Metamaterials." *J. Opt.* 19 (8): 80404; Yu, X., J. Zhou, H. Liang, Z. Jiang, and L. Wu. 2018. "Mechanical Metamaterials Associated with Stiffness, Rigidity and Compressibility: A Brief Review." *Progress in Materials Science* 94: 114-173; Kadic, Muamer, et al. 2019. "3D Metamaterials." *Nature Reviews Physics* 1: 198-210.

3 Fiddy, Michael, "Extreme Optics and Imaging (EXTREME)," DARPA, https://www.darpa.mil/program/extreme-optics-and-imaging.

4 Wagner, I. 2019. "Projected Global Additive Manufacturing Market Size between 2016 and 2020." Statista report. https://www.statista.com/statistics/284863/additive-manufacturing-projected-global-market-size/.

5 Liu, Jikai, et al. 2019. "Meta-Material Topology Optimization with Geometric Control." *Computer-Aided Design & Applications* 16 (5): 951-61; Gao, Jie, et al. 2019. "Topology Optimization for Auxetic Metamaterials Based on Isogeometric Analysis." *Computer Methods in Applied Mechanics and Engineering* 352: 211-36.

6 Deng, Yujun, et al. 2015. "Flow Behavior of Polymers during the Roll-to-Roll Hot Embossing Process." *J. Micromech. Microeng.* 25 (6): 065004; Liu, Longiu, et al. 2016. "A Programmable Nanoreplica Molding for the Fabrication of Nanophotonic Devices." *Scientific Reports* 6: 22445.7.

7 Mirotznik, M.S., et al. 2012. "Broadband Electromagnetic Modeling of Woven Fabric Composites." *IEEE Trans. Microw. Theory Tech.* 60: 158–169.

8 Matlack, Kathryn H., et al. 2018. "Designing Perturbative Metamaterials from Discrete Models." *Nature Materials* 17: 323-28.

9 Malkiel, Itzik, et al. 2018. "Plasmonic Nanostructure Design and Characterization via Deep Learning." *Light: Science & Applications* 7 (60).

10 So, Sunae, Jungho Mun, and Junsuk Rho. 2019. "Simultaneous Inverse Design of Materials and Structures via Deep Learning: Demonstration of Dipole Resonance Engineering Using Core–Shell Nanoparticles." *ACS Applied Materials & Interfaces*, 11 (27): 24264-68.

11 Anselmi, Nicola, and G. Gottardi. 2018. "Recent Advances and Current Trends in Metamaterial-by-Design." *Journal of Physics: Conference Series* 963: 012011; Massa A., and G. Oliveri. 2016. "Metamaterial-by-Design: Theory, Methods, and Applications to Communications and Sensing." Editorial *EPJ Appl. Metamat.* 3: 1-3.

12 Liu, Jikai, et al. "Meta-Material Topology Optimization with Geometric Control." *Computer-Aided Design & Applications* 16 (5): 951-61; Gao, Jie, et al. 2019. "Topology Optimization for Auxetic Metamaterials Based on Isogeometric Analysis." *Computer Methods in Applied Mechanics and Engineering* 352: 211-36.

13 Walsh, Timothy F., et al. 2018. "Design, Optimization and Fabrication of Mechanical Metamaterials for Vibration Control." *J Acoust Soc Am* 143 (3): 1917.

14 Brown-Shaklee, Harlan, et al. 2019. "Design of Acoustic Metamaterials for Shock and Vibration Control." Sandia National Laboratories report. *SAND2019-14281*.

15 Rummler, Troy. 2019. "Mirage Software Automates Design of Optical Metamaterials." Sandia Lab News. https://share-ng.sandia.gov/news/resources/news_releases/optical_metamaterials/; Personal communications with Ihab El-Kady (ielkady@sandia.gov).

16 Dede, Ercan, et al. 2018. "Thermal Metamaterials for Heat Flow Control in Electronics." *Journal of Electronic Packaging* 140.

17 Yoon, Sang-Hee, and Sungmin Park. 2011. "A Mechanical Analysis of Woodpecker Drumming and Its Application to Shock-Absorbing Systems." *Bioinsp. Biomim.* 6 (1): 016003.

18 Juhl, Abigail. "Dynamically Tunable Resonant Metamaterials for Acoustic and Vibration Mitigation." (Presentation at AFRL-Sandia Labs Metamaterials TIM, Albuquerque, NM, September 4, 2019). Albuquerque, NM.

19 Pagliaroli, Tiziano, et al. 2018. "Metamaterials for Hypersonic Flow Control: Experimental Tests on Novel Ultrasonically Absorptive Coatings." Proceedings of the *5th IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace)*, DFP1832W-ART: 284-289.

20 Vicari, Anthony, et al. June 20, 2019. "Metamaterials Market Forecast." Lux Research report. https://www.luxresearchinc.com/metamaterials-executive-summary.

21 Thomas, Paul "Rusty," "Blackjack," DARPA, https://www.darpa.mil/program/blackjack.

22 Treml, Benjamin, et al. 2018. "Origami Mechanologic." Proceedings of the *National Academy of Sciences*. 115 (27): 1805122115; Overvelde, Johannes T.B., et al. 2016. "A Three-Dimensional Actuated Origami-Inspired Transformable Metamaterial with Multiple Degrees of Freedom." *Nature Communications*. 7: 10929.

23 Hauser, Helmut, and Fritz Vollrath. "Leverhulme Trust Project: Computing with Spiders' Webs – An inspiration for New Sensors and Robots." http://www.morphologicalcomputation.org/the-spiders-web-as-a-computer/; Miniaci, Marco, et al. 2016. "Spider Web-Inspired Acoustic Metamaterials." Appl. Phys. Lett. 109 (7): 071905.

24 Estakhri, Nasim Mohammadi, Brian Edwards, and Nader Engheta. 2019. "Inverse-Designed Metastructures that Solve Equations." *Science* 363 (6433): 1333-8.

25 Personal communications with Francois Leonard (fleonar@sandia.gov) regarding DARPA proposal DARPA-PA-18-02-08, "Neuromorphic Computing with Optical Materials." Oct 2019.

26 Yu, Peng. 2018. "Metamaterial Perfect Absorber with Unabated Size-Independent Absorption." *Opt. Express* 26 (16): 20471-80.

27 Zhong, Shuomin, et al. 2018. "Transparent Transmission-Selective Radar-Infrared Bi-Stealth Structure." *Opt. Express* 26 (13): 16466-76.

28 Lu, Cui, et al. 2016. "Manipulating Scattering Features by Metamaterials." *EPJ Applied Metamaterials* 3 (3): 2016005.

29 Liu, Zhengyou, et al. 2000. "Locally Resonant Sonic Materials." *Science* 289 (5485): 1734-36.

30 Rummler, "Mirage Software Automates Design of Optical Metamaterials," 2019.

CHAPTER 16

Armor of the Future: Spider Webs, Buckyballs, Nanotubes, and Beyond

S. Robert Skaggs and Frank D. Gac

In Memory of

Samuel Robert (Bob) Skaggs

June 23, 1936 – February 20, 2020

Introduction: Yesterday, Today, and Projecting into the Future

Two words, "protection" and "armor," go hand in hand, as do the words "armor" and "threat." The development of armor parallels the advent of new threats, with the objective of defeating the new threats. Consequently, armor design and performance have come a long way in the last 4,000 years, be it for personnel, vehicles (including horses), or structures. Three factors seem to drive armor design with the goal of achieving maximum performance against specific threats: materials availability; weight, particularly weight per area covered (areal density); and ease of use. Overshadowing all of this is armor system manufactureablility and a "reasonable" cost.

An early example of how the connection between threats and armor can play out is recorded in the Bible in the book of 1 Samuel, when King Saul gives his armor to a teenage David to fight the fearsome giant Goliath.[1] Note this event occurs at the end of the Bronze Age and the beginning of the Iron Age.

> *Then Saul clothed David with his armor; he put a helmet of bronze on his head, and clothed him with a coat of mail. And David girded his sword over his armor, and he tried in vain to go, for he was not used to them. Then David said to Saul, "I cannot go with these; for I am not used to them." And David put them off.*[2]

In David's case, the state-of-the-art armor—a bronze helmet and coat of bronze or iron (likely a low-grade steel) mail—and the weapon—a state-of-the-art "steel" sword—were too heavy and cumbersome. David then undertook a "special operation" with a sling and some smooth stones from a brook.[i]

In August and September 2019, the authors conducted telephone interviews with existing and former members of US special operations forces (SOF). The common refrain of the special operators echoes that of David of 3,000 years earlier, albeit in slightly different wording, "the lighter and less cumbersome the armor, the better, especially for personnel armor."[3]

i Incidentally, David's battle with Goliath is also a great example of strategic latency, in which existing but latent technology, coupled with other important circumstances, result in a shift in the balance of power.

With materials availability, weight, and ease of use keenly in mind, this chapter takes the reader on a journey commencing with an assessment of the threat space the special operator faces today and may face in 20-30 years. The latter includes directed-energy (DE) weapons, such as high-energy lasers. The paper then discusses the physics, chemistry, and engineering principles that can be applied in the design of armor to defeat various threats. The journey includes examining some successful and unsuccessful armors of today, which will illustrate the remarkable advancements in materials, manufacturing and armor designs that have occurred since the 1940s. At that point, time travel begins, with the jump into the future, in which the special operator's "dream armor" is presented, accompanied by a discussion of how some advanced materials and the concept of "modeling and materials by design" might help us get there.

The Threat Space

As we look out 5, 10, 20, and even 30 years, it is clear that kinetic threats, be they bullets (perhaps even "smart" bullets), explosively formed projectiles, shrapnel (including screws, nails, and ball bearings), land mines, improvised explosive devices, and debris from nearby explosions will be a continuing concern. The Department of Defense and the National Institute of Justice have developed rigorous testing standards for armor, which include precise definitions of threats. This paper cannot present the plethora of available information on these topics. However, we do wish to call attention to the National Institute of Justice standard for body armor and a National Research Council report as important starting points for examining potential armors and advanced materials.[4]

Those documents show the design basis for body armor has been divided into five categories—IIA, II, III, IIIA, and IV—based on ballistic performance against increasingly powerful threats. For example, a new type IIA armor must defeat a 9 millimeter full metal jacket round nose (FMJ RN) bullet with a specific mass of 8.0 grams (g) [124 grain (gr)] and a velocity of 373 meters per second (m/s) $\pm$ 9. 1 m/s (1225 feet per second [ft/s] $\pm$ 30 ft/s). In contrast, a type IV hard or flexible armor must defeat a .30 caliber armor-piercing (AP) bullet (US military designation M2 AP) with a specified mass of 10.8 g (166 gr) and a velocity of 878 m/s $\pm$ 9.1 m/s (2880 ft/s $\pm$ 30 ft/s). However, for body armor, stopping the projectile is not the only issue. The armor must also not deflect to a level that would result in severe injury to the wearer, termed "blunt force trauma." This is an additional constraint that must be considered. It will be revisited later in the chapter, as we review armor-penetrator defeat mechanisms and propose new, advanced materials for future armor designs.

Now, what about directed energy threats? In 1977, George Lucas captivated moviegoers and others with the introduction of the *Star Wars* film saga, which continues today. As with most science-fiction films, it was equipped with a suite of weapons built around the concept of directed energy. Now for the real-life spoiler alert: DE weapons are here! In the October 29, 2019 issue of *Air Force Magazine*,

Kelly Hammett, who runs the Directed Energy Directorate at the Air Force Research Laboratory, stated:

> *[Directed energy technology] has matured significantly in the last five years or so. . . . Directed energy weapons are emerging in the battlespace for all three services. You're going to see them in your battlespace, whether you like it or not. They may be aimed at you."*[5]

This article refers specifically to high-power microwaves (HPMs) and high-energy lasers (HELs)[ii] as counterdrone weapons, but, once in field, they can be applied readily to other targets. So, the question becomes, "What is the DE threat to the SOF?" Let's first look at HPMs. They can be used to attack all forms of electronic systems, be they weapons, sensors, or communication systems.[6] However, a metal wrap (i.e., a Faraday shield or cage[iii]) can limit, if not eliminate, the effects of HPMs. Typical, short dwell-time HPMs have nonlethal effects on humans. Depending on the electromagnetic frequency, the HPM can produce temporary pain by stimulating nerves in the skin but causes no permanent damage. Again, a Faraday shield can limit the effect.

HELs are a different story. Each type of laser emits in a specific wavelength range.[7] In general, the output power of a laser increases with the wavelength, namely as one proceeds from ultraviolet (UV) to visible to near infrared (NIR). Diode-pumped solid-state (DPSS) laser technology is the exception. It can be engineered to emit in all three portions of the aforementioned electromagnetic spectrum. Plus, with the advent of solid-state laser technology, 50-100 kilowatt (kW) HEL weapons have evolved from the railroad boxcar-sized system to something that can be fielded on a small truck-like vehicle.[8] If we project 20 or 30 years into the future, an HEL system, which basically can burn through most objects, may even become portable by humans. The current and future HEL threat to the SOF is real and will likely increase.

Armor-Threat Defeat Mechanisms

We have some idea of both current threats and the bottom-line philosophy that armor needs to be lightweight and uncumbersome. However, before we embark on discussions of potential advanced materials for armor systems, we need to review the basic physics, chemistry, and engineering principles underpinning the ways in which armor defeats various threats, which will enlighten our materials selection.

In his famous Christmas sermon of 1967, Martin Luther King Jr. begins a statement with the words, "It really boils down to this" and completes the statement

ii HEL weapon systems are different from so-called low-energy blinding laser weapons and low-energy laser systems used as rangefinders, target designators, simulations systems, and guidance systems, where the laser itself is not used to inflict harm. The 1995 Protocol on Blinding Laser Weapons, termed Protocol IV, annexed to the 1980 Convention on Certain Conventional Weapons, prohibits "blinding" laser weapons.

iii A Faraday shield or cage is an enclosure constructed from a sheet or mesh of conductive material, usually a metal, used to block electromagnetic fields. When an external electric field encounters a Faraday cage, the electric charges within the cage's conductive material are redistributed so that they cancel the electric field's effect within the cage.

with "that all life is interrelated."[9] As we talk about armor-threat defeat mechanisms, perhaps our next word is not as socially transcendent as King Jr.'s phrase, but it is scientifically overarching. It really boils down to this: *energy*. An incoming projectile has kinetic energy. A HEL has thermal energy. A HPM has electromagnetic energy. The purpose of armor is to do something with that incoming energy, in a way that mitigates damage from weapon effects so that the operator can perform the mission.

Deflect/Reflect

One possibility is to deflect, or perhaps reflect, the energy. For an incoming projectile, this means causing the projectile to bounce off or ricochet from the surface being attacked, accomplished by having the first surface impacted at a high angle of incidence with respect to the incoming projectile. The glacis or front surface of an armored vehicle is typically slanted about 55-75 degrees with respect to the line of fire of the incoming projectile. The projectile then gouges into the glacis material, usually hard steel, tipping the trajectory of the projectile away from penetrating the vehicle hull. Thus, the maximum amount of energy in the projectile is carried away into free space. However, a downside exists. A ricochet can result in unexpected collateral damage, because one never quite knows where the deflected projectile, or piece of projectile, will travel. This is particularly worrisome for body armor, and a first-hand, real-life example will be discussed in the next section.

The equivalent mechanism for an incoming laser beam is to reflect it with a mirrored surface. However, the effectiveness depends on the wavelength of the laser.[10] For an IR beam, up to 96 percent can be reflected. For a UV beam, greater than 50 percent gets through. Things get complicated quickly with a 50-100kW HEL because the beam deposits an incredible amount of energy in a small spot, and it does not take long for the absorption of heat energy to overpower the reflectance effect. Nonetheless, this gives us food for thought about materials selection and advanced armor design.

Consume (Absorb, Break and Catch, Conduct)

Another possibility is to "consume" the energy. One way to do this is to put a sufficient thickness of steel in the armor to absorb the kinetic energy and bring the projectile to a complete stop. For the purposes of this discussion, we will restrict our focus to bullets, rather than something more severe, like a long-rod penetrator.[iv] The steel will deform, but the projectile, namely the bullet, will stop. However, steel gets heavy quickly, which defeats the objectives of lightweight and uncumbersome armor.

iv A long-rod penetrator (LRP), which is also termed a kinetic energy penetrator (KEP) or kinetic energy weapon (KE weapon), is a type of ammunition designed to penetrate vehicle armor, such as a tank (body armor does not stand a chance against this type of weapon). It maximizes the stress delivered to the target by maximizing the mass, which entails using the densest metals practical, like depleted uranium or tungsten alloys, and minimizing the width (diameter) of the projectile to focus the energy, like a stiletto high heel impacting a wood floor.

A creative alternative is to equip the armor face with a hard material that will "break up" or erode the projectile. High-strength, low-weight, ceramic plates serve this purpose well. Examples include boron carbide, silicon carbide, and aluminum oxide (listed in order of ballistic performance per areal density, with boron carbide being the best). However, because of their brittle mode of fracture, the ceramic plates also break up. Consequently, the ceramic plate must be backed up with a material that has a high strain to failure (i.e., "stretchiness") to catch the projectile and ceramic debris. This is where high-strength, synthetic polymer fibers have come into play. Aramids and the well-known commercial product Kevlar[v] represent one such class of materials. Kevlar armor basically consists of multiple layers of woven fabric mats or sheets. Another class of polymer fibers is ultra-high-molecular-weight polyethylene (UHMWPE).[vi] This takes the form of Spectra fibers, produced by Honeywell, and Dyneema fibers, manufactured by DSM. Spectra Shield Armor Panels are not a woven fabric but a thin, flexible ballistic composite made from two layers of unidirectional fibers held in place by flexible resins.

This is a good time to revisit the deflect mechanism as it relates to ceramic hard plates. Because ceramics are brittle, they break up and produce debris when impacted by the projectile. If the incoming angle of the projectile is oblique (shallow) compared to the surface of the armor, some of the debris can be forced "out." Consequently, ceramic hard faces are covered with a ballistic fabric to catch this debris and prevent it from spraying onto the soldier. Now let us discuss the first-hand, real-life example involving collateral damage, which was alluded to earlier.

One of the authors was involved in the ballistic evaluation of novel body armor, consisting of a fabric cover, then partially overlapping ceramic disks (like fish scales), and backed with a polymer fiber composite.[11] A severely oblique hit by the penetrator caused the partially overlapping ceramic disks to peel up while breaking up, causing significant spray (release) of the ceramic and projectile debris. In a real-life scenario, the result would be significant collateral damage to the wearer's neck and face. Consequently, this type of armor was removed from inventory. The novel body armor had a good basic concept in that it provided flexibility, which other hard-face body armor did not. However, upon closer examination, it had a serious flaw. Quoting a close friend of one of the authors while discussing the preparation of this book, in research "you want to be on the cutting edge, but not the bloody edge."[12]

A variation on the "consume" theme is a mechanism to bring the projectile to a slow stop, which has been used routinely in energetic materials research by filling a steel containment vessel with glass Christmas ornaments or other lightweight

v Kevlar (poly-paraphenylene terephthalamide) was invented in 1964 by Polish American chemist Stephanie Kwolek while working for DuPont. It derives its strength from strong bonding between relatively short molecules.

vi UHMWPE is made up of extremely long chains of polyethylene, which all align in the same direction. It derives its strength from the overlap of these long, molecular chains.

materials, such as perlite,[vii] to absorb and dissipate energy.[13] It has also been used to capture and study penetrators in an ~23 meter-long (75 feet-long) by ~1 x 1 m (4 x 4 ft) steel "tube," also filled with glass Christmas ornaments.[14] Finally, application of this method has been proposed for catching engine fragments from the failure of an aircraft jet engine, by lining the nacelle with a polymer "wool" that will entangle the engine fragment prior to potential penetration of the aircraft cabin.[15] One more class of materials that offers potential for slow stop are aerogels, an extremely light structure that has been dubbed "solid air."[viii]

Yet another variation on the "consume" theme involves the shear-thickening concept. A shear-thickening fluid is one whose viscosity increases with increased rate of shear stress, or, simply put, "faster mixing." It consists of tiny particles suspended in a liquid. In the version jointly developed by the Army Research Laboratory and the University of Delaware, it consists of nanoparticles of silica (high purity "sand") suspended in polyethylene glycol (a common lubricant).[16] Under normal conditions (slow stirring), the particles flow with the liquid. However, under impact (fast stirring), the particles become rigid. This technology can work well to protect against a knife or spike but any improvement in ballistic performance, for example by adding this shear-thickening fluid to a Kevlar vest, is offset by the increased weight of the fluid. One could have just as easily added more Kevlar to improve the balistic performance.

Applying the "consume" theme to a HEL threat might consist of constructing a layered armor design that absorbs and conducts the heat away from the beam spot. The specific heat capacity[ix] of ceramics is 3 to 4 times greater than metals.[17] However, the thermal conductivity of metals is 2 to 20 times greater than ceramics.[18] Thus, a plausible HEL armor concept is a high-melting ceramic face, to withstand and absorb the heat, backed by an intimately bonded metal sheet, to conduct the heat away. Perhaps an even better approach would be to incorporate an aerogel layer behind the metal sheet, to insulate the wearer of the HEL vest. Incidentally, aerogel is an even better thermal insulator than the fused silica ("ceramic") Space Shuttle tiles, displaying a 70 percent lower thermal conductivity.

React/Attack

Yet another way to deal with incoming energy is to "attack" it. One way to do this is with reactive armor. Reactive armor has taken many forms, with confusing terminology and acronyms, including explosive reactive armor (ERA),

vii Perlite is a naturally occurring, volcanic glass that has relatively high water content. When sufficiently heated, it expands greatly, resulting in a low-density filler for construction applications, such as lightweight plasters, concrete, mortar, insulation, and ceiling tiles.

viii An aerogel is not a gel but a class of porous, solid materials displaying an extremely low density. Thus, they are ultralight. Their name is derived from the fact that they are synthesized from gels.

ix The heat capacity of an object is the amount of heat required to raise its temperature by one degree Celsius. The specific heat capacity is simply a little refinement; it is the heat required to raise the unit mass of a substance by one degree Celsius. That facilitates a more meaningful comparison between materials.

nonexplosive reactive armor (NERA), semienergetic reactive armor (SERA), and electromagnetic armor.

Although the Soviets explored the ERA concept in the late 1940s, the first successful developer of ERA may have been Manfred Held in the late 1960s and early 1970s.[19] ERA consists of a slab or sheet of explosive sandwiched between two metal plates. The trigger for the explosive is the kinetic energy of the projectile concentrated at the nose of the projectile, which contacts the first metal plate and subsequent layer of explosive. The explosion moves the first plate into the direction of the incoming projectile, hence the word, "attack." The second metal plate moves away from the projectile. As the two plates move in opposite directions at a high angle with respect to the incoming projectile, they shear the projectile into fragments and drive them off the axis of the projectile. The downside to ERA is that anyone in the immediate vicinity of the exploding armor package could suffer serious collateral damage. Thus, ERA is restricted to vehicle armor for dealing with threats like LRPs.

Next, NERA refers to both nonexplosive and nonenergetic reactive armor.[20] The basic concept consists of rubber sandwiched between two metal plates. When a projectile impacts the first metal plate, the rubber is compressed (or further compressed if it was preloaded), then the compressed energy in the rubber is released, driving the plates in opposite directions, similar to the plates in the ERA but with far less energy and effectiveness. If Teflon,[x] which has a very low specific heat capacity, replaces the rubber it does not take much time and energy to heat up, as the incoming projectile drives into the face plate, causing it to decompose into a gaseous state and, thus, produce gas pressure. The gas energy drives apart the metal plates, albeit with far less effectiveness than an ERA. A further variation is semienergetic reactive armor (SERA).[21] In this case, an insensitive energetic material, such as a mixture of aluminum powder and Teflon, is sandwiched between the two metal plates. Upon mechanical impact of the projectile into the faceplate, the aluminum-Teflon mixture ignites and burns fast, releasing chemical energy to drive apart the metal plates.

Electromagnetic armor is basically a high-power capacitor, namely two or more conductive plates separated by an air gap or electrically insulating material.[22] A high-voltage power source is used to charge the armor package. When an incoming projectile penetrates the plates, it closes the circuit or triggers a switch, dumping energy into the projectile, causing it to melt and maybe even vaporize. At a minimum, the structural integrity of the projectile is reduced. Potential down sides of electromagnetic armor are the required power and the accompanying weight of the total system.

We summarize and illustrate the basic threat defeat mechanisms in Figure 1. We could present much more information, but doing so is beyond the scope of this chapter. Our objective is to present the essential information for facilitating the next

x Teflon is a commercial name for polytetrafluoroethylene (PTFE), a synthetic polymer discovered in 1938 by DuPont, consisting wholly of carbon and fluorine. It is commonly used as nonstick coating on cookware.

level of discussion about advanced materials and potential new armor designs. Nonetheless, those interested in additional detail are encouraged to explore short courses on subjects such as penetration mechanics and laser lethality science.

Advanced Materials and Armor—What Might Be Possible?

The SOF "dream armor" for the soldier is a shirt and pants that protects the entire body from the ballistic or DE threat, eliminates blunt force trauma, manages the heat load on the body, and is equipped with flexible electronics that facilitate communications, harvest and store power, monitor the health and location of the soldier, and administer immediate local medical treatment if needed.[23] That is a tall order! However, based on the content of the other chapters in Section 3 of this book, aspects of the SOF "dream armor" are not beyond the realm of possibilities, particularly as one looks out 10 to 30 years. Those other chapters—which deal with nanotechnology, flexible electronics, metamaterials (think antennas), advanced power sources, additive manufacturing, and novel energetic materials—speak to components of the "dream armor." This chapter addresses only armor needs. Nonetheless, the overlap with other chapters will be readily evident.

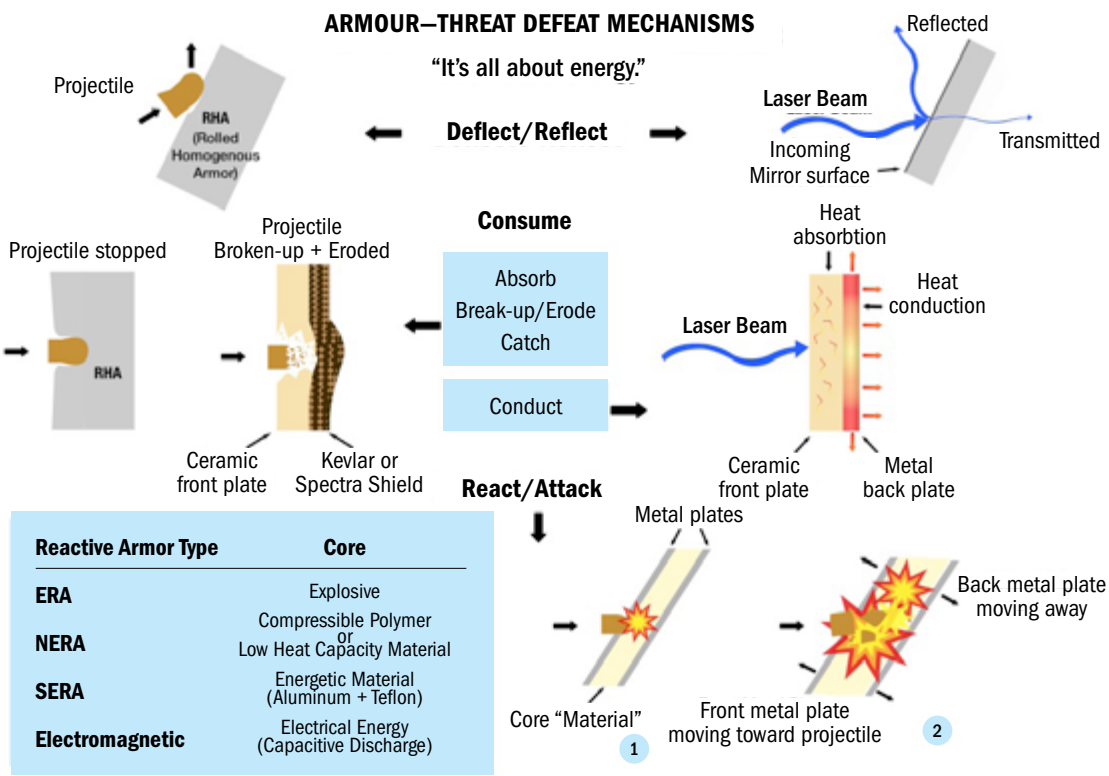


Figure 1. Summary of basic mechanisms for defeating an incoming projectile or laser beam.

Advanced Carbon Chemistry Materials

Vibranium is a fictional metal associated with at least two characters featured in Marvel Comics.[24] The Black Panther wears a flexible suit of vibranium, and Captain America has a stiff shield made from vibranium. The fictional material has extraordinary abilities to absorb, store, and release incredible amounts of kinetic energy. Analogous to a fictional metal, a nonfictional material, carbon, has evolved in a manner tht could meet some of these notional qualities. It turns out carbon chemistry has come a long way since the accidental synthesis of fullerenes in 1985.[xi] We now have "buckyballs," carbon nanotubes, and graphene at our disposal. The C_{60} buckminsterfullerene, or buckyball, has a high coefficient of restitution, meaning the energy it absorbs when hit by an object compresses the "soccer ball" shape and sends it back in the direction from which it entered. Thus, we kind of have a real-life version of the fictional vibranium.

Similarly, carbon nanotubes (CNTs) and graphene display remarkable strength. In fact, Citizen Armor, founded in 2017, offers a T-shirt-like armor, termed T-Shield, based on functionalized CNT technology, whereby the CNTs bond to each other, purportedly achieving NIJ-level IIIA body-armor performance.[25] Thus, advanced carbon chemistry research has brought us a class of materials that did not exist 20 to 30 year ago, but the next 20 to 30 years are required to learn how to synthesize the materials in quantities and at a cost viable for research study and limited commercial use.

Speaking of advacements in systhesis, the Los Alamos National Laboratory received an R&D 100 Award for "Atomic Armor," which consists of a single graphene layer.[26] In reality, the graphene layer is not armor in the traditional sense, but rather a corrosion barrier for sensitive electronic devices. However, the synthesis technique, which entails chemical vapor depositon of a single graphene layer on a wide variety of substrates, including flexible polymer films, offers the potential for manufacturing multiple graphene layer sturctures for ballistic armor applications.

However, CNTs and graphene are not the end-all, even if they do show promise, and it is important to make knowledgeable comparisons. For example, the areal density of the T-Shield armor is 6.44 kilograms per square meter (kg/m^2) [1.32 pounds / square foot (psf)], compared to the Safariland Xtreme vest, made with Kevlar fabric and Honeywell Goldshield,[xii] which displays an areal density of 5.61 kg/m^2 (1.15 psf), also for NIJ level IIIA protection.[27]

---

xi A fullerene is an allotrope of carbon (an allotrope is a different physical form in which an element can exist; for example, the element carbon can exist as graphite, diamond, and fullerenes). The fullerene molecule consists of carbon atoms connected by single and double bonds to form a closed or partially closed mesh of fused rings consisting of five to seven atoms. The family is named after the buckminsterfullerene (C_{60}), the most famous member, which in turn is named after Buckminster Fuller, an American architect who popularized the geodesic dome. The closed fullerenes, especially C60, are also informally called buckyballs for their resemblance to a soccer ball. Cylindrical fullerenes are termed carbon nanotubes or "buckytubes." Graphene (isolated layers of graphite), which is a mesh of regular hexagonal rings, can be viewed as an extreme member of the fullerene family.

xii Gold Shield GV-2018, is a roll product manufactured by Honeywell Specialty Materials, consisting of four layers of unidirectional Kevlar fiber; thus, it is not a woven fabric.

Advanced "Fibers"

We have already mentioned Kevlar, Spectra, and Dyneema, which are polymer-based fibers, and we have touched on CNTs and graphene. However, there are also continuous macrofibers made from carbon, silicon carbide, aluminum oxide (chief chemical ingredient in automotive spark plugs), and a host of other materials. Table 1 provides a comparison of key properties for some of these reinforcement materials. For familiarity, we have also included Nylon 6, E and S glass, piano wire (which is a high carbon spring steel), and human hair.

TABLE 1. PROPERTY COMPARISON OF REINFORCEMENT "FIBERS"

"Fiber"	Density (g/cm^3)	Tensile Strength (GPa)	Young's Modulus (GPa) "Stiffness"	Strain to Failure (%) "Stretchiness"	Manufacturer
Kevlar 49[28]	1.44-1.47	3.4-4.1	70.5-112.4	3.6	DuPont
Dyneema SK76[29]	0.970	3.3-3.9	109-132	3-4	DSM
CNTs[30]	0.897	8.8	357		
Graphene	0.2-1.8,[31] 2.0	0.14,[32] 130[33]	1,000[34]		
IM-6 Carbon[35]	1.76	4.4	276	1.4	Hexcel (Hercules)
Silicon Carbide SCS-Ultra[36]	3.08	5.9	415		Specialty Materials, Inc.
Aluminum Oxide Nextel 610[37]	3.9	2.8	370		3M
Nylon 6[38]		0.21	16	2.5-67	DuPont
E Glass[39]	2.54-2.55	3.1-3.8	76-78		
S Glass[40]	2.48-2.49	4.38-4.59	88-91		
Piano Wire ASTM A228[41]	7.86	1.6-2.8	79	12[42]	Optimum Spring Mfg.
Human Hair[43] (protein)		0.13	1		
Spider Silk[44] (protein)	1.25	~2	~30	~30	

As one reviews the table, keep these important points in mind:

- The lower the density, the lighter the weight of the resulting armor.
- Generally, the higher the tensile strength, the better the stopping power against a projectile.
- The higher the Young's modulus, the stiffer the material, which can be good or bad. A stiff armor can be cumbersome. However, a less stiff armor may not provide the same level of ballistic protection.
- Strain to failure, or "stretchiness," is also a mixed bag. Too high a strain to failure can result in severe blunt force trauma to the wearer of the body armor. Too low a strain to failure, and the fibers simply break.

Nylon is a well-known fabric, originally made famous by its use in women's stockings, namely "nylon" hosiery. In World War II, it was widely used by the American military for parachutes and flak jackets. Today, nylon is commonly used in motorcycle jackets. E glass is the reinforcement in everyday glass fiber-reinforced plastics, such as lawn chairs. S glass is stronger and stiffer, and therefore ideal for high-performance products, such as fiberglass boats. Piano wire is reasonably strong but heavy and, thus, generally not suitable for body-armor applications.

Kevlar and Dyneema (and Spectra) are strong materials with low density, which translates to low weight. Plus, they are readily available in commercial quantities and at "reasonable" cost. More important, they are improved constantly. Dr. David L. Reichert of DuPont recently shared that the next generation Kevlar will make a big jump in performance and be 10-20 percent lighter than current state of the art soft armor materials.[45] A SOCOM spokesperson reported it is field-testing a lightweight armor, based on Dyneema/Spectra-like materials, which weighs 25 percent less than standard armor gear, covers 44 percent instead of 19 percent of the body and offers protection against small-arms fire.[46]

As we contemplate other fibers—such as carbon, silicon carbide, and aluminum oxide, which display comparable or higher strength and significantly higher stiffness—the question becomes, "Why not consider ceramic-fiber reinforced ceramic matrix composite (CMC) front faces for armor layups?" Might these offer improved ballistic performance, multihit capability, or perhaps lighter weight? Swab and Sandoz-Rosado do a superb job summarizing the history and state of the art of CMCs for armor applications as of 2017.[47] The bottom line is CMCs may offer potential for improved ballistic protection.

However, CMCs are certainly not yet comparable to monolithic ceramic armor plates. In contrast, fiber-reinforced CMCs are making great strides in the aerospace and automotive industries, which require lightweight, high-temperature structural components.[48] We recommend monitoring advancements in these industries and reconsidering CMCs in a few years.

Bio-inspired Materials

The bottom of Table 1 highlights human hair and spider silk, both bio-inspired materials. Human hair is a remarkable material. Approximately 95 percent of a strand of hair consists of keratin, a helix-shaped protein. As illustrated in Figure 2, the structure of a hair is divided into three layers. The medulla is the porous, marrow core of the hair. Next is the cortex, the main component, consisting of long chains of keratin, in the form of macrofibrils, microfibrils, and protofibrils, which provide strength to the hair. Intercellular cement, rich in lipids (fatty acids) and protein, joins the cells of the cortex together. The third part is the cuticle, a thin protective outer armor layer, also rich in keratin and composed of cells shaped like overlapping scales.[49]

There are a number of features worth noting from the structure of the human hair, which affirm current and will stimulate advanced armor design. First is the existence of hair layers. We have already seen the value of layered structures in armor, as

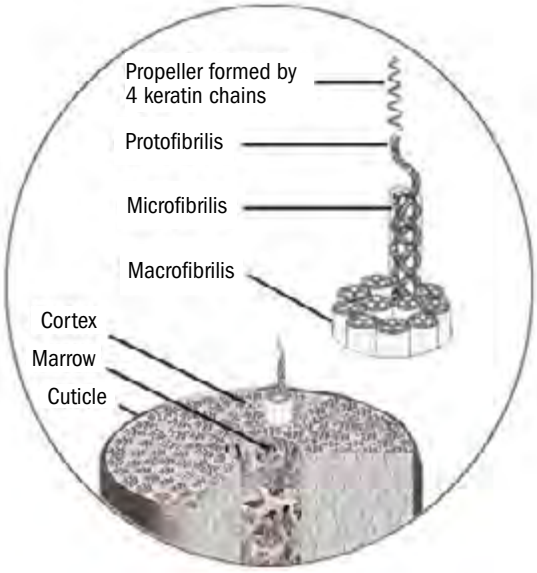


Figure 2. Structure of Hair (from reference 49).

shown in the "Consume" portion of Figure 1, which portrays a layered ceramic hard-face/polymer composite back-face (also multilayered) structure. As we contemplate advance armor designs, it begs the question of whether to use even more creative layered structures to consume and dissipate the energy of an incoming projectile. This leads to the next notable feature, intercellular cement.

In polymer-based composites, such as Spectra Shield, the polymer is the "intercellular cement" between the Spectra fibers. In metal matrix composites (MMCs), such as silicon carbide reinforced aluminum, the aluminum matrix is the "intercellular cement." In the 1980s, Ilhan Aksay and his research team pioneered innovative work pertaining to the development of boron carbide—aluminum cermet composites for lightweight armor applications.[50] Aksay and his team found inspiration in the structure of nacre, also known as mother-of-pearl, an organic-inorganic composite material produced by mollusks (think sea shells). The nacre structure is a laminated and tabular nanocomposite held together with protein, reminiscent of a brick-and-mortar structure. The man-made result is boron carbide-aluminum monoliths and laminate structures. These structures display improved multihit armor capabilities and possibly lower manufacturing cost, while achieving 90 percent of the ballistic performance of hot-pressed, fully dense boron carbide, a premier but costly ceramic armor.

One more feature worth noting is the fibrils within fibrils, which might argue for different-size fibers or even different compositions of fibers within a composite layup or weave. The objective would be to utilize materials with complementary properties to achieve enhanced performance or perhaps entirely new functions. Namely, in addition to ballistic protection, thermal conductivity might be enhanced to keep the wearer cooler, or electrical conductivity might be available to achieve a Faraday cage to protect embedded electronics.

Let us shift attention to spider silk, another truly amazing material. To start, a spider is an incredible manufacturing plant that produces a variety of silk compositions for different applications. The compositions include the dragline silk, which is used for a web's outer rim, the spokes of the web, and the lifeline as the spider transits. Another application is the silk used to secure and wrap a freshly captured prey, reported to be even stronger than dragline silk. Yet another application is the silk for temporary scaffolding during web construction. The tensile strength of spider silk is similar to high-grade steel or roughly 50-60 percent of that of Kevlar and Dyneema, but with 10 times the strain to failure and considerably more flexibility than Kevlar and Dyneema. It serves the spider well and may offer potential for creative armor design, but it has not been produced in commercially useful quantities.

Without significant advancements in synthesis, even man-made spider silk will remain in the realm of science fiction or at most a scientific curiosity. However, the spider has a characteristic just now being appreciated. We can look to the spider as a pioneer of complex additive manufacturing (AM). Advancements in this area for polymers, metals, ceramics, and, most recently, continuous fiber composites are staggering.[51] Plus, the spider illustrates the value of "portable AM," a theme of increasing importance to the defense industry.

Closing Remarks and Recommendations

We hope this chapter has been educational at the least, but ideally eye-opening and inspiring. Again, as stated earlier, advancements in materials, manufacturing, and armor systems have been remarkable since the 1940s. However, it should be noted these advancements have not been restricted to the United States; they are truly global in nature.

What are the implications of advances in armor systems for SOF? The SOF "armor of the future" is perhaps closer than one might think. Advancements in materials and manufacturing will continue, likely at a surprisingly fast pace. Below are some things to watch in the future.

- Advancements in CNTs: this offers some of the greatest opportunity for weight reduction and improved flexibility, assuming one can translate the impressive stopping power of an individual CNT to a macro system of CNTs. Chemical functionalization of the surface of CNTs may be a key to successful utilization. The same concept is applicable to interface chemistry in composites writ large, to enhance performance. In fact, chemical functualization of surfaces and interfaces may also be the approach required to incorporate infection-fighting medication or advanced electronics in the SOF's armor of the future.
- Advancements in CMCs: this is a key to tougher ceramics, while ideally maintaining high strength. This may become even more important in future body armor to deal with both ballistic and DE threats.
- Novel application of AM: for example, to produce unique laminate and functionally graded materials (FGMs) or structures. The acronym FGM has a

nice ring to it because it suggests one can accomplish multiple phenomena as one proceeds through a material or structure. In 2006, McCauley and others investigated the FGM concept for titanium-boron-based armor material, and it showed potential; but, like CMCs, FGM is not ready for primetime.[52] Perhaps advancements in AM can help advance FGMs. AM may also be an interesting approach for incorporating low-density, energy-absorbing materials, such as porous micro- or nanospheres.

- Follow the sports industry: It often leads the charge in incorporating advanced materials in commercial products. The authors heard but were unable to corroborate that graphene layers are being used in high-performance snow skis, to dampen vibration. That was one of the advantages of Kevlar-based skis developped in the 1980s. If graphene layers can accomplish the same thing, such material could be considerably lighter.
- Materials by Design: This pertains to a process of designing materials from the atomic to the macroscopic scale with the objective of producing a particular suite of mechanisms and properties that are required for specific performance and applications. It is not about how to design coponents with existing materials but rather how to select and design materials for an application. The Army Research Laboratory has spearheaded a Materials by Design effort focusing on extreme dynamic environments, like armors.[53] This merits following, and, in fact, independent activity has already shown success. The Atomic Armor, mentioned earlier, was based on a Materials by Design approach.

In closing, consider the following advice: Think "out of the box." How does one do that? Quoting a friend of a friend, "it's very simple . . . believe in 'open boxes,' 'open minds,' and 'leaving egos at the door.'"[54]

Acknowledgements

The authors wish to express appreciation to James W. McCauley and G. Andrew Erickson for their review of the manuscript to ensure it passed the technical "giggle test." In addition, a sincere "Thank You!" is extended to Evan C. Wells for transforming an author's sketch of "Armor-Threat Defeat Mechanisms" into computer-generated, world-class "eye candy." The manuscript was reviewed and approved for publication in the open, unlcassified literature by the US Government Prepublication Classification Review Board (PRB) and the Los Alamos National Laboratory. The PRB granted approval in an e-mail to Frank Gac, dated March 2, 2020. The latter approval is reflected by the Los Alamos National Laboratory Technical Information Release No. LA-UR-19-32622 Rev. 1.

Extra Note by Frank D. Gac

I first met Bob Skaggs in February 1975, shortly after hiring into what was then the Los Alamos Scientific Laboratory. We quickly became friends, and Bob was a significant mentor throughout my career, including inspiring and encouraging me to

pursue and complete a doctorate. One of my first projects was for Bob. Now, one of Bob's last professional projects was with me. What an honor and exciting journey, as we investigated radiation absorbing materials, developed advanced ceramic matrix composites, and fielded innovative armor systems! Bob, I will miss you dearly.

Endnotes

1 Harper Study Bible, Revised Standard Version, 1 Samuel 17:12-58, Zondervan, 2nd ed. (1972), pp. 417-419.
2 Harper Study Bible, 1 Samuel 17:38-39, 418.
3 Jonathan N. Fagins, Major (US Army), Naval Postgraduate School, Telephone interview, 2 August 2019; Jeffrey Wells, EyeTwo, Telephone interviews, 26 August and 4 September 2019.
4 "Ballistic Resistance of Body Armor," NIJ Standard-0101.06, US Department of Justice, July 2008, available online at https://www.ncjrs.gov/pdffiles1/nij/223054.pdf;
National Research Council. 2011. *Opportunities in Protection Materials Science and Technology for Future Army Applications*. Washington, DC: The National Academies Press. https://doi.org/10.17226/13157.
5 Shaun Waterman, "Directed Energy Weapons Move Closer to Prime Time," Air Force Magazine, 10 October 2019. http://www.airforcemag.com/Features/Pages/2019/October%202019/Directed-Energy-Weapons-Move-Closer-to-Prime-Time.aspx?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%2010.30.19&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief.
6 John Tatum, "HPM DEWS and Their Effects on Electronic Targets,"
Defense Systems Information Analysis Center, Summer 2017, Volume 4, Number 3.
https://www.dsiac.org/resources/journals/dsiac/summer-2017-volume-4-number-3/hpm-dews-and-their-effects-electronic-targets
7 Sri Venkat, "Processing Ceramics with Lasers," 1 June 2001, Ceramic Industry Magazine.
https://www.ceramicindustry.com/articles/86090-processing-ceramics-with-lasers
8 Patrick Tucker, "US Army to Test Powerful New Truck-Mounted Laser 'Within Months,'" Defense One, 16 March 2017.
https://www.defenseone.com/technology/2017/03/us-army-test-powerful-new-truck-mounted-laser-within-months/136239/;
Kip R. Kendrick, "Army Looks to Optimize Lethality with High-Energy Lasers," 18 February 2018,
January – March 2018 issue of Army AL&T magazine.
9 Martin Luther King, Jr., "A Christmas Sermon on Peace," 24 December 1967.
https://bsahely.com/2017/09/23/martin-luther-king-jr-a-christmas-sermon-on-peace-1967/
10 Sri Venkat, "Processing Ceramics with Lasers."
11 Frank D. Gac, Recollection of the ballistic evaluation of a novel body armor, 2008-2009.
12 Joseph D. Matthews, M.S., D.D.S., M.Sc., private communication, 9 November 2019.
13 Lawrence M. Hull, Los Alamos National Laboratory, private communication, 15 November 2019.
14 Work performed under National Armor/Anti-Armor Program, spearheaded by the Defense Research Projects Agency, in collaboration with the US Army, the US Marine Corps, and 130 corporations, laboratories, and universities; for overview see article by Richard Mah and Phyllis Martell, "ATAC and the Armor/Anti-Armor Program," Los Alamos Science, Summer 1989.
15 S. Robert Skaggs, consulting project with Don Shockey of SRI International, 2005.
16 Mike Hanlon, "New Shear Thickening Fluid (STF) enables flexible, comfortable armor," 13 August 2006, in New Atlas.
https://newatlas.com/go/5995/.
17 The Engineering Toolbox, "Specific Heat of Some Common Substances."
https://www.engineeringtoolbox.com/specific-heat-capacity-d_391.html.
18 The Engineering Toolbox, "Thermal Conductivity for Common Materials and Products."
https://www.engineeringtoolbox.com/thermal-conductivity-d_429.html.
19 Norbert Eisenreich, "Manfred Held, a life devoted to explosive science," Propellants, Explosives and Pyrotechnics, February 2016, vol. 41, issue 1, p. 7. https://onlinelibrary.wiley.com/doi/epdf/10.1002/prep.201680131
20 Timothy Soh, "NERA: Understanding Non-Explosive Reactive Armour," Defense Politics Asia, 17 November 2017.
http://defensepoliticsasia.com/nera-understanding-non-explosive-reactive-armour/;
Andrew Robinson, Nikki Rasmussen, and Ben Langhorst, "Non-Energetic Reactive Armor (NERA) and Semi-Energetic Reactive Armor (SERA) FY13 Final Report," Idaho National Laboratory Report INL/EXT-13-29988, August 2013.
21 Robinson, "Non-Energetic Reactive Armor (NERA)," 2013.
22 Noah Shachtman, "US Military Uses the Force," 22 August 2001, Wired News.
https://www.wired.com/2002/08/u-s-military-uses-the-force/.
23 Steve Magnuson, "NEWS FROM SOFIC: Special Operators Wearing Ultralight Version of 'Iron Man' Suit,"
National Defense, 23 May 2019.
https://www.nationaldefensemagazine.org/articles/2019/5/23/news-from-sofic-special-operators-wearing-ultralight-version-of-iron-man-suit;
Lumawant Godage, Global Military Sensors Market – Industry Analysis and Forecast (2019-2026), Science Examiner, 17 Oct. 2019.
https://sciexaminer.com/news/global-military-sensors-market-industry-analysis-and-forecast-2019-2026-46488.html.

24 "Vibranium," *Marvel Database*, https://marvel.fandom.com/wiki/Vibranium; Marvel Comics, Encyclopedia Britannica, accessed 16 December 2019. https://www.britannica.com/topic/Marvel-Comics.
25 Citizen Armor webpage. https://citizenarmor.com/.
26 Nathan A. Moody and Hisato Yamaguchi, "Atomic Armor; Innovative Nanomaterials Designed to Protect Exquisitely Sensitive Technologies with a One-Atom-Thick Shield," 2019 R&D 100 Entry, Los Alamos National Laboratory, LA-UR-19-24053.
27 The SAFARILAND Group, accessed 16 December 2019. http://www.safariland.com/brands/more.../safariland-armor/.
28 Yadav, Manishkumar D., et al., "High Performance Fibers from Carbon Nanotubes: Synthesis, Characterization and Application in Composites—A Review," *Industrial & Chemical Engineering Research,* 17 October 2017.
29 Sanborn, Brett, Ann Mae DiLeonardi, Tusit Weerasooriya, "Tensile Properties of SK76 Single Fibers at Multiple Loading Rates Using a Direct Gripping Method," Journal of Dynamic Behavior of Materials, 1.1, March 2015, https://link.springer.com/article/10.1007%2Fs40870-014-0001-3
30 Yadav, "High Performance Fibers," 2017.
31 Yadav, "High Performance Fibers," 2017.
32 Yadav, "High Performance Fibers," 2017.
33 Hone, James and Changgu Lee. "Measurement of the Elastic Properties and Intrinsic Strength of Monolayer Graphene," *Science*, 2008, DOI:10.1126/science.1157996.
34 Hone and Lee, "Measurement of the Elastic Properties," 2008.
35 Chung, Deborah D.L. Carbon Fiber Composites, Butterworth-Heinemann (1994), 67.
36 Silicon Fiber Properties, Specialty Materials, Inc., accessed 18 November 2019. http://www.specmaterials.com/siliconcarbidefiberproperties.htm.
37 3M Nextel Ceramic Fibers and Textiles Technical Reference Guide, accessed 19 November 2019. http://multimedia.3m.com/mws/media/1327055O/3m-nextel-technical-reference-guide.pdf.
38 Polyamide (PA, Nylon) 6, in MakeItFrom.com, accessed 22 November 2019. https://www.makeitfrom.com/material-properties/Polyamide-PA-Nylon-6/.
39 Wallenberger, Frederick T., James C. Watson, and Hong Li, "Glass Fibers," *ASM Handbook, Vol. 21: Composites*, (2001), p. 28. https://www.asminternational.org/documents/10192/1849770/06781G_p27-34.pdf.
40 Wallenberger, "Glass Fibers," 28.
41 ASTM Grade A228 high carbon steel, Optimum Spring Manufacturing, accessed 19 November 2019. http://optimumspring.com/technical_resources/materials/carbon_steels/music_wire_228_spring_wire.aspx
42 AISI 304 Stainless Steel vs. ASTM A228 Music Wire, in MakeItFrom.com, accessed 19 November 2019. https://www.makeitfrom.com/compare/AISI-304-S30400-Stainless-Steel/ASTM-A228-SWP-A-K08500-Music-Wire
43 Tensile Testing Hair, Instron web page, accessed 20 November 2019. https://www.instron.us/testing-solutions/by-test-type/tension/testing-hair.
44 Frank K. Ko, Sueo Kawabata, Mari Inoue, Masako Niwa, Stephen Fossey, and John W. Song, "Engineering Properties of Spider Silk," MRS Proceedings (2001). http://web.mit.edu/3.064/www/slides/Ko_spider_silk.pdf.
45 David L. Reichert, DuPont Specialty Products USA, LLC, Telephone interview, 17 September 2019.
46 Jared Keller, "SOCOM is field testing lightweight body armor originally developed for its 'Iron Man' suit," Task & Purpose, 13 November 2019. https://taskandpurpose.com/socom-body-armor-iron-man?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%2011.14.19&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief.
47 Jeffrey J. Swab and Emil J. Sandoz-Rosado, "Identifying Opportunities in the Development of Ceramic Matrix Composite (CMC) Materials for Armor Applications," US Army Research Laboratory report no. ARL-TR-7987, March 2017. https://www.arl.army.mil/arlreports/2017/ARL-TR-7987.pdf.
48 Jim Steibel, "Ceramic matrix composites taking flight at GE Aviation," American Ceramic Society Bulletin, April 2019, Vol. 98, No. 3, pp. 31-33.
49 "Structure and composition of the hair," (2018), Activilong – Paris webpage, accessed 23 November 2019. https://activilong.com/en/content/95-structure-composition-of-the-hair.
50 Danny C. Halverson, Alexander J. Pyzik, and Ilhan A. Aksay, "Boron-carbide-aluminum and boron-carbide-reactive metal cermets." US Patent #4,605,440 (1986); Alexander J. Pyzik and Ilhan A. Aksay, "Multipurpose boron carbide-aluminum composite and its manufacture via the control of the microstructure," US Patent #4,702,770 (1987).
51 Press Release: "Desktop Metal Set to Transform Continuous Fiber 3D Printing," Lynda McKinney (press contact), 1 Nov. 2019. https://www.desktopmetal.com/news/desktop-metal-set-to-transform-continuous-fiber-3d-printing/.
52 James W. McCauley, G. D'Andrea, Kyu Cho, Matthew S. Burkins, Robert J. Dowding, and William A. Gooch, Jr., "Status Report on SPS TiB2/TiB/Ti Functionally Graded Materials (FGMs) for Armor," Army Research Laboratory report number ARL-SR-143, September 2006. https://www.arl.army.mil/arlreports/2006/ARL-SR-143.pdf.
53 James W. McCauley, "Introduction to Materials by Design, Including a Dynamic Environment," Engineered Ceramics: Current Status and Future Prospects, 1st ed., Wiley & Sons, (2019).
54 Stephen J. Harkins, D.D.S., Cell phone text communication, 9 November 2019.

CHAPTER 17

Emerging Trends in Flexible Electronics: Opportunities and Challenges for a Clandestine Community

Brian Holmes and Michael David

> *Mr. Universe: Can't stop the signal, Mal. Everything goes somewhere, and I go everywhere*—Serenity[1]

Pervasive Electronic Technology in a Clandestine World—Lessons from a Fitbit

In January 2018, Liz Sly from the *Washington Post* revealed the extent to which aggregated heat map signatures, caused from worldwide data collected through fitness-device subscribers, could be tracked, revealing the location and activities of US military personnel abroad.[2] Pentagon leadership had encouraged the use of fitness devices such as Fitbit initially, promoting the utility of electronics that support a culture of physical exercise and healthy activity. Several months after the *Washington Post* revealed its discovery and subsequent implications to the security of the troops, the Pentagon released a memo restricting the use of such devices by defense personnel, particularly in sensitive locations around the world.[3]

This case is important for several reasons. Seemingly harmless, ubiquitous electronic devices are being adopted en masse for use by a global population hungry for small electronics that incorporate an incredible assortment of features, data, and sensors. An innovative product made possible by miniature rechargeable batteries, small circuits, and an interconnected data ecosystem manufactured to provide continuous feedback to the user through the interface supplants a simple watch. The idea that aggregated information from a population's watches could be exploited by foreign state and nonstate actors in a potentially nefarious manner might not have been part of the company's business plan when creating the product.

Examples like the Fitbit are part of a far more pervasive global trend built around a constantly evolving microelectronics industry. The Internet of Things (IoT), of which Fitbit plays a small part, is driving a world in which all manner of electronics will feature prominently in our daily lives.[4] The only way to meet that reality fully is for industry, academia, and government laboratories to research and develop a diverse spectrum of semiconductor materials that can be incorporated into a variety of new devices and substrates. Consumer demand in this domain is growing and insatiable. Ultimately, this technological trend poses future opportunities and challenges for US special operations forces (SOF), a community dependent on electronics and clandestine positioning.

SOF and Signals Intelligence—Historical Case Study

During the 1960s and 1970s, the United States Army Security Agency (ASA) secretly deployed Radio Research Units (RRU) in Vietnam.[5] On April 29, 1961, President John F. Kennedy formally approved the deployment of ASA personnel, the US Army's electronic intelligence branch, to support the Army of the Republic of Vietnam (ARVN). The deployment was based on Operations Plan (OPLAN) 7-61 (WHITEBIRCH) and OPLAN 8-61 (SABERTOOTH). The ASA contingent organized itself as the 400th USASA Operations Unit (Provisional) with a cover designation as the 3rd Radio Research Unit (RRU). Throughout the Vietnam conflict ASA called its units "Radio Research" to shield its presence. According to J. L. Gilbert's *The Most Secret War*, the 3rd RRU landed at Tan Son Nhut Air Force Base on May 13, 1961.[6] In the interim, the 3rd RRU created short-range direction finding (SRDF) teams, using AN/PRD-1s,[7] a lightweight mantransportable radio direction finder system. Direction finding (DF), or radio direction finding (RDF), measures the direction from which a received signal was transmitted. RDF is a key tool of signals intelligence (SIGINT) for the military. The ability to locate the position of an enemy transmitter has been invaluable since World War I and played a key role in World War II's Battle of the Atlantic (Figure 1).[8]

The war in Vietnam provides an example of how the wrong type of equipment contributed to an early tragedy. Due to equipment limitations, the SRDFs had to operate close to the enemy. Given the size and weight of the equipment, it necessitated deploying in two jeeps and a three-quarter-ton truck.[9] The example we use relates to Specialist 4 James T. Davis, an ASA cryptologist, who joined the 3rd RRU in 1961. On December 22, 1961, Davis was leading an SRDF Vietnamese team to an area approximately 12 miles from Tan Son Nhut in an attempt to locate a Vietcong guerrilla force operating in the area. They moved by truck to the area, set up, and, in concert with another SRDF team, attempted to locate the enemy using direction finding techniques. Unfortunately, 10 miles outside the base, the truck hit a mine and was attacked. Davis and nine members of his team were killed in action.[10]

This case highlighted a significant problem the Army encountered during the Vietnam era and one that remains, to a lesser extent, today: incorporating cumbersome electronic detection equipment unsuited for the terrain and environment while maintaining a clandestine posture. On May 24, 2019, the United States Special Operations Command (USSOCOM) posted a request for information, referenced on the website intelligencecommunitynews.com with the title "USSOCOM Looking for Next-Gen SIGINT." The request focused on detection, DF, and geolocation of frequency agile radio transmitters. Even though the technology has evolve, the requirements remain the same.[11]

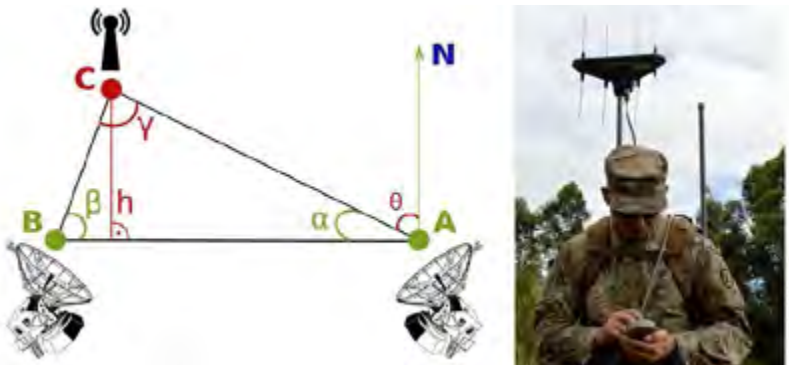


Figure 1. Radio Direction Finding—From Concept to Practice.[12]

Emerging Trends in Flexible Electronics—A New Paradigm of Materials Integration

In response to a congressional request, a committee of the National Research Council's Board on Science, Technology, and Economic Policy (STEP) reviewed programs worldwide and their potential to advance the production of flexible electronic technologies. This review resulted in a 2014 study titled *The Flexible Electronics Opportunity*, published by the National Academies Press and cofunded by the National Academy of Sciences, Department of Energy, and the National Institute of Standards and Technology.[13] According to the report, flexible electronics "refers to technologies that enable flexibility in the manufacturing process as well as flexibility as a characteristic of the final product" and can be found today in displays, image sensors, photovoltaics, and electronic paper. More important, the report noted the global market for flexible electronics could reach $250 billion by 2025 based on a significant growth rate.[14]

Circuits that bend and stretch are expected to have performance characteristics that cannot be obtained from rigid equivalents.[15] Many of these characteristics, often measured by the efficiency, technology, and lifetime of the device, are described in detail in the seminal 2010 World Technology Evaluation Center (WTEC) Panel Report "European Research and Development in Hybrid Flexible Electronics."[16] When these characteristics are combined with the promise of cost reductions predicated on printed roll-to-roll processes, they have inherent appeal. According to a 2013 symposium by the National Research Council, next generation radio frequency identification tags and organic light-emitting diode displays have already begun to displace some conventional equivalents.[17]

A 2019 article in *Macromolecules* evaluates the growing trends in flexible electronic materials, the impetus behind the research, and potential markets for their applications.[18] The article also describe clearly the barriers to progress toward more fully integrated systems. While stretchable and elastic electronic-skin–inspired polymers are being developed, self-healing, conformal, adhesive, and transient materials are still challenging to incorporate functionally without affecting device performance parameters. These limitations can be attributed primarily to a lack of flexibility in key components. However, research groups are aggressively attempting

to reconcile these known deficiencies with innovative solutions. Small wearables, the primary market driver, are expected to become more intimate, functional, and informational at the millimeter level.[19] The range of flexible electronic devices developed recently demonstrates the scope of the field, including patches to communicate with robots, wearables to detect heartbeats for healthcare, and solar cells that can be sewn into clothing.[20] According to some, elastic circuity is finally coming of age, and the national security community is taking notice.[21]

Today's SOF SIGINT units require light, mobile, and highly functional electronic devices.[22] In addition to its interest in smaller, more traditional components, the Department of Defense (DOD) has a burgeoning interest in flexible electronics. In 2005, the Army Research Laboratory actively pursued miniaturized and flexible electronics, including flexible displays and faceplates to incorporate into future military systems.[23] The Air Force Research Laboratory (AFRL) is also developing flexible and stretchable electronics and conformal devices as well as sensors for communication and analysis.

Next-generation SOF require a new wave of materials whose properties can be maintained while exposed to extreme mechanical conditions. AFRL is researching new form factors for these electronics to include textile integration of circuitry and ultrathin, high-performance materials that impart shock insensitivity and mechanical durability. AFRL is also developing integrated and robust sensing paradigms to transmit information to and from humans and machines by exploring traditional materials in nontraditional form, such as conformal printed antennas and emerging technology such as 2D materials that can be used to gather, process, and distribute information via electrical, optical, and tactile pathways.[24] In 2015, the DOD helped create NextFlex, a public-private cooperative "with a shared goal of advancing US manufacturing of flexible hybrid electronics (FHE)."[25]

So where are these developments taking us? One direction is a concept described in a patent issued in 2004 for a body-worn DF system. The system uses body-worn antennas that operate in combination with a DF processor to detect the presence of electromagnetic radiation involved in communication as well as the direction of the source of the electromagnetic radiation.[26] If Specialist Davis and his unit had been equipped with this type of technology instead of truck-borne systems, they might have been able to employ stealthier approach tactics and avoided being ambushed.

Toward Next Generation Collection Systems—Progress in Wearable Antennas

The first components required for wearable collection systems are wearable antennas. An example of this type of functional research appeared in 2012 in an *Institute of Electrical and Electronics Engineers (IEEE)* letter on antennas and wireless propagation. This research described E-fibers that offer improved mechanical and radio frequency (RF) performance when compared to traditionally flat and rigid antennas and circuits. The E-fibers comprise high-strength and flexible polymer cores that incorporate conductive metallic coatings. They are readily embroidered onto regular textiles and can be laminated onto polymer dielectric substrates. Prototype

body-worn, multiband/wideband antennas and medical biosensors were constructed to demonstrate their efficiency and comparable performance to that of copper. The designs were fabricated with high precision and resolution down to 0.5 mm.[27] The chemistry and fabrication are complex, but the authors elucidate the complexity in detail. For our purposes, suffice it to say, RF and sensor designs can be translated into embroidery software, followed by digitizing stitches of the assistant yarn. Figure 2 outlines the concept and process.

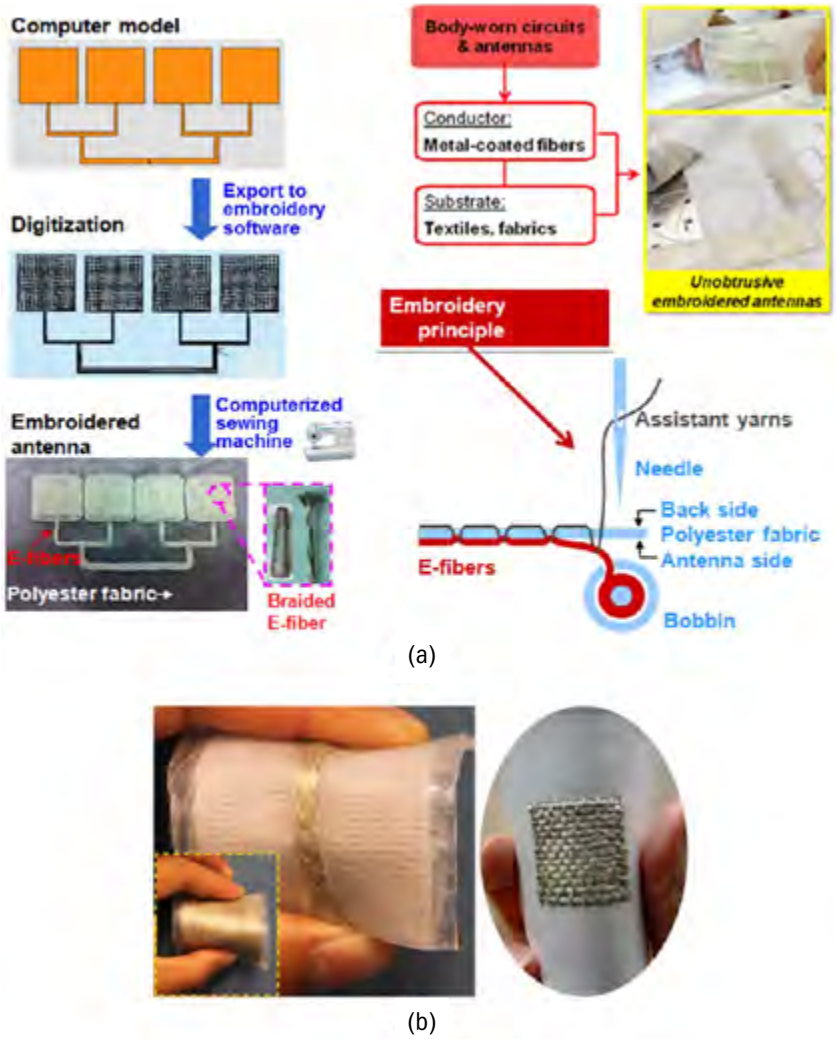


Figure 2. (a) Fabrication process of body-worn antennas, sensors, and RF circuits. These E-fiber RF components offer several new functionalities unavailable previously, such as inconspicuous weaving into garments, omnidirectional high-strength signals for connecting faraway cell towers and even satellites, and excellent conformality for interior body imaging. (b) Fabricated textile transmission line and patch antenna after placement onto a polymer substrate.[28]

L. Zhang and others described the design and fabrication of a textile, triband antenna. The multiband antenna was designed using E-fiber fabrication, displayed in Figure 3(a). The antenna covers three communication bands, namely the GSM (850 MHz), PCS (1900 MHz), and WLAN (2450 MHz). The fabricated textile antenna and its RF performance are exhibited in Figure 3(b) and (c).

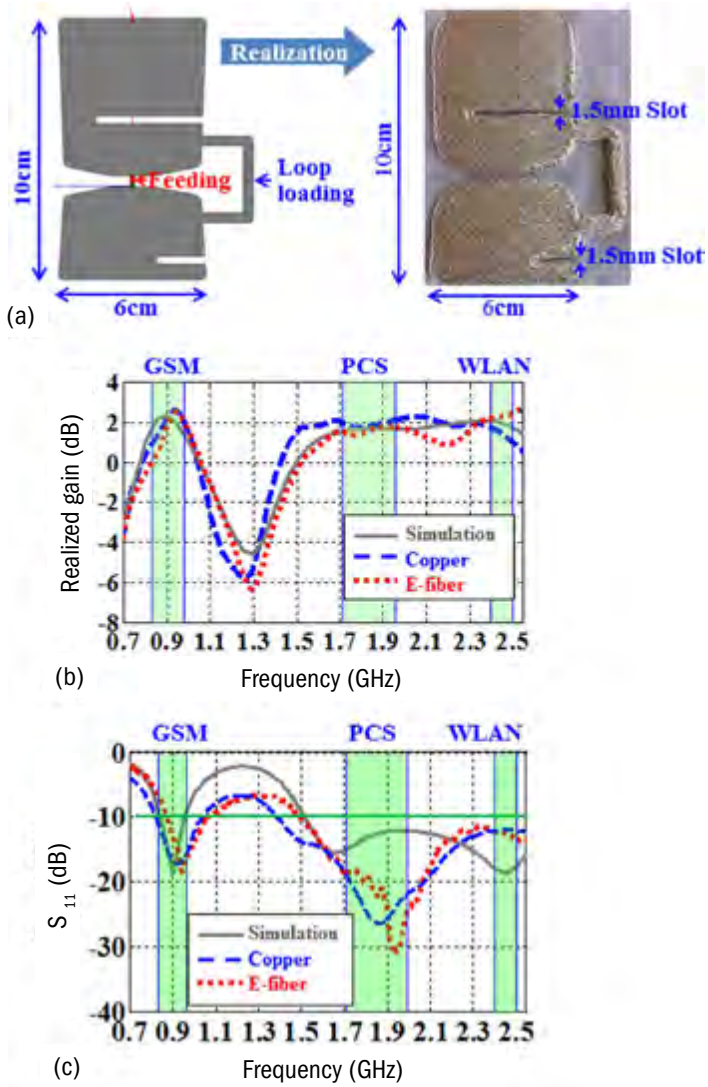


Figure 3. Textile version of the triband antenna: (a) design and fabricated antenna, (b) realized gain, and (c) return loss.[29]

In June 2019, M. El Abassi and K. Kablin reviewed the main technological advances and contributions in the field of wearable antennas for wireless body-sensor network applications.[30] The research focused on detecting the body when exercising,

monitoring vital signs like pulse and blood pressure, and determining general network connection, rather than focusing on DF.[31] The capabilities described in the article reflect considerable improvements in flexibility and overall functionality. Most important, they reveal smaller size, lighter weight, and less effect on the human body than previous incarnations. The systems are nearly maintenance free, comfortable, and meet durability requirements.

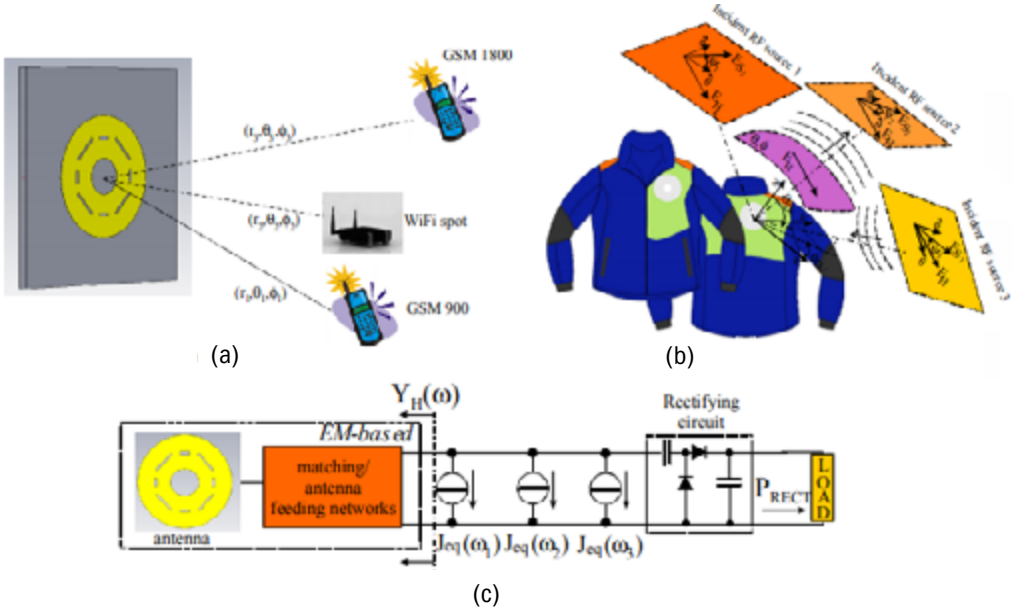


Figure 4. (a) Multiple incident RF sources of wearable rectenna. (b) Harvesting antenna electromagnetic (EM) field sources. (c) Tri-band wearable rectenna circuit.[32]

Figure 4 illustrates the main incident RF sources of wearable antennas, the rectifying circuits of each, and their affect on on-body wireless communication. The authors concluded the most important considerations for future research include the selection of material, critical parameters of antenna performance, conductive ground plane dimensions, material conductivity, the use of electromagnetic band gap structure, human body effect on antenna performance, and specific acceptable absorption rate levels.[33]

According to researchers at Florida International University, the goal for textile-based electronics is to enable communications, IoT, and sensing without using handheld devices or additional accessories.[34] Existing sensor electronics, including micro-electromechanical system sensors, remain rigid and bulky.[35] Military operators carry an incredible amount of weight and gear. In addition to armor and weaponry, batteries for electronics account for a significant percentage of the load.[36] Stealthy activities inherently require less obtrusive equipment. In 2016, researchers at the US Army's Natick Soldier Research, Development, and Engineering Center evaluated textile-based supercapacitors (designed to serve as power sources) incorporated

into military uniforms to enable the autonomy of wearable sensors. Examples of the wearable sensor technology include eyewear, smart textiles, tattoos, and jewelry, as displayed in Figure 5.[37] A significant percentage of the notional military-applied technology is predicated on advancements in the flexible electronic material sector.

Figure 5. Screen-printed Military Textiles for Wearable Energy Storage[38]

Back to the Future

As noted earlier in the section, Specialist Davis was killed in 1961 while leading an SRDF team moving in trucks and jeeps along an open road. In an attempt to overcome this type of land-based targeting vulnerability, the Army began to employ airborne radio direction finding (ARDF) capabilities. Once again though, there were initial weaknesses with the platform. In the case of ARDF, the main challenge was selecting the right type of aircraft to employ the system correctly. Early tests using a UH-19 "Chickasaw" helicopter failed because of structural vibration problems. Subsequently, engineers turned to the U-6A, which was a small, fixed-wing aircraft nicknamed the "Beaver."[39] Fortunately, there were numerous U-6 aircraft utilized in Vietnam at the time, and, as a result, maintenance support was readily available.

The aircraft also provided the pilot good ground visibility and could transport three crew members plus a small load of equipment.[40]

The 3rd RRU conducted one early effective demonstration of ARDF in an attempt to locate, identify, and destroy the Vietcong communications net in 1962. Staging from Qui Nhon on the central coast and Da Nang, aircrews flew two U-6s during a four-day operation in mountainous regions under hazardous conditions. On May 27, the Republic of Vietnam Armed Forces responded to the ARDF fixes with air strikes, successfully destroying a command post.[41] In February 1964, the 400th USASA Special Operations Detachments (SOD) deployed a team for a 120-day field test in Vietnam. For the next two years, personnel of the 400th shuttled back and forth to Vietnam from Okinawa on one-of-a-kind assignments. These missions provided an opportunity to test direct support to tactical forces and represented an important milestone in shaping ASA's future assistance to Special Forces (SF). This included developing techniques to exploit SIGINT and ARDF to support SOF missions.[42]

Based in part on the successes of the 400th, 51 soldiers of the 403rd ASASOD deployed from Fort Bragg to conduct SIGINT to support the 5th SF Group in September 1966. The 403rd ASASOD strove to provide communications-intelligence support at the lowest tactical level possible while maintaining maximum mobility and flexibility.[43] During its first year in Vietnam, the 403rd focused on targets in the northern II Corps area. The 403rd ASASOD—based in Kontum—conducted manned manual Morse intercept and ARDF tip-off, deployed DF/voice intercept teams, ran the local DF net, and performed second- and third-echelon maintenance. The 403rd could also deploy a small intercept team to support mobile operations.[44]

Today, virtually the same functions are performed by US Army Special Operation Team Alpha (SOT-A) units. The mission of a SOT-A is to conduct signals intelligence/electronic warfare (SIGINT/EW) to support information operations (unilaterally or in conjunction with other SOF elements) and to facilitate existing and emerging SOF missions worldwide. SOT-As are the direct descendants of the USASASODs.[45] The major difference is the surrounding operational environment.

The Future Operational Environment

Special Operations Forces Acquisition, Technology, and Logistics (SOF AT&L), a critical component of USSOCOM, posted information describing three areas of importance to their near and future (2020–2030) mission: small unit dominance, mission assured communications, and signature management. Each post conveyed several technical requirements contextualized against a reassessment of their mission and force posture.[46] The significance of advanced materials, manufacturing, communications, and concealment of presence were referenced throughout the areas, as was the importance of size and weight restrictions for the operators in remote and highly contested environments.

In every area the need for new sensors and electronics incorporated into the operator's toolkit were implied as a high priority. Advancements in embedded flexible

electronics, once fully realized, could be used to conduct specialized reconnaissance missions and exact human-intelligence-enabled SIGINT, in addition to integrating biosensors specifically designed for health monitoring for more effective soldier performance. Clandestine operators are often "first in" the fight and forward deployed to better determine the position and capabilities of the enemy through information-gathering techniques, exactly why the USASA secretly deployed RRUs to Vietnam and their more recent counterparts to Afghanistan after the events of 9/11.

In 2018, United States Marine Corps Forces Special Operations Command (MARSOC) published "MARSOF 2030—A Strategic Vision for the Future" to evaluate the future operating environment based on their unique vantagepoint. To meet their commander's intent, the author(s) depicted two conceptual vignettes and guiding concepts to better prepare the force for "service in a volatile and uncertain future." Both vignettes better delineate the types of scenarios in which the military might find itself where technology solutions could enable small units to reach their objectives using minimal footprint solutions. Each highlighted or implied SIGINT via manned and unmanned platforms and integrated data analysis through a variety of different types of sensor interfaces.[47]

A more daunting challenge might be how to develop and deploy sensors, including flexible electronics predicated on low-power systems, that will operate not only in jungles, deserts, and mountainous regions but also in dense urban terrain (DUT). Even more esoteric would be how to conduct SF cyber operations in DUT.[48] Some of the key factors affecting the environment include IoT devices, surveillance cameras, and "always on" personal assistants like Alexa and Siri.

Adding further complexity, the United States or allied entities do not make, supply, or maintain many IoT devices and surveillance systems. For example, DuerOS, Baidu's answer to Amazon's Alexa, has reached over 200 million deployed devices. This means the DuerOS is built into Baidu-built and third-party related devices.[49] Emerging 5th generation (5G) mobile networks are primarily supplied by the Chinese firm Huawei. Chinese tech companies—particularly Huawei, Hikvision, Dahua, and ZTE—supply artificial intelligence surveillance technology in 63 countries, according to a September report by the Carnegie Endowment for International Peace think tank.[50] Of those nations, 36 have signed onto China's massive infrastructure project, the Belt and Road Initiative.[51] These Chinese-built surveillance systems are likely to be found in the megacities around the globe where SOF units may have to operate. What might this environment look like? How can we exploit these systems? How can airborne and terrestrial autonomous systems, such as drones and robot sensors, be linked to both SOT-A units and embedded electronics to provide situational awareness?

Conclusion

According to the US Army Training and Doctrine Command summary of ES2, "the individual soldier is the most capable, sophisticated collector of intelligence in today's Army."[52] Ideally, each soldier acts as a sensor. Not only do SOFs require

a spectrum of new electronic materials to develop innovative sensor technology, including flexible embedded devices, but they also need to function in an electronically networked society. An additional challenge will be developing the capability to deploy these devices in the underground scenario described in author John Higgins's article for the Army titled "R2TD: A New Tool for an Ever-Present Threat."[53] Tunnels are as effective as any known electronic jammer.

Regardless the conundrums facing the devlopment and implementation of flexible electronics, the military clearly realizes the distinct advantages flexible electronics can enable based on historical endeavors, from the Defense Advanced Research Projects Agency–led display research to more recent joint ventures, such as the 2004 establishment of the Flexible Electronics and Display Center at Arizona State University with the US Army.[54] Ideally, global advancements in materials and manufacturing research can align with commercial market drivers and user input from the operators to formalize innovative solutions such as body-worn direction finding (DF) systems. History demands an approach Specialist Davis would approve of.

All statements of fact, analysis, or opinion are the author's and do not reflect the official policy or position of the National Intelligence University, the Department of Defense or any of its components, or the US government.

Endnotes

1 *Serenity*, 2005, directed and written by Joss Whedon, featuring Nathan Fillion, Gina Torres, Chiwetel Ejiofor, Universal Pictures, https://www.imdb.com/title/tt0379786/characters/nm0472710.
2 "US Soldiers Are Revealing Sensitive and Dangerous Information by Jogging," *Washington Post,* January 29, 2018, https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?utm_term=.ea3f51bb2ddb.
3 "Pentagon Restricts Use of Fitness Trackers, Other Devices," AP News, August 06, 2018, https://apnews.com/d29c724e1d72460fbf7c2e999992d258.
4 "Say Goodbye to Privacy," *WIRED*, February 5 2015, https://www.wired.com/insights/2015/02/say-goodbye-to-privacy/.
5 "History of the Army Security Agency," National Security Agency, https://www.nsa.gov/news-features/declassified-documents/army-security-agency/.
6 J. L. Gilbert, *The Most Secret War: Army Signals Intelligence in Vietnam, Military History Office, INSCOM,* January 2003, https://ia800403.us.archive.org/34/items/mostsecretwararm00fort/mostsecretwararm00fort.pdf, 5-7.
7 Gilbert, *Most Secret War*, 10.
8 Williams, Secret Weapon: US High-Frequency Direction Finding in the Battle of the Atlantic, 1996.
9 Gilbert, *Most Secret War,* 10.
10 "James Thomas Davis," Virtual Wall, Vietnam Veterans Memorial, June 19, 2004, http://www.virtualwall.org/dd/DavisJT01a.htm
11 Blinde, L., "USSOCOM Looking for Next-Gen SIGINT," May 28, 2019, https://intelligencecommunitynews.com/ussocom-looking-for-next-gen-sigint/.
12 "Electronic Warfare Soldiers Train with Radio Direction Finding System," Army.mil, April 11, 2018, https://www.army.mil/article/203723/electronic_warfare_soldiers_train_with_radio_direction_finding_system.
13 *The Flexible Electronics Opportunity,* Washington, DC: The National Academies Press, National Research Council, 2014, https://doi.org/10.17226/18812.
14 TMR, Flexible Electronics Market—Global Industry Size, Share, Trends, Analysis and Forecasts, 2012–2018 (2013).
15 *Flexible Electronics Opportunity*, 2014
16 "European Research and Development on Hybrid Flexible Electronics," World Technology Evaluation Center (WTEC) Panel Report, July 2010, https://apps.dtic.mil/dtic/tr/fulltext/u2/a532818.pdf.
17 Brown, "Impact of a Flexible Form Factor for Displays and Lighting," in National Research Council, *Flexible Electronics for Security, Manufacturing, and Growth.*
18 Tran, H.; et al., "Polymer Chemistries Underpinning Materials for Skin-Inspired Electronics." *Macromolecules* 2019, 52, 3965-3974.
19 Tran, H, "Polymer Chemistries," 3965-3974.

20 Scudellari, M., "Printing Electronics Directly on Delicate Surfaces—Like the Back of Your Hand," *IEEE Spectrum*, October 10, 2019, https://spectrum.ieee.org/the-human-os/biomedical/devices/printing-electronics-directly-on-delicate-surfaces.
21 "It's 2016, So Where Are Our Flexible Electronics?" *Gizmodo*, January 20, 2016, https://gizmodo.com/its-2016-so-where-are-our-flexible-electronics-1750986122.
22 CRFS, "SIGINT Capability for Special Operations Forces," https://www.crfs.com/blog/sigint-capability-for-special-operations-forces/.
23 Army AL&T Magazine, May-June 2005, https://asc.army.mil/docs/pubs/alt/archives/2005/May-Jun_2005.pdf, Pg-48.
24 Air Force Research Laboratory, https://community.apan.org/wg/afrl_materials/flex/.
25 Nextflex, https://www.nextflex.us/.
26 Patent No.: US 6,771,224 B2, issued August 3, 2004, https://patentimages.storage.googleapis.com/6b/9a/3d/6d166ccecb83f7/US6771224.pdf.
27 Zhang, L., Zheyu Wang, J. L. Volakis, "Textile Antennas and Sensors for Body-Worn Applications," *IEEE Antennas Wireless Propag. Lett.*, vol. 11, pp. 1690-1693, 2012.
28 Zhang, "Textile Antennas," 1691.
29 Zhang, "Textile Antennas," 1691-92.
30 El Abassi, M., and K. Kablin, "Revolutionizing the Development of Wearable Antennas", *IEEE Xplore,* June 6, 2019, https://ieeexplore.ieee.org/abstract/document/8730832, Accessed Sep 2, 2019.
31 "Soldiers May Soon Have Implantable Health Monitors and Robotic Surgeries Done Remotely," *Army Times,* May 18, 2018, https://www.armytimes.com/news/your-army/2018/05/18/soldiers-may-soon-have-implantable-health-monitors-and-robotic-surgeries-done-remotely/.
32 Costanzo, Alessandra, Diego Masotti, and Martino Aldrigo. "Compact, Wearable Antennas for Battery-Less Systems Exploiting Fabrics and Magneto-Dielectric Materials. Electronics (Basel)," 2014, https://www.researchgate.net/publication/307825202_Compact_Wearable_Antennas_for_Battery-Less_Systems_Exploiting_Fabrics_and_Magneto-Dielectric_Materials3.10.3390/electronics3030474.
33 Abassi, 57.
34 Carnegie Mellon University website, https://www.cmu.edu/nanotechnology-forum/Forum_14/US_Presentation/4_C%20 Volakis--US-Korea%20Forum%20on%20Nanotechnology.pdf
35 "As US Army Rethinks How Soldiers Will Communicate in Future Combat, Harsh Realities Loom," Forbes, Sep 7, 2018, https://www.forbes.com/sites/lorenthompson/2018/09/07/as-u-s-army-rethinks-how-soldiers-will-communicate-in-future-combat-harsh-realities-loom/#17e3d9ad342a.
36 "The Overloaded Soldier: Why US Infantry Now Carry More Weight than Ever," *Popular Mechanics,* December 26, 2018, https://www.popularmechanics.com/military/research/a25644619/soldier-weight/.
37 Zopf, S. F., and M. Manser, "Screen-Printed Military Textiles for Wearable Energy Storage," *Journal of Engineered Fibers and Fabrics,* Volume 11, Issue 3, 2016.
38 Zopf, "Screen-Printed Military Textiles," 2016; "Global Military Sensors Market—Industry Analysis and Forecast (2019-2026)," *Science Examiner*, October 17, 2019, https://sciexaminer.com/news/global-military-sensors-market-industry-analysis-and-forecast-2019-2026-46488.html.
39 G. B. Blackburn, and L. M. Long, *Unlikely Warriors: The Army Security Agency's Secret War in Vietnam 1961-1973,* 2013.
40 Gilbert, *Most Secret War,* 13.
41 Gilbert, *Most Secret War,* 14.
42 Gilbert, *Most Secret War,* 22.
43 Gilbert, *Most Secret War,* 41.
44 Gilbert, *Most Secret War,* 42.
45 US Army FM 3-05-102, Army Special Operations Forces Intelligence.
46 Special Operations Forces Acquisition, Technology, and Logistics (SOF AT&L), Hard Problems, Science & Technology – Preparing for the Future 2020-2030, https://www.socom.mil/SOF-ATL/Pages/SOF-Hard-Problems.aspx, Accessed Sep 03, 2019
47 Marine Forces Special Operations Command, March 2018, MARSOF 2030 – A Strategic Vision for the Future, https://www.marsoc.marines.mil/Portals/31/Documents/MARSOF%202030.pdf?ver=2018-03-29-143631-557.
48 Maxwell, P., Hall, A., and Bennett. D., "Cyber Operational Considerations in Dense Urban Terrain", URL: https://smallwarsjournal.com/jrnl/art/cyber-operational-considerations-in-dense-urban-terrain, Accessed 27 Oct 2019.
49 "China's Baidu says its answer to Alexa is now on 200M devices", *TC*, January 8, 2019, https://techcrunch.com/2019/01/07/baidu-dueros-200-million-devices/.
50 Maxwell, P., "Cyber Operational Considerations," 2019.
51 "The Global Expansion of AI Surveillance," *Carnegie Endowment for International Peace,* September 17, 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.
52 US Army, https://www.army.mil/standto/2005-07-26.
53 US Army, October 27, 2019, R2TD: A new tool for an ever-present threat, https://www.army.mil/article/229037/r2td_a_new_tool_for_an_ever_present_threat.
54 The Flexible Electronics Opportunity, National Research Council, 2014, Washington, DC: The National Academies Press, https://doi.org/10.17226/18812, p-236-237.

CHAPTER 18

Adapting SOCOM to an Electrified World

Karen Swider-Lyons, Joshua Lamb, and Yet-Ming Chiang

Introduction

The United States Special Operations Command (SOCOM) envisions its future with hyper-enabled operators empowered by "data assets, adaptive and flexible sensors, scalable tactical communications, edge computing, embedded algorithms, and tailorable human-machine interfaces . . . integrated into architectures that will sense, monitor, transport, process, and analyze data to aggregate information."[1] Many of these technological advances are possible because of the rapid pace of microelectronics development, which has famously followed Moore's law. This extra computing power however is increasingly hungry for electrical power.

Underlying the fielding of advanced communication, computing, and sensors is the need for adequate electrical power and energy. Vast technological changes have occurred since the 1980s in electrochemical power sources, particularly with lithium-ion battery technology for mobile devices, automobiles, and energy storage. Fuel-cell technology is also being steadily commercialized. The capacity of batteries depends on their chemical composition but has been doubling once every ten years as new materials are discovered and developers can cram more "energy in the can." Fuel-based systems are progressing slower because the energy content of fuels is fixed; however, improvements are made through creating lighter and more efficient conversion devices. To accommodate additional energy requirements for microelectronics, developers of commercial electronic products simply use more space and weight in devices for the power sources, a design luxury that SOCOM might not have.

We assert continued progress in electrochemical energy technologies by 2050 will affect SOCOM significantly, as electric-powered, unmanned systems become more effective, assuming that SOCOM manages the resources appropriately. Power requirements will increase for communication in Global Positioning Systems–denied areas, as both the distance between receivers and transmitters increases and signals must overcome clutter in the environment. Electrical energy is poised to have an even broader impact as the Department of Defense (DOD) moves to directed-energy weapons and as demands increase for high-quality power at its temporary installations for electronics and communications. New technologies are trending toward increased electrification of even traditionally nonelectric devices, with the gap for implementation often being the lack of a suitable power source.

Maintaining future technological supremacy requires developing and adopting power sources capable of powering new advances. The United States might also depend on different countries to keep access to the materials needed for new energy sources and rely less on oil-producing countries. This chapter attempts to project how

the movement to electric power sources, such as batteries and fuel cells, may affect SOCOM's technological and geopolitical outlook by 2030.

Electrochemical Energy Systems

Lithium-Ion Batteries for Energy Storage

In 1991, Sony first commercialized rechargeable lithium-ion batteries (Li-ion) for portable electronics in Japan.[2] Since then, the energy-storing capacity of Li-ion batteries has increased by more than three times, while their cost has decreased by 85 percent since 2010. Such increases in capacity and decreases in cost are forecast to continue as Li-ion batteries have become ubiquitous in everything from tools to automobiles. As the manufacturing and safety of these batteries continues to improve, they are being applied in on-grid and off-grid energy storage when coupled with wind or solar power. The market prospects for Li-ion batteries and related energy storage systems are discussed in *Future of Batteries: Winner Takes All?* Investments in battery-related technologies by the private sector were $13.7B in 2016–2017, and such investments continue to grow.[3]

Rechargeable Li-ion batteries are electrochemical energy storage devices that store energy produced by another source (e.g., natural gas/turbines, diesel/generators, solar panels). As illustrated in Figure 1, the materials in the cathode and anode of the batteries shuttle lithium ions between them upon charge and

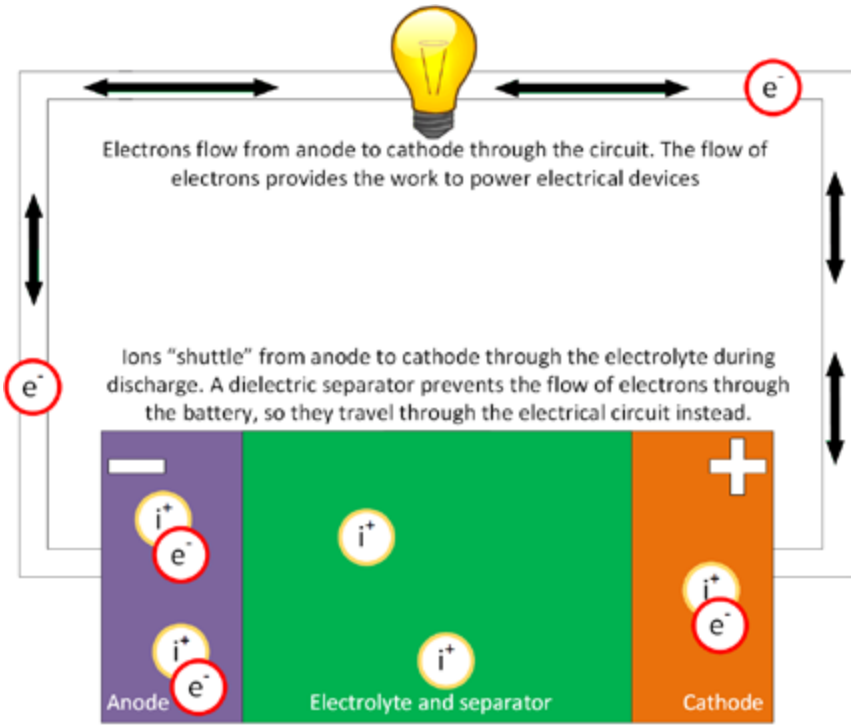


Figure 1. Schematic of battery charging and discharging. The cycle is about 90–95 percent efficient.

discharge. During charging, the cathode transition metal oxides (containing typically cobalt, nickel, and manganese) release electrons and positively charged lithium ions to the carbon/graphite anode of the battery. The reverse process occurs on discharge, and the potential energy of the stored electrons is released to an external device. Li-ion batteries store more energy than their lead-acid or nickel-cadmium counterparts, mainly because their chemistry yields a higher voltage (nominally 4 volts versus 1.5 volts for lead acid). Power (P) in watts (W) is equivalent to the product of voltage (V) and current (I) represented as ($P = V \times I$). Energy (E) is power over time, expressed as ($E = [V \times I] / t$).

Li-ion batteries also feature much higher cycle life than other rechargeable technologies, with commercially available technologies able to achieve 500 full charge-discharge cycles or more before losing energy storage capability.[4] The materials in Li-ion batteries are also lighter than in their traditional counterparts, giving them higher power and energy-per-unit weight and even volume. New materials and manufacturing methods have been developed to make batteries lighter and denser, so more watts and watt-hours (Wh)[i] are produced per unit weight or volume of the batteries, with projections for more improvements. Further details of Li-ion battery materials and technology, plus future prospects, including environmental impact and lifecycle costs, can be found in "Science for Environment Policy: Towards the Battery of the Future."[5]

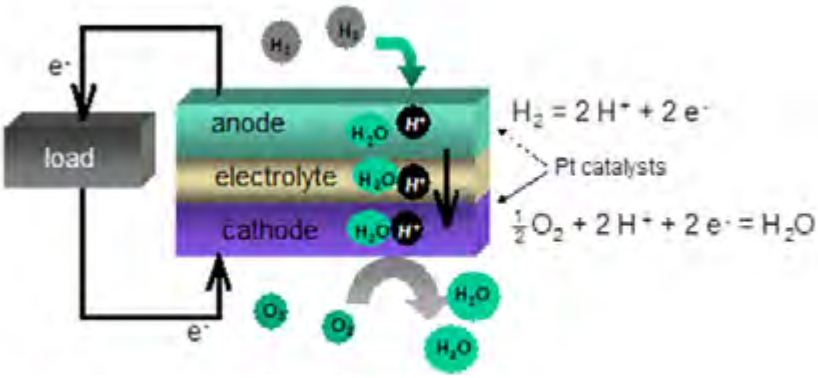
Li-ion batteries, however, have not broken the relationship between power and energy (typically, increasing power capability leads to a reduction in stored energy and vice versa), making battery selection highly dependent on the application. A careful consideration of power, energy, and operating conditions (particularly temperature) must be considered when selecting a battery for an application. Li-ion, for example, typically has a narrow operating window of ~5–55°C.[4] Selecting the wrong battery for an application can lead to a device being unable to complete its mission, or it can even present a safety hazard to users. The stored energy in batteries always carries an inherent risk, described in greater detail later in this chapter.

Fuel Cells

Fuel-cell technologies are also poised to change how energy is distributed worldwide. As illustrated in Figure 2, like batteries, fuel cells produce electricity directly via electrochemical reactions at the cathode and anode; however, the fuel cells are open and use air for the oxidizer, and they do not store energy (the energy resides in the fuel). The reactions are facilitated by electrocatalysts, typically containing platinum, and the electrolyte is a perfluorinated polymer, such as Nafion.[ii]

i A watt-hour is a measure of electrical energy equivalent to one watt (1W) of power expended in one hour (1h) of time.

ii Nafion is a brand of the Chemours Company.



Proton Exchange Membrane fuel cell
Perfluorosulfonic acid (Nafion polymer) membrane

Figure 2. Schematic of hydrogen, or PEM, fuel-cell mechanism.

Hydrogen fuel cells—the most advanced type of fuel cell—are being used for automobile propulsion, materials handling (forklifts), and backup power. Hydrogen fuel cells operate at low temperatures (e.g., less than 100°C) and with approximately 60 percent efficiency. Hydrogen fuel cells fill some niches well. Because they convert the high energy of hydrogen gas to electricity efficiently, they typically have more energy than large-scale batteries. They refuel quickly, keeping equipment in use longer than those powered by batteries, a key attribute for warehouse forklifts and fleet vehicles. The cost of fuel-cell development is mainly in manufacturing rather than in raw materials, so experts project their cost to decrease.[6] While investment in fuel cells is far smaller than into batteries, fuel-cell automobiles are being developed worldwide; Japan, South Korea, and China have set ambitious goals to have millions of fuel-cell cars on the road by 2030 and are also targeting long-haul trucking.[7] Amazon bought a large stake in Plug Power for its fuel-cell forklift business.[8] Cummins bought a large stake in Hydrogenics for hydrogen fuel cells and hydrogen production for backup power.[9]

Hydrogen fuel is the main detraction for fuel cells, as it must be made by reforming natural gas or electrolyzing water by processes that are marginally efficient. The hydrogen is typically stored at high pressures, and the infrastructure has been too sparse to make it convenient for most consumers. More recent demonstrations have shown that hydrogen is an asset, as renewable energy plants are able to make it "for free" with excess solar and wind. Excess electricity is provided to electrolyzers to produce hydrogen from water. The hydrogen is either fed into natural gas lines or compressed and stored as fuel.[10] Hydrogen can also be stored indefinitely, with no loss of energy (unlike batteries, which will self-discharge).

Other types of fuel cells include direct methanol fuel cells—which are limited to small sizes because of thermal restrictions with heat rejection—and solid oxide fuel cells, which operate near 800°C typically on natural gas, but have not been as

successful on liquid fuels such as JP-8.[iii] As discussed later, these types of fuel cells have some niche markets for the military.

Electric Power for SOCOM Missions

Portable Power

The heavy load of batteries required for the dismounted soldier is a well-known problem. US Marines inculde batteries as one of the three B's needed for survival: "Beans, Bullets, and Batteries." The US government has spent hundreds of millions of dollars for new energy systems in the 20–50 watt range, or adequate to power radios and communication systems. The Army strives to network all the power loads on the soldier so that only one type of battery must be carried. A range of technologies has been explored, such as lithium batteries, energy-harvesting devices (e.g., heel strikes[iv]), and direct methanol fuel cells. Researchers also explored solid oxide fuel cells and Stirling engines[v] because of their promise of operating on JP-8 only.[11] While this government investment clearly "energized" the interest in small power sources, the main technology now in this power range is rechargeable Li-ion batteries.

The specific energy and energy density of state-of-the art batteries is given in Table 1, along with values for some small, commercial fuel cells and the target for the next generation of automotive battery systems. The military has adapted Li-ion batteries to conform to soldiers' bodies, thus providing better volumetrically efficiency. Methanol fuel cells (using liquid or reformed methanol) have had some successes, as have propane-fueled, solid oxide fuel cells. However, no energy-harvesting devices beyond solar blankets have been deployed for the military. Stirling engines never received enough investment to get beyond the prototype stage. Polymer electrolyte membrane (PEM)[vi] fuel cells with compressed hydrogen (Figure 2) are the most effective for energy-per-unit weight (specific energy), although they are not energy dense. Compressed hydrogen is unappealing for a soldier to carry. Using solid forms of hydrogen (uncompressed) is also possible. Metal hydride canisters are commercially available, but have low hydrogen storage per weight. More hydrogen-rich solutions—such as alane[vii] or hydrogen made from aluminum in water—are available, but these systems are less mature, more expensive, and have less energy than compressed hydrogen.

iii JP-8 stands for Jet Propellant 8. It is a jet fuel specified and widely used by the US military.

iv Technology designed to harvest dynamic energy from the heel-strike phase of walking, convert it to electrical energy, and store the electrical energy in a battery.

v A Stirling engine is a heat engine vastly different from the combustion engine used in automobiles. It is based on the cyclic compression of a fixed amount of air or other gas (the working fluid) at different temperatures, such that there is a conversion of heat energy to mechanical energy.

vi PEM is also known as proton-exchange membrane.

vii Alane, also known as alumane, is aluminum hydride, an inorganic compound with the chemical formula AlH_3.

TABLE 1. SPECIFIC ENERGY AND ENERGY DENSITY OF 20–50 WATT BATTERY AND FUEL-CELL SYSTEMS, AND DOE ENERGY TARGETS. FUEL-CELL SYSTEMS ASSUME 1200-WH MISSIONS.

	Systems (20–50 W)	Specific energy Wh/kg	Energy density Wh/L	Notes
Rechargeable batteries	Lead-acid battery	30–40	60–75	Well-established, high-power battery
	Li-ion—standard for soldier	170	274	Brentronics BB2590
	Conformal, wearable, rechargeable Li-ion battery	120	184	Palladium CWB-150
	US DOE vehicle battery goals	235	500	Target for system-level batteries[12]
Primary batteries	Primary battery—Li-CFx/MnO2	266	325	Eagle Picher—not rechargeable
Portable fuel cells	Direct methanol fuel cell	273	126	UltraCell XRT-25
	Direct methanol fuel cell	275	181	SFC Energy, Jenny 1200
	PEM fuel cell with 5000 psi H2	515	205	Estimated

The development of cost-effective, reliable power sources can cost in the billions of dollars once all the materials development, manufacturing, and systems integration is taken into account, so the US government will not likely be able to fund a technology alone; dual-use technology, with a broad commercial acceptance is ideal. A boon is the level of investment in battery technology from both commercially and publicly funded research and development. Significant funding for advanced battery development is currently in place through the Department of Energy's Vehicle Technology Office and a consortium of US auto manufacturers, the United States Advanced Battery Consortium (USABC).[13] They have provided performance targets for near-term (CY 2023) battery development for electric vehicles (EVs). This represents a significant investment by both commercially and publicly funded research and development, and it shows what performance targets may be commercially available in the near term. Developments made for the EV market represent a significant resource if they can be adequately adapted to the needs of the special operations forces (SOF) mission.Progress is also being made on managing the electric loads better, and new iPower software is being implemented to better match new technologies to existing power sources.[13] The recommendation still stands that the US SOF community must manage its power loads wisely and effectively[11] and not expect an advanced power/energy source to become available.

Backup Power and Remote Sensors

The specific energy and volume of batteries is essentially linear with sizing. Fuel cells become more compelling for longer missions because the weight and size of the fuel-cell power plant stays the same over time, with the requirement only to add more fuel. Diesel generators are state-of-the-art and used successfully; however, they are readily

heard, and the electric power is noisy or nonuniform and less ideal for electronics. Both methanol fuel cells and propane-fueled, solid oxide fuel cells scale favorably with size and as the mission endurance increases from 24 to 72 hours, as shown in Table 2. The fuel cells are still relatively expensive compared to batteries, and while commercial vendors exist, the required propane and methanol fuels are a specialty fuel for the DOD, complicating logistics.

TABLE 2. ESTIMATED SPECIFIC ENERGY OF 110- AND 275-W FUEL CELLS VERSUS BATTERIES FOR 24- AND 72-H MISSIONS COMPARED TO LITHIUM ION BATTERY.

	Rated power, Watts	24-h Specific energy, Wh/kg	72-h Specific energy, Wh/kg	Notes
Solid oxide fuel cell/ propane fuel	275	350	750	Ultraelectronics D300, limited cycle life
Direct methanol fuel cell	110	110	900	SFC EFOY 2400
Soldier Li-ion battery	100–275	170	170	Brentronics BB2590—Batteries can be added in series to increase power

Unmanned Aircraft Systems

Electric power has many advantages over combustion technologies for unmanned aircraft systems (UAS), as it is directly compatible with electronics. In addition, it has low electric noise, instant starting, decreased maintenance, reduced vibrations, and negligible thermal signatures.

Small toys, robotics, and air vehicles have proliferated with the introduction of lithium polymer (LiPo) batteries, which are a form of lithium-ion batteries with a gelled interior electrolyte. LiPo's tend to have less strict manufacturing than cells used for cell phones and computers but can be designed in very small sizes and with very high power. Drones,[viii] or quadcopters,[ix] are one technology that have particularly benefitted from LiPo batteries. The precise control of drones is enabled by electric power to the electric motors on each propeller, so that they can adapt dynamically with the wind and fatigue on the motors and keep the vehicle level.

Small quadcopters (or multicopters[x]) are now commonplace as the result of the confluence of advanced Li-ion batteries, electric motors, and small electric cameras and payloads. Sophisticated mapping can be carried out with drones that can be purchased for a few thousand dollars. Most notably, the DJI Phantom and other drones are affordable to consumers and are now being used for jobs ranging from wedding photography to electric power-line monitoring.[14] The batteries on these

viii In this case, drone refers to a remote-controlled, pilotless aircraft.

ix A quadcopter, also termed a quadrotor, is rotorcraft (e.g., "helicopter") that is lifted and propelled by four rotors.

x A multicopter is simply a rotorcraft with more than two rotors.

vehicles last on the order of 20 to 30 minutes,[15] making them inadequate for complex, over-the-horizon surveillance.

The endurance of commercial drones is expected to increase incrementally as new battery technology develops. While commercial drones might be considered too simplistic for advanced SOCOM missions, the SOCOM community should expect that their adversaries will be equipped with this technology for both surveillance and carrying out attacks. Even without longer endurance, the systems can still be made more lethal by grouping the systems together in swarms for more complex attacks and/or decoys. This threat will only grow by 2050 as the technology continues to develop with the shared commercial market.

As shown in Figure 3, hydrogen fuel cells have been demonstrated to increase drastically the endurance of small, tier 2 (15–50 pound) unmanned air vehicles with a two to eight times increase over Li-ion batteries. The Naval Research Laboratory has demonstrated 24-hour flights of 35-pound vehicles with hydrogen fuel cells[16] and envisions adding endurance with solar panels and autosoaring so that the vehicles can stay up for days at a time and serve as communication networks or provide persistent surveillance.[17]

Other countries are also actively pursuing hydrogen fuel cells for long-endurance small UAS. Such vehicles are likely to become a threat, as they are more frequently deployed.

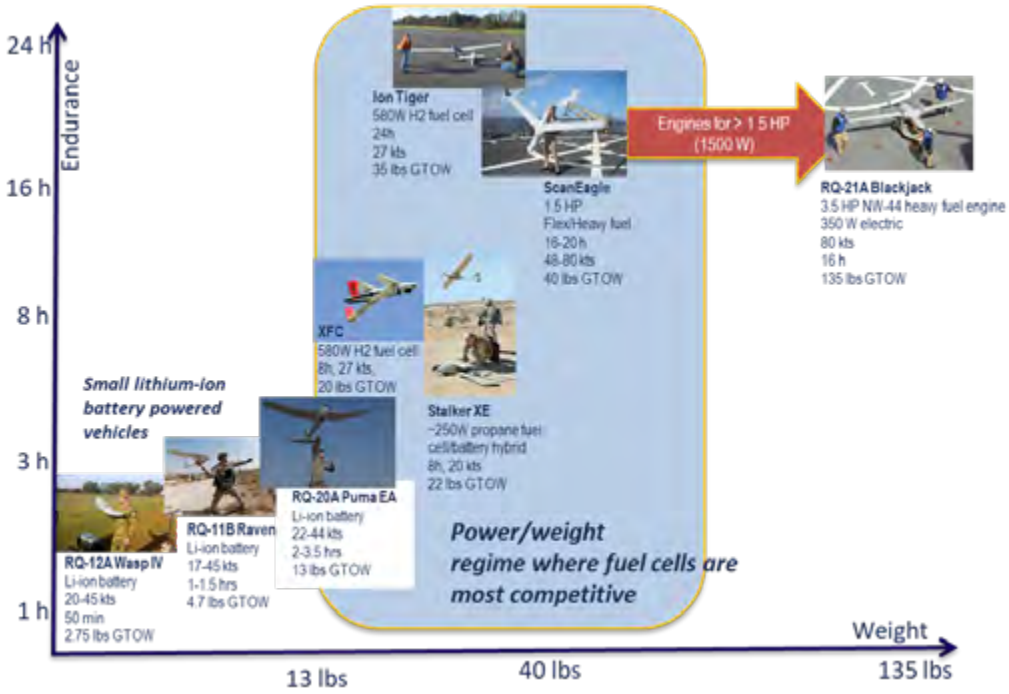


Figure 3. Tier 1 to tier 3 battery, fuel cell, and engine-powered UAS: comparison of propulsion/energy source, speed, endurance and gross takeoff weight (GTOW).

Other SOF Missions

Power requirements for exoskeletons, such as the Tactical Assault Light Operator Suit (TALOS) were assessed as too demanding for electrochemical power sources.18 However, new exoskeleton concepts are arising with reduced electronic loads and swappable Li-ion batteries.19 As researchers learn to decrease the power needed for the loads and battery and/or fuel-cell technology improves, exoskeletons are likely to become an aid on the battlefield.

The SOF community also envisions upgrading wet SEAL delivery systems to dry systems with longer ranges. The program to develop the Advanced SEAL Delivery System (ASDS) ended with a failure of the Li-ion batteries, resulting in fire and destruction to the vehicle.[20] This sobering accident effectively halted the use of advanced Li-ion batteries for the Navy. However, progress is being developed toward the adoption of new Li-ion commercial batteries with better safety pedigrees. There are also numerous programs to extend the endurance of unmanned undersea vehicles with Li-ion batteries.

Risks of Advanced Battery Sources

All stored energy carries an inherent risk, particularly if the stored energy is released uncontrollably. Currently, the largest forms of stored energy on the US electric grid are in the form of pumped hydroelectric reservoirs, where water is cycled between reservoirs at different elevations to store electrical energy. The uncontrolled stored energy in this case is potentially catastrophic, particularly for those living downstream from the dam. Like any form of stored energy, batteries carry this risk, but they also present some particular challenges. Looking at batteries in terms of the fire triangle,[xi] a fully charged battery holds fuel and oxidizer in intimate contact with one another. The only other places this is common is in high explosives and rocket fuel. While battery failure is certainly less catastrophic than the risk presented by an explosive, advanced electrochemical systems present an increasingly energy-dense component of many systems. Not only can a failure render the device inoperable, a severe enough incident can lead to damage beyond the power source and even injury to the user in extreme cases.

Li-ion cells present a modern case study of this problem. The specific concerns of Li-ion cells are well known. They are intolerant of abusive conditions, the active materials exhibit energetic breakdown, the inactive components (the electrolytes in particular) are flammable, and flammable gasses are often produced as part of the decomposition. Much the same could also be said of chemical fuels. Gasoline and other fuel fires happen routinely, yet the hazards inherent to the fuel are rarely seen as a reason to prohibit its use. The difference ultimately is familiarity with risks inherent to the technology. We have 100-plus years of dealing with liquid-fuel fires,

xi The fire, or combustion, triangle is a simple model for understanding the necessary ingredients of most fires: heat, fuel, and an oxidizing agent (usually oxygen or air).

and most organizations feel well equipped to handle liquid fuels safely and respond to any emergency situations surrounding them. Li-ion batteries, by comparison, have been in common use since their initial commercialization by Sony in 1991, and in most of that time have been relegated to single-cell, consumer electronic devices. Applications using more than three or four small cells have become common with the initial commercial success of electric vehicles, including the Tesla Roadster (2008) and the Nissan Leaf (2010).

The current solution to field high-energy-density batteries is to rely on sophisticated engineering of the battery pack, including both active and passive controls to mitigate a potential failure. These solutions add significantly to the size, weight, and cost of the system, effectively reducing the energy density of the underlying technology. Research and development is underway for advanced battery reliability, including more sophisticated diagnostics, cell-level improvements for better safety, and pack-level improvements.

While DOD has been slow to adopt new battery technologies because of safety concerns, potential adversaries may be less reticent. A higher tolerance for risk presents other countries with an opportunity to leapfrog our own technologies by adopting new power-source technologies where the safety concerns have not been fully addressed. Russia's stealthy use of Li-ion batteries in the Losharik submarines was revealed when a vehicle had a lethal fire at sea, possibly caused by a Li-ion battery fire.[21] The Japanese, Australians, Chinese, and others continue to develop submarines with Li-ion batteries.[22] Howaldtswerke-Deutsche Werft AG has built a fuel-cell-based submarine for years for the German, Italian, and other navies.[23] The adoption of advanced power sources by SOCOM will be critical to maintaining a technological advantage. This requires both a better understanding of the potential consequences so users can appropriately assess the risks of a technology and improved technologies to mitigate risks when they are deemed unacceptable.

Geopolitical Concerns for Manufacturing, Raw Materials, and New Electric Microgrids

Li-ion batteries were first invented in the United States, and the materials were discovered in the United States, Europe, and Japan. However, Sony led the first effort to commercialize and manufacture the technology.[24] The centers of manufacturing then moved to South Korea. China now dominates 73 percent of the manufacturing market as part of their strategic government efforts to become leaders in new energy technologies and electric vehicles, much like the path that China took for solar energy.[25] Meanwhile, the United States has 12 percent of the world's manufacturing capability for Li-ion batteries today; with no national plan for electrification, its worldwide share is forecast to drop.[26]

Up to 70 percent of the cost of Li-ion batteries is in their raw materials.[26] Lithium batteries require lithium for their anodes, plus an assortment of transition metal oxides for their cathode. The original cathodes contained cobalt (as lithium cobalt

oxide), but these have been replaced by higher-capacity and higher-voltage materials containing nickel and manganese. The majority of cobalt (69 percent) is mined in the Democratic Republic of the Congo; however, China holds 62 percent of the cobalt chemical supply, as shown in Figure 4. Nickel is mined primarily in Indonesia (26 percent) and the Philippines (17 percent),[27] where it is also causing significant environmental damage.[28]

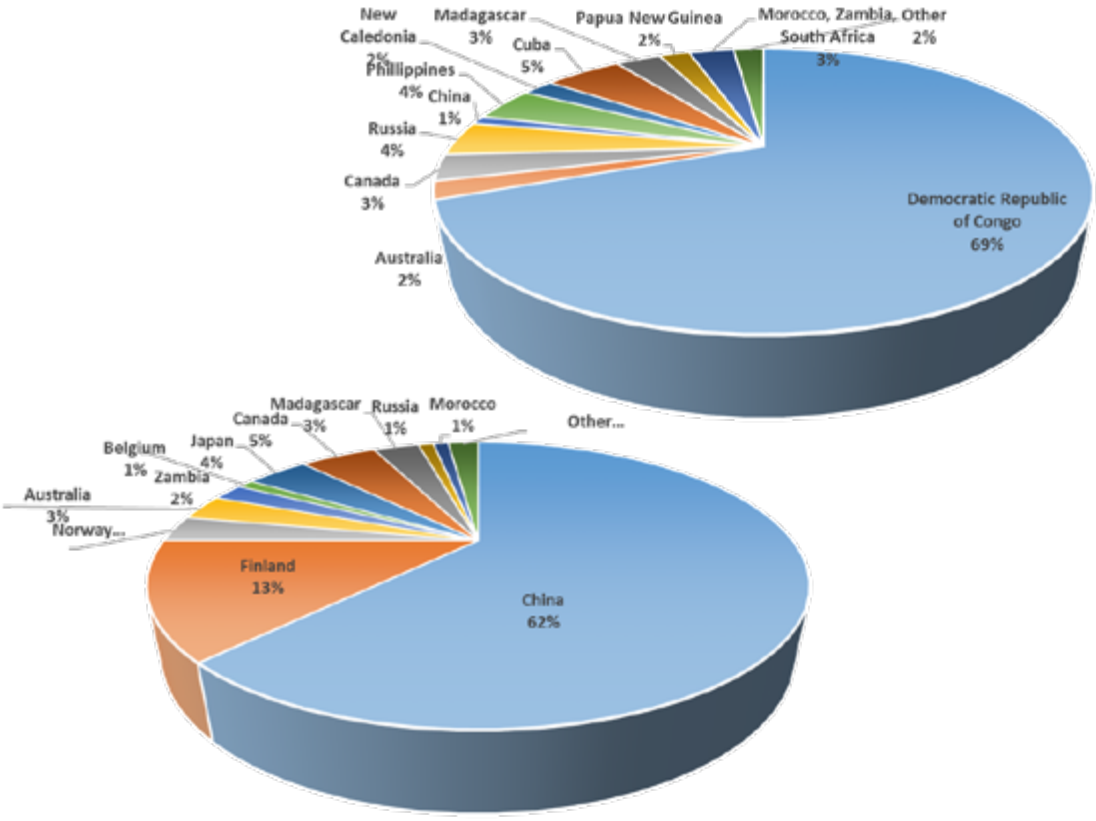


Figure 4. 2018 Distribution of cobalt as a raw material (top) and chemical (bottom), adapted from "Written Testimony of Simon Moores,"Benchmark Mineral Intelligence, February 5 2019.

Benchmark Mineral Intelligence, a company that tracks markets for Li-ion batteries, briefed the US Congress in 2019 to raise concerns about the United States losing its manufacturing and technological lead. The number of Li-ion battery "mega" or "giga" factories increased from 17 in 2017 to 70 in 2019, 46 of which are based in China, with only 5 currently planned for the United States.[29]

A RAND study raised similar concerns about the United States maintaining a ready manufacturing source of batteries for soldier-portable battery supply,[30] and the lack of supplies produced by the United States would likely impact SOCOM as well. One challenge for low-volume manufacturers for soldier-specific or custom batteries is having enough clout to affect the purchase of the materials needed for batteries, as

the giga-factories dominate purchasing, raising concern that it might not be possible to have a surge of battery production for soldiers in war time. The recent proposal of the US executive branch to purchase Greenland from Denmark could be seen as a means for more reliable access to the raw materials in batteries, fuel cells, and electric motors, as the ice shelves melt and allow new mining projects, such as the magmatic massive sulfide project for nickel-copper-platinum-cobalt.

SOCOM should also expect the use of batteries and fuel cells in microgrids, in combination with renewable energy (solar and wind), will provide power to thousands of communities worldwide that were previously without stable sources of power. Microgrids are being implemented now in Pacific island communities, where all power is generated by imported fuel from generators. As the technology costs continue to decrease, stable electric power will likely come to Africa, India, and developing-world communities. The availability of stable electric power from hybrid microgrids will undoubtedly improve living conditions for hundreds of millions of people worldwide. While peace typically follows improvements in living conditions and economic stability, in 2050, SOCOM might find some emerging communities with aggressive ambitions.

Summary

The world is presently experiencing a revolution in electric power sources, as Li-ion battery and fuel cells are becoming ubiquitous, reliable, and cost-effective for portable electronics, vehicles, tools, and homes. The technologies are expected to proliferate with the growing demand for electric vehicles and grids, and will likely affect SOCOM missions at both the technical and geopolitical levels. SOCOM must manage the deployment of electronic loads around realistic expectations of the capabilities of commercial power sources and work to integrate new technologies effectively into its missions. Even though battery and fuel-cell energy will not improve at the rate of microelectronics, the electrification of unmanned systems will unleash new, small technologies that can be used effectively both by and against the United States. New economies might emerge around microgrids in developing countries. SOCOM will also have to consider relationships with countries that hold the raw materials for batteries, fuel cells, and electric motors.

Acknowledgements

Karen Swider-Lyons is grateful to the Office of Naval Research for support for this research. Joshua Lamb thanks Sandia National Laboratories, a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the US Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. Yet-Ming Chiang acknowledges financial support from the US Department of Energy, Office of Science, Basic Energy Sciences, through the following awards—DE-SC0002633, DE-SC0012583, SC0002626—and the Joint Center for Energy Storage Research, an Energy Innovation Hub.

Endnotes

1 MacCalman, A., et al. 2019. "The Hyper-Enabled Operator." *Small Wars Journal*. June 7, 2019. https://smallwarsjournal.com/jrnl/art/hyper-enabled-operator; United States Department of Defense. 2018. Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge. 2018.

2 Scrosati, B. 2011. "History of Lithium Batteries." *J. Solid State Chemistry,* 15, 1623-1630 (2011).

3 Arthur D. Little. 2018. "Future of Batteries: Winner Takes All?" May 2018. https://www.adlittle.com/sites/default/files/viewpoints/adl_future_of_batteries-min.pdf.

4 Dahn, J. R. and Ehrlich, G. M. "Lithium-Ion Batteries" *Linden's Handbook of Batteries* 2011

5 European Commission. 2018. "Science for Environment Policy: Towards the Battery of the Future." Future Brief 20. September 2018. https://www.readkong.com/page/towards-the-battery-of-the-future-future-brief-8438036.

6 Schmitt, B. 2019. "Exclusive: Toyota Hydrogen Boss Explains How Fuel Cells Can Achieve Corolla Costs." *The Drive*. January 18, 2019. https://www.thedrive.com/tech/26050/exclusive-toyota-hydrogen-boss-explains-how-fuel-cells-can-achieve-corolla-costs.

7 Alaswad, A., et al. 2016. "Developments in Fuel Cell Technologies in The Transport Sector." Int. J. Hydrogen Energy, 41, 16499–16508 (October 2016). https://www.sciencedirect.com/science/article/abs/pii/S0360319915315810; D'Allegro, J. 2019. "Elon Musk Says the Tech Is 'Mind-Bogglingly Stupid,' But Hydrogen Cars May Yet Threaten Tesla." CNBC News. February 24, 2019.

8 Coren, M. J. 2017. "Amazon's Hydrogen-Powered Forklifts Are Its Latest Attempt to Beat Walmart in the E-Commerce War." *Quartz*. April 18, 2017. https://qz.com/961175/amazons-hydrogen-powered-forklifts-are-its-latest-attempt-to-beat-walmart-in-the-e-commerce-war/.

9 Hitch, J. 2019. "Engine Maker Acquisition Could Fuel Hydrogen Disruption." 2019. *Industry Week*. September 24, 2019. https://www.industryweek.com/technology-and-iiot/article/22028284/engine-maker-acquisition-could-fuel-hydrogen-disruption.

10 Gahleitner, G. 2013. "Hydrogen from Renewable Electricity: An international Review of Power-To-Gas Pilot Plants for Stationary Applications." *Int. J. Hydrogen Energy*, 28, 2039–2061 (February 2013). https://www.sciencedirect.com/science/article/abs/pii/S0360319912026481.

11 National Research Council (US) Committee of Soldier Power/Energy Systems. 2004. "Meeting the Energy Needs of Future Warriors." Washington (DC): National Academies Press (US). 2004. https://doi.org/10.17226/11065.

12 *Goals for Advanced High-Performance Batteries for Electric Vehicle Applications*. USCAR Energy Storage System Goals, 2019.

13 Stroman, Richard O., Eric Ledbetter, and Christopher Buesser. 2018. "iPOWER: Energy Analysis and Mission Planning Tools for Dismounted Soldiers." NRL Technical Report. NRI/MR/6110-18-9781. February 23, 2018.

14 González-Jorge, H., J. Martínez-Sánchez, and M. Bueno. 2017. "Unmanned Aerial Systems for Civil Applications: A Review," Drones, 1(1), 2(2017).

15 Phantom 4 Pro V2.0, specification sheet: https://www.dji.com/phantom-4-pro-v2/specs. Last accessed: 27 May 2020.

16 Swider-Lyons, K. E., et al. 2014. "Hydrogen Fuel Cells for Small Unmanned Air Vehicles." *ECS Transactions*, 64 (3) 963–972 (August 2014).

17 Navaltoday.com. 2018. "US Navy Adding Solar Power to Its Hybrid Tiger UAV." May 15, 2018.

18 Ainsworth, N., et al. 2016. "U.S. SOCOM Grand Challenge #3: NREL Technical Roadmap for a Man-Portable Power Supply System for TALOS." NREL National Renewable Energy Laboratory. NREL/TP-5D00-65985. June 2016. https://www.nrel.gov/docs/fy16osti/65985.pdf.

19 Naval Technology. 2019. "Sarcos Wins USSOCOM Contract to Supply XO Robotic Exoskeleton." March 20, 2019. https://www.naval-technology.com/news/sarcos-wins-ussocom-contract-to-supply-xo-robotic-exoskeleton/.

20 Cavas, C. P. 2008. "Fire Deals New Setback to Navy's Heralded Mini-Sub." *Honolulu Advertiser*. December 14, 2008.

21 Trevithick, J. 2019. "Russia's Fire-Damaged 'Losharik' Spy Submarine Heads for Repairs and New Details Emerge." *The Drive.* August 16, 2019. https://www.thedrive.com/the-war-zone/29448/russias-fire-damaged-losharik-spy-submarine-heads-for-repairs-as-new-details-emerge.

22 Yeo, M. 2020. "Japan Commissions its First Submarine Running on Lithium-Ion Batteries." *Defense News*. March 6, 2020. https://www.defensenews.com/global/asia-pacific/2020/03/06/japan-commissions-its-first-submarine-running-on-lithium-ion-batteries/.

23 Stattler, G. 2000. "Fuel Cells Going On-Board." *J. Power Sources,* 86, 61-67 (March 2000). https://www.sciencedirect.com/science/article/abs/pii/S0378775399004140.

24 Scrosati, B. 2011. "History of Lithium Batteries." *J. Solid State Chemistry*, 15, 1623-1630 (2011).

25 Rapier, Ian. 2019. "Why China is Dominating Lithium-Ion Battery Production." Forbes Magazine, Aug 4, 2019. https://www.forbes.com/sites/rrapier/2019/08/04/why-china-is-dominating-lithium-ion-battery-production/#13694c0b3786.

26 Schmitt, B. 2019. "Exclusive: Toyota Hydrogen Boss Explains How Fuel Cells Can Achieve Corolla Costs." *The Drive.* January 18, 2019. https://www.thedrive.com/tech/26050/exclusive-toyota-hydrogen-boss-explains-how-fuel-cells-can-achieve-corolla-costs.

27 Benchmark. 2019. "Written Testimony of Simon Moores, Managing Director, Benchmark Mineral Intelligence, to US Senate Committee on Energy and Natural Resources Committee." February 5, 2019. https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=9BAC3577-C7A4-4D6D-A5AA-33ACDB97C233.

28 Morse, Ian. 2019. "Mining Turned Indonesian Seas Red. The Drive for Greener Cars Could Herald a New Toxic Tide." Washington Post. November 20, 2019.

29 "Written Testimony of Simon Moores," Benchmark Mineral Intelligence, US Senate Committee on Energy and Natural Resources Committee, February 5, 2019.

30 Silberglitt, Richard, James T. Bartis, and Kyle Brady. 2014. "Soldier-Portable Battery Supply: Foreign Dependence and Policy Options." Rand Corporation. 2014. https://www.jstor.org/stable/10.7249/j.ctt6wq842.

SECTION 4

GLOBAL BUSINESS AND THE ROLE OF THE PRIVATE SECTOR IN NATIONAL SECURITY: IMPLICATIONS FOR SOF

CHAPTER 19

Cryptocurrency: Will the Digitization of Currency Allow Malign Actors to Achieve Strategic Effects?

Sara Dudley

Your money is no good here—"THE" US dollar (USD)—literally.

As developed nations move deeper into life as cashless communities, the declining acceptance and use of fiat currency marks a critical evolution of society from physical cash to digital value transfers. What if rogue and revisionist nations could unite behind a digital currency that supplanted the USD? Could they establish a secondary monetary system that avoids the international sanctions and anti-money-laundering protocols in the international financial systems to modulate bad behavior? Venezuelan, Russian, Iranian, and North Korean pursuits of just this sort of cryptocurrency alternatives give credibility to this concept. The potential next major world war might not be on a traditional battlefield but between financial systems. Corrupt and criminal networks are no longer the only communities finding ways to obfuscate their financial flows from the policing bodies protecting the international commercial banking system—nation-states have arrived in earnest.

The complement of emerging cryptocurrency technologies is poised to provide a backbone strong enough to threaten US security and international stability. As the epitome of disruptive technology, cryptocurrency may subvert the USD's coercive economic power, replacing or usurping the USD as the world's single preferred market currency. The actualization of this possibility would represent a revolutionary change in US national power. With the increasing viability of secure and pseudo-anonymous cryptocurrency blockchain transactions and direct peer-to-peer (P2P) payment systems gaining support, substantial global investment incentives are pushing development in the fintech market space. Increases in the technology's ease of use, security, and emphasis on enhanced privacy add momentum to surge up the Rogers innovation adoption curve.[1]

The final question to answer is not *if* this technology will upset the infrastructure of the international financial system dominated by World War II–winning allies, but when?

Given the nascent nature of this field, this chapter will cover the following thought exercises:

- General understanding of the technology and effect on the concept of "money."
- Current security concerns (enemy focused).
- Adoption potential (strategic latency).
- How special operations forces (SOF) can best capitalize (friendly focused).

This chapter is a near-term assessment of adversaries' ability to utilize the foundational properties of crytocurrency to function with impunity and strategic effects. This technological leap opens gaps and seams and causes regulatory lags, the exact gray space in which illicit actors thrive inside the global financial markets. In international economic and financial circles, the USD represents the epitome of power. Effects born from illicit-actor adaptation of cryptocurrency, intended to alter this balance of power, stand to be revolutionary in a manner potentially unimaginable to the Western world. As such, temporary disruption should not be a consideration. This technological genie will not retreat into the lamp. It warrants a review of the basic concepts and dynamics of money, implications to national security, and any conclusions and ideas on how best to position SOF in the security posture of the future.

"Tell Me Again Why I Should Be Concerned About This Flash-in-the-Pan 'Cryptocurrency' Thing?"

> *"Everything you don't know about money combined with everything you don't know about computers."*
>
> ***—John Oliver[2]***

What is a cryptocurrency? In generalconversations with average Americans and most Western populations, mentioning the word *cryptocurrency* divides a crowd instantaneously. Among glazed-over looks; volunteers offering knowledge and throwing out tertiarily related buzz words like "volatility," "criminals," "blockchain," and "dark web"; and finally some people engaging in a dialogue of interest that most often leads to questions on the soundness of cryptocurrency as an investment, a basic knowledge has not taken root. No one in the mix mentions the underlying concept being a fundamental change in the fabric of societies, that being money, which is a means to relay value between individuals in a trusted transaction.

The term *money* garners many definitions. Understanding the concepts of money and value transfer systems within societies relates to the intrinsic value that SOF bring to the broader strategic security picture. SOF forces offer individuals versed in international cultural context, linguistic expertise, and direct integration and understanding of the societies in which we partner. Considered neutral and the most secular force in society, money must be understood in the context of specific communities. Economists generally boil down the concept of money to three functions: providing a medium of exchange, a unit of accounting, and a store of value.[3] All three of these traditional functions resolve to or are supported internationally through banks. Under the current international construct, banks circulate the currency, hold the ledgers of account, and store the money. Cryptocurrency technology breaks the need for banks to provide the function as trusted brokers. Because banks have the centralized power to control the monetary system, governments focus on regulating and protecting the financial system at the three critical primary nodes

of the overarching system. Of particular note, the US Bank Secrecy Act, Executive Order 13224, the Financial Action Task Force (FATF) Forty recommendations for Anti-Money Laundering and Countering the Financing of Terror (2012), and UN Resolution 2462 (2019) focus on protecting the international financial system while encouraging individual nations to target specific illicit actors criminally. The focus of the international cooperation resides in protecting money transfers within the global financial system. To accomplish this task, a secondary positive effect results via the need to disrupt illicit-actor use.

How did banks become the primary nodes of all currency in the twenty-first century? In the evolution of money, when shells and stones replaced barter, when paper replaced precious metals and coins, and, finally, when paper lost the battle to plastic, some entity needed to provide the trust between parties. Each of these currency manifestations resulted arguably from demands to stretch across increasing distances, be it physical (for trade) or technological (to keep pace with the information age and the dawn of the internet). These transitions resulted in greater ease of use but, subsequently, a more significant trust relationship between the two parties in the exchange. Barter items had intrinsic value to both individuals but often not in a precise relational scale. Shells and stones translated to some scarcity or labor required for possession. Moving from precious metals and coins marked the transition from scarcity in materials to scarcity in circulation, given governmental management of paper bills. All the while, one certainty remained: record-keeping of these assets existed on ledgers. Fiat currency, the USD specifically, after the breakdown of the Bretton Woods gold standard, gave way to a pure trust of the US government backing the USD to support its continued use as the world's market currency and the basis of the petrodollar.[4] With the USD as the world market currency, US banks became the centralized ledger holders for the world. With such circumstances comes immense responsibility and consolidated power in US financial institutions.

Centralized Power at the Banks

> *"Power tends to corrupt, and absolute power corrupts absolutely"*
>
> ***—Lord Acton[5]***

In 1999, Paul Krugman, the Nobel Prize–winning economist, stated, "inadequately regulated financial institutions, an extensive moral-hazard problem, and euphoric market expectation" foreshadowed the return of Depression economics.[6] In 2008, President George W. Bush signed a $700 billion bailout for the banking industry, which held mortgage-backed securities.[7] The effects of the subprime mortgage meltdown in US banks rippled internationally, generating a global financial crisis. The trusted agent ledger holders at the US banks became rightfully vilified and suspect.

The general public became disillusioned with corporate greed and massive bailouts and considered banks guilty of excessive risk and profiteering within the US and

world markets. In response, Satoshi Nakamoto introduced the algorithms underlying a cryptographic blockchain to support Bitcoin, a P2P decentralized ledger system that imbued trust via mathematical computation, not banks. On January 3, 2009, the Bitcoin genesis block emerged with a "text" portion that read "The Times 03/January/2009 Chancellor on brink of second bailout for banks."[8] Understanding the context from which cryptocurrency evolved is paramount to seeing the future. Removing banks as the trusted ledger holders encapsulate the pure essence of origin for the first viable cryptocurrency: Bitcoin. Societies around the world must now reconcile this next-generation financial-ledger technology. Perhaps a brief quote from Satoshi Nakamoto's original email to a cryptography mailing list best describes the utopian vision and disruptive potential of this technology:

> *Bitcoin: A Peer-to-Peer Electronic Cash System:*
>
> *Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.*[9]

Are US Adversaries Interested in Cryptocurrency?

> *"Power over a man's subsistence is power over his will."*
>
> ***—Alexander Hamilton***[10]

I'll take your sanctions and raise you—I don't need your USD. As noted previously, since the end of the Cold War, when nations worldwide began to march to the drumbeat of globalization and doubled down on the USD as the world's market reserve currency, the economic and financial infrastructure of the United States surged. Friedrich Nietzsche's definition that "money is a crowbar of power" best describes how this situation progressed.[11] With power consolidated in the US financial and market systems, these USD ledger holders emerged as the main controllers in the system. International sanctions, Specially Designated Nationals (SDN) and Blocked Person Lists, and Office of Foreign Asset Controls (OFAC) penalties disrupt illicit actors' ability to move money based on monitoring these ledgers. Adversaries benefit by finding a way to operate unhindered by US banking-system sanctions and regulations.

Cryptocurrencies allow for a ledger system outside the aforementioned traditional international financial markets.Computer algorithms tasked with running code to establish and validate the trust relationship between private parties wishing to transfer value replace the need for banks as trusted intermediaries. These open, decentralized ledgers also generate pseudoanonymity up to the point that

correlations can be made between persons and public addresses. Secondarily, categorization must occur to determine the strategic risks among differing types of cryptocurrency. The three main types range from 1) commonly adopted cryptocurrencies operating in open-source solutions with fully transparent public blockchains, 2) secrecy focused cryptocurrencies, and 3) most problematically, closed blockchain cryptocurrencies at a nation-state level. This array of currency types parallels the security population mission sets in which SOF must engage: open foreign internal defense partners, countering collective violent extremist and insurgent bad actors, and near-peer nation-state actors.

The broad-spectrum adversarial use of cryptocurrency to bypass US economic power warrants a brief threat analysis like that within the 2018 US Treasury National Terrorist Financing and Proliferation Financing Risk Assessments. These financial assessments use the national level FATF risk-assessment framework to outline the threat, vulnerability, consequence, and risk. The key to this new technology is to amplify the goodness while managing the risks.

- Threat: Cryptocurrencies have no centralized regulating authority since they are set up expressly to establish P2P trusted relationships that negate the need for a banking system. All current international efforts toward anti-money laundering and countering the financing of terror (AML/CFT) reside in the entry and exit points from the international banking system. All adversaries named in the US National Defense Strategy, from sanctioned nation-state actors to violent extremist organizations (VEOs), benefit from the ability to transmit value outside the USD and international regulatory bodies safeguarding the financial system.[i] Rogue states motivated to avoid USD can dedicate substantial investment in the advancement of privacy or secrecy coins, as well as pursuing their internal cryptocurrency and blockchain.
- Vulnerability populations: The highest expected cryptocurrency adoption rates will be in communities with the following demographics: internet connectivity, high remittance populations, corrupt or low governance, and high inflation in local currency.[12] These characteristics share some overlap with those for areas prone to crime, terror, and corrupt network exploitation.[ii] The increased international development of the new crime-terror nexus plagues these at-risk populations to an even greater extent when considering the availability of crytpocurrencies and technology exposure.[13] In the case of crime networks connected to developed nations, drug traffickers occupy the territories within other countries where the "state" has retreated or been forced out because

i Adversaries listed in the National Defense Strategy include China, Russia, North Korea, Iran, and terrorist organizations (i.e., VEOs).

ii The fundamentals on the interaction between crime, terror, and corruption networks are drawn from research and documentation of Louise Shelley *in Dirty Entanglements* (2014).

of poor or lacking governance. Illicit actors penetrating into these areas further exacerbate the downward spiral of the monetary situation. Populations in these areas have limited access to formal financial systems because of bank derisking because of potential exposure to those same sources of illicit funding and criminal activities. When people do not have access to broader financial markets, criminal and terror networks gain an advantage and can offer a "better than what you have" scenario to many populations. Criminal and illicit actors' increased use of cryptocurrency via the dark web portends their support of the technology. Given these scenarios, one might expect bad actors to teach and train these vulnerable populations to utilize cryptocurrency to obfuscate bad-actor financial transfers.

- Vulnerable adversaries: While concerned parties worry about the anonymity cryptocurrency provides to illicit actors, an immutable digital blockchain record also provides transparency. If law enforcement, banking, and intelligence officials have access to the decentralized ledger, they can trace criminal activity. Given that cryptocurrency emerged from a revolution against the power of the banks, observers ought to expect a continued libertarian basis for the advancement of increased privacy within transactions.[14] As technology continues to develop more complex ways to meet the anonymity demands of communities wishing to retain individual liberty, the ability to follow the transparent blockchain pathways to enforce regulation and law decreases. However, the potential for "good actors" to crowd out or marginalize illicit ones has promise. The legal actors in the cryptocurrency space, intent on maximizing the societal and economic benefits, have a vested interest to promote increased investment in technologies to help map, understand, and regulate the corresponding advancement of the anonymity technology of bad actors.
- Consequence: Potential of dual market systems of "Western vs. outcast" economies. The benefits of applying this technology for good must outweigh the strategic risk in developing a financial system that diverges from the the traditional international financial markets and infrastructure. International organizations concerned with the threat-finance space—like the FATF, the United Nations Security Council Resolutions (UNSCR), or the International Monetary Fund—do three things that help secure and stabilize nations. First, institutions provide information about what states are doing; such transparency helps countries cooperate and build trust among one another. Second, the promise of repeated interactions between known parties decreases the incentive to cheat or attack one another. Third, institutions provide a mechanism to arbitrate, sanction, or punish offender behavior. Pairing the US financial system at the center of international commerce with the value and role of the USD in the global economy, international financial institutions become a significant executor of US economic statecraft.

However, the power of global institutions to maintain norms of behavior, and of the US ability to employ economic power to influence the behavior of other actors, degrades significantly if another financial system operates in parallel or replaces the USD as the most influential standard of global currency.

- Risk: By increasing the potential wealth and reach of illicit-goods markets, cryptocurrency value-transfer platforms represent a new borderless and digital mechanism for bad actors to manipulate underlying populations. In countries where terror and criminal organizations continue to govern better than governments, the threats remain to national security within the counter violent extremist organizations (C-VEO) realm. SOF forces will be engaged in a never-ending battle against the "disease," never able to address the root cause of terrorism. As Marshall Billingslea noted in a statement to the UN Security Council on Preventing and Combating the Financing of Terrorism, "States must also address fundamental contextual issues that create environments conducive to terrorism and terrorist financing. Corruption, weak or ineffective governance, and lack of respect for the rule of law—these problems can lead to regional instability and render economies vulnerable to terrorist financing."[15] Cryptocurrency technology makes it easier for threat groups to sustain financing, which makes it harder for governments to interdict. This entrenches the relationship between populations and criminal or terror networks and makes it even more difficult for legitimate governments to address the sources of instability via foreign internal defense, counterinsurgency, or the introduction of general security assistance forces.

How Can Cryptocurrency Generate the Ability to Unseat the USD as the World's Market Currency?

The convergence of early interest from crime, corrupt, and terror networks with investment by rogue nation-state actors guarantees the advancement of technologies in this field.[16] As cryptocurrency becomes easier to both use and scale and internet connectivity becomes more widespread, the international economic order must adjust. Several new technologies possess the latent potential for bad actors to train underlying populations to move from the USD to digital payment systems. Transitional or "gateway" digital payment platforms within high-secrecy countries, anonymity-based or closed cryptocurrency blockchain development by nation-states, and alternative-purpose blockchain technologies all represent developmental technologies that stand to change USD economic power dynamics internationally.

"Gateway" Platforms within High-Secrecy Countries

Digital payment platforms display exponential growth and arguably represent a transitional mechanism to cryptocurrency use, requiring neither fiat currency nor credit cards to relay value at the point of sale. Examples in the United States include Venmo, Zelle, and PayPal. Most digital platforms still require linkage to a traditional

bank account or credit card to backstop the digital application. However, the secrecy level of the banking industry of each country comes into play for researching illicit activities or threat financing.

WeChat Pay and Alibaba Pay applications, which each have over a billion users, support over 90 percent of all payments within the largest cities in China.[17] Both these apps use quick-response (QR) codes to instantly transmit required currency-transaction information between buyer and seller, reducing costs and eliminating fees paid to banks with traditional credit card payments. Both of these applications run through the Chinese technology megacompanies, Tencent (Facebook equivalent) and Alibaba (Amazon equivalent), not banks.

Hosted out of Russia, WebMoney (WMZ) is another combined digital and bank composite universal-payment platform (utilizing secret keys) that claims to have 39 million users.[18] WebMoney supports an e-wallet with guarantor entities (all incorporated in high-secrecy financial safehaven areas) confirming eleven different possible purse types. Each purse can hold a different underlying asset: multiple types of fiat currencies, property, prepaid cards, gold, and two cryptocurrencies.

The international economic movement to digitize the transfer of value at the speed of the internet rides the wave of revolutions of information technology. Conversion to solely electronic or digital payments represents a departure from the stepwise improvements of traditional banking. Technological leaps of this nature tax the ability of monetary system regulations and legal bureaucracy to keep up. Meanwhile, it also conditions underlying populations to use digital solutions that creep away from financial institutions where the regulatory stopgaps occur.

Sanctioned Nations and Illicit-Actor Use

Both profit and participation in the world markets drive illicit actors' pursuit to decouple US banks and international sanctions policy, the watershed cryptocurrency event by sanctioned actors being the announcement by Venezuela that it would release the petro.The petro represents a state cryptocurrency backed theoretically by the nation's underlying oil reserves. In Venezuela, a population motivated to escape government controls and a government seeking to evade global sanctions collided to unite behind cryptocurrency. While the underlying population still prefers bitcoins to the petro, Venezuela records the second-highest P2P cryptocurrency trading volume, behind Russia, within the cryptocurrency trade platforms localbitcoin.com.[19] Evolving international and US regulations that hold formal cryptocurrency marketplaces to the same customer due-diligence rules as US financial institutions foment networking P2P platforms like localbitcoin and Paxful to support unregulated transactions.

Iran, Russia, and North Korea have initiated similar cryptocurrency pursuits both to avoid US and global sanctions and to allow for trade and international marketplace participation. Blockchain technology applied at the state level generates national security concerns, given the new pathways to operate entire economies outside the USD-dominated financial system. Therefore, these rogue regimes are prioritizing

blockchain technology as the keystone of their efforts to counter US financial power. While none of these efforts have manifested in a way that would challenge the USD yet, the petro should remain on the radar as a first mover.

In addition to individual illicit actors, crime, corrupt, and terror networks open additional latency to support criminal profiteering within the high-risk populations identified previously.[20] At 20 percent, Turkey tops the list of countries with the highest cryptocurrency adoption rates.[21] Turkey's proximity to two states rife with terror groups and one that functions as a known sponsor of terror illustrates the potential intersection of at-risk populations and illicit marketplaces. This Statista survey goes on to illuminate that five of the ten top countries with populations that have owned or used cryptocurrency are in Latin America (Brazil, Colombia, Argentina, Chile, and Mexico.)[22] In 2019, protests and outrage emerged in some of the same and surrounding Latin American states known historically to have economic malaise, corrupt governance, and inflationary issues with national currencies (e.g. Colombia, Bolivia, Venezuela, Ecuador, and Chile.)[23] The primary expectation is that populations in these nations are adopting cryptocurrency as an alternative to traditional banking out of necessity, unlike the speculative investment mindset of adopters in Western nations. However, one must also consider potential influences of the underlying drug-trade challenges in these same regions.

The pairing of bad-actor incentives and the underlying anonymity of cryptocurrencies has supported new capabilities to scramble the transparency built into open blockchains. Specific privacy coins along with applications that mix transactions together battle against companies developing computer software to map out and provide visualization of all blockchain transactions to governing and regulatory bodies. The use of "The Onion Router" (Tor) to enter the dark web provides the final touch to obfuscating cryptocurrency transaction history. Tor answers the demand signal for anonymity coming from both legitimate and illegitimate actors.

Alternative-Purpose Blockchains

As the naming convention implies, cryptocurrency has more potential than simply as "currency." The underlying private-key-public-key blockchain technology supporting cryptocurrency as a store of value can support anything requiring a trust/validation relationship between exchanging parties. Specialized crypto coins already compete to distinguish themselves in the marketplace via uses specific to this revolutionary concept of decentralized computer applications (dApps.) Unleashed by cryptographic concepts underpining Bitcoin, more open-source, decentralized public ledgers—with networked computers incentivized to validate unique algorithmic blockchain—developed. Additional currencies, encrypted communications, smart contracts, digital-identity management, games, and token exchanges represent just a few primary dApp capabilities.

The dApps technology negates the need for centralized trust and control from banks, marketing agencies, communications companies, and repressive governments—all brokers in this regard. As of 2020, the primary blockchains that

allow for dApp capability are Ethereum, EOS, and Tron. Moving into the future, these cryptocurrency hybrid options offfer the advantage of the speed and scalability of the underlying consensus algorithm that participating computers solve.

SOF Can Provide an Engagement Counterbalance in At-Risk Adoption Populations

> *"Grand strategy begins and ends with macroeconomics, and perhaps the single most important insight from the Cold War is that geopolitical success is a function of economic vitality."*
>
> ***—Hal Brands[24]***

SOF have a long history of rapid adaptation, flexibility, and innovation. The purest essence of value that a SOF force brings to the national security apparatus is the combination of creative problem-solving, relationship building, and culturally informed assessment. SOF forces employing disruptive tactics offer commanders nonkinetic solutions and means to affect both the full spectrum of conflict and broad-ranging adversaries. Utilizing latent cryptocurrency capabilities in both a defensive and offensive way represents a viable disruptive, nonkinetic capability SOF might bring to the competitive gray space short of armed conflict.

"Disruptive" in the definition used by Clayton Christensen, represents an innovation that makes products and services both more accessible and more affordable to a larger volume of the population.[25] The disruptive potential of cryptocurrencies need not only manifest in a catastrophic light. The essence of blockchain, digital, and cryptocurrency assets represents undeniable positive societal benefits allowing the acceleration of access to global markets for billions of currently unbanked individuals. The cryptographic potential of this technology can be utilized positively as a counterbalance to bad actors. This level of transparency can inoculate populations from monetary ramifications of corrupt governance and as a defense against crime, corrupt, and terror influences.

The SOF-value proposition to influence positively a large volume of the population in these at-risk areas would manifest via partner-nation training events and long-standing military-to-military relationships. In place of utilizing Western-centric payment mechanisms, often based in USD, SOF forces should engage in preexisting local digital payment platforms or cryptocurrency payments or present at-risk populations access to a specialized dApp system developed based on answering communal needs. Promoted by economist Bernard Lietaer, new cryptocurrency technologies offer communities an efficient complementary mechanism in which to retreat from the scarcity models generated by national fiat currency systems dictated by monetary policy.[26] Cities around the world are testing this type of technology to create complementary "civic or city" currencies that support local economic development, societal cohesion, and active participation in the sustainability of local communities.

Following intergovernmental and nongovernmental organization coordination, initiation of this sort of economic stabilization dApp could support a community or cooperation coin. Distribution would occur via traditional leaflets based on the technological infrastructure of the mobile phones in the area. The more developed phone *coverage* areas could incorporate the addition of a "smart chip" on the pamphlets. Current testing of these smart chips within US Army SOF utilizes these programmable near-field communications (NFC) technology tags to support the direction of recipients to real-time information on a website. These small sticker tags could support everything from directing populations to websites explaining the use and architecture of community-specific coins to containing an encrypted currency. Less developed areas not in possession of smartphones with NFC technology could use a QR-code-based system to scan and load with coins.

Using existing digital payment platforms, expanding cryptocurrency in areas of adoption, and introducing community cooperation currencies would allow for the signature reduction of both our forces and partner forces. By promoting open-source cryptocurrency technology, we can generate an offense way to utilize this technology and support culturally appropriate funding solutions. SOF forces could use software capabilities offered by multiple private companies to map the complete use of digital currencies through these open blockchain constructs, following exactly where payments ultimately land. Instead of fearing this technology, accepting and embracing it provides defense and offense against the those who use the USD to warp local markets, generate perverse unsustainable economics, or support corrupt kleptocratic governance temptations to abscond with payments.

At the End of the Day . . . Give Me the "So What"?

> *"Lack of money is the root of all evil."*
>
> ***—George Bernard Shaw***[27]

In the hands of adversaries from nation-states to VEOs, does cryptocurrency make the United States vulnerable to strategic effects? And if the strategic results are legitimate and likely to advance with this technology, what should be done?

US adversaries of varying skill and capacity have indeed employed hybrid, disruptive, and catastrophic capabilities to undermine the instruments of US national power. These attempts have been mainly to affect the US comparative advantage in the financial and economic marketplace. Cryptocurrency in the technological arsenal opens unimaginable consequences should adversaries use it successfully to unseat the USD as the world's market currency. Countering the new ways that bad actors across the spectrum fund and support their maligned activities must be addressed.

The juggernaut of the DOD-military hierarchy and organization now hum the tune of large-scale combat and multidomain operation, retreating to the familiarity of past formations primarily equipped for combat operations with advanced material solutions

and deterrence. Joint Publication 1-02 defines irregular warfare as "a violent struggle among state and nonstate actors for legitimacy and influence over the relevant populations."[28] The overhauls in modernization for SOF ought to favor these indirect and asymmetric approaches to erode the power, will, and influence of this broadening scope of adversaries.

Monitoring the cryptocurrency adoption rates, actively participating in these markets, and watching the creative ways that bad actors modify their financing will only become more important as the safeguards in the banking systems are averted. In concert with the interagency, SOF can drive good-actor behavior. Full support of open-source cryptocurrency adoption within at-risk communities would silhouette and crowd out bad-actor use. Harnessing this technology to address underlying causes of illicit-actor penetration into vulnerable communities might finally allow SOF forces the ability not only to fight symptoms of bad acting and terror through direct action but also to employ the will of the underlying populations effectively to effect influence on their governance.

Bibliography

Antonopolous, Andreas. *The Internet of Money: Volume One*. 2016. Lexington, KY: Merkle Bloom. https://TheInternetOfMoney.org.

Antonopolous, Andreas. *The Internet of Money: Volume Two*. 2017. Middletown, DE: Merkle Bloom. https://TheInternetOfMoney.org.

Demirgüç-Kunt, Asli, et al. 2018. *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*. Washington, DC: World Bank. http://documents.worldbank.org/curated/en/332881525873182837/The-Global-Findex-Database-2017-Measuring-Financial-Inclusion-and-the-Fintech-Revolution.

Ehrlich, Steven. "A Crypto Arab Spring?" *Forbes*. November 6, 2019. https://www.forbes.com/sites/stevenehrlich/2019/11/06/a-crypto-arab-spring/#352817b24608 (accessed November 6, 2019).

Gilman, Nils, Jesse Goldhammer, and Steven Weber. 2013. "Deviant Globalization." In *Convergence: Illicit Networks and National Security in the Age of Globalization*. Michael Miklaucic and Jacqueline Brewer. pp. 8-13. Washington, DC: National Defense University Press.

Hayek, F. A. *Denationalisation of Money*. 1976. Westminster, London: The Institute of Economic Affairs. https://iea.org.uk/wp-content/uploads/2016/07/Denationalisation%20of%20Money.pdf.

Lietnaer, Bernard, and Jacqui Dunne. *Rethinking Money*. 2013. San Francisco, CA: Berrett-Koehler Publishers.

Lnidholm, Danielle, and Celina Realuyo. 2013. "Threat Finance: A Critical Enabler for Illicit Networks." In *Convergence: Illicit Networks and National Security in the Age of Globalization.* Michael Miklaucic and Jacqueline Brewer. pp. 111-130. Washington, DC: National Defense University Press.

Noveck, Beth. "More than a Coin: The Rise of Civic Cryptocurrency." *Forbes*. March 27, 2018. https://www.forbes.com/sites/bethsimonenoveck/2018/03/27/more-than-a-coin-the-rise-of-civic-cryptocurrency/#94aaf516b685 (accessed November 6, 2019).

Popper, Nathaniel. "Terrorists Turn to Bitcoin for Funding, and They're Learning Fast." *New York Times*. August 18, 2019. https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html (accessed November 5, 2019).

"**Record High Remittances Sent Globally 2018.**" April 9, 2019. Washington, DC: World Bank. https://www.worldbank.org/en/news/press-release/2019/04/08/record-high-remittances-sent-globally-in-2018.print

Rogers, Everitt. *Diffusion of Innovations*. 2003. New York: The Free Press.

Savell, Stephanie, and 5W Infographics. "This Map Shows Where in the World the US Military Is Combatting Terrorism." *Smithsonian Magazine*. January 2019. https://www.smithsonianmag.com/history/map-shows-places-world-where-us-military-operates-180970997/ (accessed October 30, 2019).

Shelley, Louise. *Dirty Entanglements*.2014. New York: Cambridge University Press.

Vigna, Paul, and Michael J. Casey. *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. 2015. New York: St. Martin's Press.

Endnotes

1 Rogers, E. *The Diffusion of Innovations*. Fifth Edition. The Free Press, New York: NY. 2003.

2 March 11, 2018 episode of "Last Week Tonight," talk show host John Oliver, https://www.youtube.com/watch?v=g6iDZspbRMg&feature=youtu.be.

3 Economic Education at the St. Louis Fed. "Episode 9: The Functions of Money," Volume 1, Episode 9 Economic Lowdown Podcast. https://www.stlouisfed.org/education/economic-lowdown-podcast-series/episode-9-functions-of-money.

4 International Monetary Fund. "The End of the Bretton Woods System (1972-81)," About the IMF: History. https://www.imf.org/external/about/histend.htm.

5 Lord Acton. "Letter to Archbishop Mandell Creighton," April 5, 1887, https://history.hanover.edu/courses/excerpts/165acton.html.

6 Krugman, Paul. "The Return of Depression Economics and the Crisis of 2008; Financial Fiasco: How America's Infatuation with Homeownership and Easy Money Created the Economic Crisis," Foreign Affairs On-line, Nov/Dec 2009. https://www.foreignaffairs.com/reviews/capsule-review/2009-11-01/return-depression-economics-and-crisis-2008-financial-fiasco-how.

7 US Congress. Public Law 110-343: Emergency Economic Stabilization Act 2008. https://www.congress.gov/110/plaws/publ343/PLAW-110publ343.pdf.

8 The Genesis Block Newspaper. https://www.thetimes03jan2009.com/.

9 Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." May 24, 2009. https://bitcoin.org/bitcoin.pdf.

10 Hamilton, Alexander. Federalist Papers: No 79. McLean's Edition, New York, 1788. Archived Yale Law School. https://avalon.law.yale.edu/18th_century/fed79.asp.

11 Nietzsche, Friedrich, edited by Del Caro and Pippin. Thus Spoke Zarathustra. Cambridge University Press, Cambridge, NY. 2006. pg. 35. http://users.clas.ufl.edu/burt/LoserLit/zarathustra.pdf.

12 Sandner, Philipp. "The Impact of Crypto Currencies on Developing Countries. Medium On-line. January 21, 2019. http://explore-ip.com/2019_The-Impact-of-Crypto-Currencies-on-Developing-Countries.pdf;
Klumov, Gregory. "Why Internet Is a Prime Crypto-currency-Adoption Driver," Cointelegraph on-line, March 26, 2020. https://cointelegraph.com/news/why-internet-growth-is-a-prime-cryptocurrency-adoption-driver;
Huang, Roger. "Cryptocurrency Would Fix Money Transfer Markets If More People Were Familiar with It," Forbes On-line. November 21, 2019. https://www.forbes.com/sites/rogerhuang/2018/11/21/cryptocurrency-would-fix-money-transfer-markets-if-more-people-were-familiar-with-it/#1155e3a39a65;
Redman, Jamie. "Countries Suffering from Rapid Inflation Show Significant Demand for Cryptos," Bitcoin.com, May 28, 2019. https://news.bitcoin.com/countries-suffering-from-rapid-inflation-show-significant-demand-for-cryptos/.

13 Basra, Rajan and Peter Neumann and Claudia Brunner. "Criminal Pasts, Terrorist Futures: European Jihadist and the New Crime-Terror Nexus," international Center for the Study of Radicalization and Political Violence (ICSR), Kings College, London, UK, 2016.

14 King, Georgia. "The Venn Diagram Between Libertarians and Crypto Bros Is So Close It's Basically a Circle," Quartz On-line. May 23, 2018. https://qz.com/1284178/almost-half-of-cryptocurrency-and-bitcoin-bros-identify-as-libertarian/.

15 Billingslea, Marshall. "UN Security Council: Preventing and Combating the Financing of Terrorism," Remarks to United Nations Security Council New York, March 28, 2019.

16 Malik, Nakita. "How Criminals and Terrorists Use Cryptocurrency: And How to Stop It," Forbes On-line, August 31, 2018. https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#21ac191b3990;
Dudley, Sara, et al. "Evasive Maneuvers: how malign actors leverage cryptocurrency," Joint Forces Quarterly 92, January 2019. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_58-64_Dudley-et-al.pdf.

17 Klein, Aaron. "Is China's New Payment System the Future?" Brookings Institute, June 2019. https://www.brookings.edu/wp-content/uploads/2019/05/ES_20190617_Klein_ChinaPayments.pdf.

18 Webmoney. On-line website for service. https://www.wmtransfer.com/eng/information/short/index.shtml.

19 Haig, Samuel. "P2P Markets: Russian Local bitcoins Trade Outpaces Venezuela," Bitcoin.com, March 8, 2019, https://news.bitcoin.com/russian-localbitcoins-trade-outpaces-venezuela/.

20 Shelley, Louise. "Terrorism and International Crime–Corruption as the Enabler," Transparency International, 54th Munich Security Conference in February 2018. https://www.transparency.de/fileadmin/Redaktion/Publikationen/2018/Terrorism_and_International_Crime_Corruption_as_the_Enabler_2018_WEB.pdf.

21 Buchholtz, Katharina. "How Common Is Crypto?" Statista, June 12, 2019. https://www.statista.com/chart/18345/crypto-currency-adoption/.

22 Buchholtz, "How Common Is Crypto?" 2019.

23 Ferreira, Francisco, and Marta Schoch. "Inequality and Social Unrest in Latin America: The Tocqueville Paradox Revisited," World Bank Blogs, February 24, 2020. https://blogs.worldbank.org/developmenttalk/inequality-and-social-unrest-latin-america-tocqueville-paradox-revisited.

24 Brands, Hal. "America's Grand Strategy: Lessons from the Cold War," Foreign Policy Research Institute, August 26, 2015. https://www.fpri.org/article/2015/08/american-grand-strategy-lessons-from-the-cold-war/.

25 Christensen, Clayton and Michael Raynor and Rory McDonald. "What is Disruptive Innovation?" Harvard Business Review, December 2015. https://hbr.org/2015/12/what-is-disruptive-innovation.

26 Lietaer, Bernard and Jacqui Dunne. Re-thinking Money: How New Currencies Turn Scarcity into Prosperity. Berrett-Koehler, San Francisco: CA, 2013.

27 Wei, Jessica. "Lack of Money Is the Root of All Evil," DUE on-line, February 20, 2016. https://due.com/blog/lack-of-money-is-the-root-of-all-evil-george-bernard-shaw/.

28 Joint Chiefs of Staff. Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms. November 8, 2010: amended through February 15, 2016. https://fas.org/irp/doddir/dod/jp1_02.pdf.

CHAPTER 20

Blockchain and the Battlefield

Girish Sreevatsan Nandakumar and Jon Cederquist

Hybrid warfare is the new norm. Economic competition—a key "gray zone" in hybrid warfare—plays a central role in today's great-power conflicts. Governments are increasingly aware of the potential threats posed by decentralized financial systems that can change global power dynamics. In the future, such decentralized systems are likely play a major role because of the ever-increasing erosion of trust in governments and other centralized systems. Countries across the world are striving to cut down on their use of cash to have more efficient monetary systems. Such "cashless societies"[1] of the future, possibly powered by companies such as Facebook (Libra) and Alibaba (Alipay), are likely to involve new digital cryptocurrencies, some of which will not be issued by nation-states or regulated in the same way central banks and governments control monetary systems today.

Cryptocurrency is a digital or virtual currency that uses electronic cryptography for security, which makes it difficult to counterfeit.[2] One of the defining features of a cryptocurrency is that it is a peer-to-peer system that cuts out the middleperson necessary for a transaction. Such "decentralization" is made possible through the blockchain technology—a distributed system of secure and immutable online ledgers.[3] Since cryptocurrencies are not issued by any central authority, they are theoretically shielded from government interference or manipulation.[4] These decentralized, denationalized systems have captured the trust of small groups of people across the world. For example, Bitcoin rose in prominence during the 2009 financial crisis because it was seen as an alternative to the highly centralized systems that had failed. Since the introduction of the first cryptocurrency, Bitcoin (BTC), in 2009, several decentralized cryptocurrencies have been released.

With the help of blockchain technology, two strangers can safely and directly engage in business transactions without the need for any intermediaries, thereby making lawyers, bankers, brokers, and governments potentially irrelevant. Blockchain is a system that enables trust through its design—the system confirms the identity of participants, validates transactions, and ensures that everyone plays by the same rules. This means that all types of goods, services, and information can be traded through such systems, which opens the doors for a wide range of possibilities and problems because anyone can participate in the system.[i] *Blockchain* has also become a buzzword for several sectors—from diamonds to recycling[5]—and there has been a staggering amount of research and funding for applications of this technology.[6]

If large decentralized financial systems are widely adopted for both storage of value and medium of exchange, the international monetary system, which has been

i The statement is true in the case of nonpermissioned blockchains such as Bitcoin but not true in the permissioned blockchains.

dominated for many decades by national currencies—primarily the US dollar—will be disrupted. Such a disruption could unseat the US dollar's prominence and might strengthen a rival. Blockchain-based systems can also provide smartcontracts and other services that could create independently operating legal structures parallel to existing national bureaucracies.

A deep dive into the history of the international monetary system and the evolution of national and territorial currencies would at least give some benefit of doubt to the Austrian School of Economics' perspective. This school posits current governmental monopolies on the creation and distribution of money came about primarily as a result of politics, not as sound economic practice. However, there is no way to prove whether a free-market approach to currencies would be a good idea because "the only valid test of the natural monopoly argument is to abolish all barriers to entry and to admit free currency competition from private issuers on equal terms,"[7] which no national government has allowed. In today's world, where private companies are sometimes more powerful than governments,[8] private currencies owned and operated by nongovernmental entities may gain traction once regulatory agencies allow their circulation. Japan, for instance, allows Bitcoin as legal tender.[9] This pattern of domination by denationalized, decentralized systems may apply to other areas—such as businesses, marketplaces, and critical infrastructure—currenty monopolized by governments and other centralized private entities.

Future blockchain scenarios are both inspiring and terrifying. The battlefield could be impacted by some applications of the technology. For instance, once the technology matures and is integrated with other complementary technologies such as Internet of Things (IoT)—systems of interconnected computing devices, machines, and objects such as drones—a completely autonomous drone with the ability to identify and destroy a target for a bounty[ii] could pose new, hard-to-detect or -deter threats for special operations forces (SOF). On the bright side, even some existing applications of the technology might help the warfighter fight SOF missions more effectively. Consider the usage of cryptocurrencies as a method of payment for local informants behind enemy lines during SOF missions. According to one former SOF operator, this may be more efficient than cash. In the future, there are likely to be more uses and threats.

This chapter discusses potential future scenarios involving blockchain technology and its applications that may occur by 2030. Our scenarios are based on current trends and have a central focus on how SOF operations may be impacted. We first provide a background on the blockchain technology, followed by potential positive and negative future scenarios. We then review more specific implications on the battlefield.

ii Which could be pseudonymously delivered through a blockchain-based smart contract and paid in cryptocurrency.

A Bit about Blockchain[iii]

The National Institute of Standards and Technology (NIST) defines a blockchain as "tamper-evident and tamper-resistant digital ledgers implemented in a distibuted fashion . . . and usually without a central authority."[10] Blockchain technology is the backbone of modern cryptocurrencies. Cryptocurrencies have been used as speculative investments,[11] instruments for money laundering,[12] and as a payment system to send and receive money in developing countries.[13] The technology is already being adopted by major corporations[14] and institutions[15] and is poised to have a major impact on global trade[16] if it gets adopted by businesses and financial institutions on a large scale. Because blockchain provides a distributed digital record that does not require trust or coordination between firms, it allows for secure, standardized transactions. Other main applications of this technology include digitized contracts, known as smart contracts, and records relevant to voting or health. Blockchain-based systems can also be used to maintain land records, voting records, medical records, and logistics. This will likely affect SOF environments because of the difficulties involved in adapting to these changes, as well as the second- and third-order effects these changes will inevitably bring.

Smart contracts are programmable contracts that carry the terms of the agreement between buyer and seller as lines of code on a blockchain network. NIST defines smart contracts as "software deployed on the blockchain and executed by computers running that blockchain." Smart contracts often have the advantage of being a part of the same network and system that executes payments through cryptocurrencies. In a world where denationalized blockchain-based financial systems are ubiquitous, smart contracts are likely to be widely adopted. Smart contracts might be able to provide insurance and other legal services, making these networks highly valuable.[17]

The real risk in such a future scenario is that these blockchain systems will not be as decentralized as advertised, especially if authoritarian governments are involved. We are already seeing some indications of this. China has reportedly tested the application of AI[18] and blockchain[19] in their internet courts. During the 2019 Forum on China Intellectual Property Protection, the president of Beijing Internet Court claimed that AI and blockchain are used to make legal rulings and have shown impressive results.[20] The Beijing Internet Court is the second of its kind in China and is part of the country's efforts to address internet-related disputes through an online court. In combination with China's social credit system, such applications of blockchain might further strengthen Beijing's authoritarian model by offering a rigid process that does not allow due process. Other authoritarian countries that buy hardware and software from China[21] will also be able to buy blockchain-based financial and legal services. This might give China unparalleled access to economic data from these countries. The rest of the chapter discusses potential future scenarios and potential implications in the battlefield.

iii Note: Because of its highly technical nature, we adapted this section heavily from the National Institute of Standards and Technology report "Blockchain Technology Overview." The report is available at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

What to Expect

According to the 2019 Gartner Hype Cycle, which highlights emerging technologies that will have a significant impact on society over the next five to ten years, blockchain technology is sliding into the "trough of disillusionment"—a phase where interest wanes as experiments and implementations fail to deliver.[22] The Hype Cycle notes most blockchain technologies are still five to ten years away from transformational impact. While stressing the need for a cautious approach to the hype surrounding the technology, Gartner analysts encourage businesses to embrace blockchain.

The Institute for the Future, a California-based think tank, suggests that blockchain technology will go through three distinct phases over the next decade: (1) Cryptocurrencies as an application, (2) distributed computing systems that include applications like smart contracts. (The institute posits such broadly decentralized, distributed global systems could potentially disrupt the status quo.)[23] (3) Objects such as the Internet of Things (IoT) are likely to be connected to blockchain networks. These interconnected entities may be capable of transferring data over the blockchain network autonomously.[24] The institute predicts IoT devices would also integrate with smart contracts to create crowdsourced infrastructures that could replace existing centralized alternatives. In the following sections, we discuss projected developments within the next decade in the context of special operations forces (SOF). We discuss current trends and potential future scenarios involving personas, businesses and services, marketplaces, infrastructure, and systems.

Personas

The internet has already drastically changed the way humans represent themselves. In a future where decentralized systems are the norm, identities will no longer be tied solely to traditional nation-states. Instead, blockchain-based "virtual nations"[25] could offer people a higher sense of belonging because these are niche groups formed around specific belief systems. These virtual nations are similar to existing social networks, but tend to be "permissioned" (i.e., closed and secured) and offer several other services, such as cryptocurrency payments and smart contracts. For example, "Bitnation," descibes itself as "the world's first Decentralised Borderless Voluntary Nation"[26] that offers to maintain vital records, identity, and other legal events using blockchain technology.

Such virtual nations are in their infancy and do not yet pose a threat to nation-states,[27] yet they might further exacerbate multipolarization in the world by enabling smaller groups of people to isolate. A deeply multipolar world could end up having little cohesion, making it easy to turn people against each other, especially when savvy bad actors make concerted efforts. For instance, consider the 2018 Toronto van attack, which was carried out by a member of the "incel" community—a specific, insular, self-radicalized community with roots in the anti-feminist 4chan culture.[28] Though such communities of "involuntarily celibate" people have existed for a long time, they are now much easier to radicalize online when they organize in echo chambers.[29]

During SOF missions, the ability to reach such online microcommunities behind enemy lines might enable online influence operations that weaken the enemy. Bitnation-style microcommunities of disgruntled citizens behind enemy lines might open up new sources of information that may enable SOF operations. A deeper understanding of such "virtual nations" is necessary in order to tap into such opportunities.

Businesses and Services

Individuals across the world are also increasingly adopting[30] denationalized cryptocurrencies, such as Bitcoin and Ethereum. The biggest problem with such cryptocurrencies is that financial transactions might not be easily detected by law enforcement authorities. Although not all cryptocurrencies are anonymous or pseudonymous, almost all cryptocurrencies make it difficult to trace transactions when necessary. This will affect the United States' ability to counter terrorism, transnational crimes, and other illegal activities. Another major issue will be the inability to impose sanctions on individuals and businesses identified as bad actors. Freezing their accounts will no longer be easy because of decentralized control. The use of Bitcoin has already provided North Korea opportunities to circumvent Western sanctions.[31] Information and services can be traded easily and anonymously through such blockchain-based networks, making it harder for regulatory agencies to prevent such bad actors.

Some "virtual nations" have been open and positive for the economy.[32] For instance, take Estonia's e-residency program that is advertised as "the new digital nation." This program enables digital entrepreneurs to start and manage a European Union–based company online, no matter where they live. While such programs might be positive for the economy, there are several negative side effects. If there are new competing services by other nation-states that are lenient, bad actors could use such services to move money and equipment around. On the bright side, the US might want to consider offering a similar program that sets the standards for other such programs. Such a digital "belt and road" program could be one way to counter China's Belt and Road Initiative (BRI), while ensuring that the US dollar's dominance and America's economic strength prevail.[33] Such an American "virtual nation" will also help recruit support from people across borders for SOF missions by opening new methods for gathering intel and as partners in cyber-enabled operations.

Marketplaces

Marketplaces created by poorly regulated virtual nations have the option to operate worldwide, making it difficult for nation-states to manage the aftereffects of such changes. It is easy to imagine the plethora of problems that would result from such a shift—weapons and other restricted substances being sold more freely, trading information and services that affect national security.

In a scenario where it is no longer dependent on the United States for economic growth, China might consider creating a supranational system that offers

cryptocurrency, smart contracts, and other services in the Eurasian region, similar to the euro in Europe. Such a system would be immune to US sanctions and would also consolidate economic activity within countries involved in the BRI. China will get to influence, if not control, this currency the way Germany dominated the euro for a long time. Such a scenario would pose a threat to the US dollar. Russia's growing diplomatic proximity to China makes such scenarios more likely because creating a new "Eurasian" bloc has been a goal for Russia.[34] In such a case, the new bloc that would emerge would be more difficult for US forces to operate in because of increased Chinese influence—both economically and militarily.

Infrastructure

One of the best uses of blockchain technology is in underdeveloped countries that do not have advanced systems for banking, land records, and medical records. Such countries may have the potential to leapfrog ahead by implementing more advanced systems than the rest of the world. While the costs would be enormous, so would the returns. China may see value in investing in such digital infrastructure because of the leverage it would provide in terms of data, access, and control. Another alternative would be for China to use its "debt trap" method to make such underdeveloped countries borrow from China. This will create a win-win situation for China: if the underdeveloped economies prosper, so will China. If they fail, China will benefit by seizing assets, such as strategically located ports, like it did in Sri Lanka in 2018.[35] China has used some of these assets for military activity. In such scenarios, China will be able to weaponize interdependence and extend its spheres of influence, affecting SOF readiness in those regions because of increased Chinese military activity in and around those regions.

Blockchain-based networks can also lead to changes in the way electricity is distributed[36] by empowering off-the-grid solar panels with blockchain-based payment systems, which could make traditional power grids less relevant. Such blockchain-based distributed systems might make it more difficult for SOF to disrupt power supply on a large scale during operations. Future SOF missions with the objective of liberating populations might go beyond digging wells, and could use decentralized blockchain systems to create energy independence along with an economic system that will promote stability. Such empowered communities can be turned into reliable allies.

Legal, Financial, and Administrative Systems

Failing economies sometimes adopt the US dollar as the national currency—a phenomenon referred to as "dollarization." However, recently, there have been cases of "cryptonization"—the adoption or creation of cryptocurrencies instead of adopting the US dollar.[37] If this trend grows, the US dollar's position as the world's de facto reserve and most sought-after currency will be in jeopardy.[38] Revisionist powers such as Russia and China, who have been trying to "dedollarize" the world economy,[39] will

be inclined to promote cryptocurrencies across the world. China will be in the best position to do this because Chinese companies—heavily influenced by the Chinese government—are among the most innovative companies in the blockchain sector.[40]

In fact, it may be easier for China to promote and enable private cryptocurrencies that compete with the US dollar than to compete directly using its national currency. Alipay's parent company, Ant Financial, is a world leader in fintech[41] and owns more than 10 percent of all blockchain-related patents.[42] This is reportedly the highest number of blockchain-related patents owned by any company, with IBM placing second. Similar to the case of Huawei, the United States invoked national security concerns to prevent Alipay from expanding within the United States,[43] but other countries, including the United Kingdom, have been lenient in controlling their infiltration.[44] Alipay has a stake or partnership with mobile payment companies across the world and can easily consolidate the global market in the future when consumers move toward alternative financial systems based on distrust in governments and banks.

If blockchain-based financial systems become ubiquitous, companies such as Ant Financial and WeChat will have both the technical capability[45] and the scale to become undisputed world leaders. Although they are private entities, they are heavily influenced by the Chinese government. In a scenario where such blockchain-based systems are the "operating systems" that provide financial services, smart contracts, land records, health records, and other services in several countries, the United States may lose its economic superiority and diplomatic reach, creating a power vaccum. SOF preparedness will also be affected because these countries will be under the Chinese sphere of influence, affecting the way operators use monetary incentives to gather intelligence on the ground during missions without being detected.

Potential Future Implications in Hybrid Warfare

Parallel governments

As discussed in the sections above, "virtual nations" that offer competing services to citizens may be empowered to create essentially a parallel government within existing nation-states. This might lead to weaker governments, which may in turn empower bad actors, especially in the more fragile parts of the world. Future SOF missions might require an in-depth understanding of how such campaigns will be carried out to prevent strategic surprises.

Virtual Nations

In a future scenario in which numerous virtual nations exist that imitate most of the core functions of nation-states—such as securing financial transactions, providing legal systems, and keeping records—violent fringe elements could organize more sophiticated attacks under the protective cover of cryptography, transferring money and sharing information anonymously among their global members. Future SOF

missions might require a better understanding of these specific threats in order to ensure readiness and success.

"Killer Apps"

Imagine a blockchain-based system that can transfer money pseudonymously, with identity-making efforts that use smart contracts to make the completion of the transaction contingent on certain events, such as the death of a particular person identified in a photograph. With the help of IoT devices, such as the fictional autonomous "slaughterbot,"[46]—a palm-sized, autonomous drone that uses facial recognition technology and onboard explosives to commit untraceable killings—a bounty placed anonymously on a blockchain system can theoretically lead to the elimination of the target and would be be hard to trace. Such a scenario is not too far-fetched, especially in a system that has a surveillance program similar to China's social credit system that uses millions of cameras for accurate face detection.[47] Clandestine SOF missions could become more difficult because of increased constraints and risk of exposure in places that implement such technologies.[iv] On the other hand, SOF missions could use such a "killer app" to eliminate terrorists.

Conclusion

A world where decentralized blockchain systems are mainstream might sound too radical to ever be true. But, only recently, a world where people would prefer to get into strangers' cars instead of taxis, and stay in strangers' houses instead of hotels were thought of as radical scenarios. Uber and Airbnb, respectively, normalized these practices by adapting available technologies and implementing them in the right way. While the international monetary system is definitely larger and more complex than the market inefficiencies Uber and Airbnb tackled, blockchain technology and its subsequent applications may find equilibriums that may not be as radical as the scenarios discussed in this chapter. However, even at such equilibriums, the status quo will have significantly changed, and this might affect the battlefield if the United States does not have the first-mover advantage, like it did with the internet.

The "hegemonic stability theory," which posits a strong hegemon is necessary for global stability, has been observed to be true in international monetary relations.[48] History suggests a well-functioning monetary system at the international level needs strong leadership by a nation or a group of nations that have vested interest in maintaining the system. This hegemon must provide a "lender of last resort" privilege, carry out economic transactions, and provide liquidity.[49] It has always been the dominant power of the day and the one with the mightiest economy and military. First, it was Great Britain, followed by the United States. Given the rise of China's and other fast-growing economies, it remains to be seen how an increasingly multipolar world will affect the international monetary system and how these changes will affect

iv For example, Ecuador is one of the countries that uses surveillance systems designed by China.

the future of decentralized systems and its applications. Gglobalization and increased interconnectivity may have set the stage for efficient, private cryptocurrencies and smart contracts that operate globally, which might create new spheres of influence that overlap national boundaries. In such scenarios, there will be increased complications for military planning, especially unconventional SOF missions.

Endnotes

1 Marria, Vishal. "What A Cashless Society Could Mean for The Future," 2018, https://www.forbes.com/sites/vishalmarria/2018/12/21/what-a-cashless-society-could-mean-for-the-future/#7f63f6232638
2 Frankenfield, Jake. "Crypocurrency," Investopedia, 2019, https://www.investopedia.com/terms/c/cryptocurrency.asp.
3 Sloane Brakeville, and Bhargav Perepa. "Blockchain Basics: Introduction to Distributed Ledgers," 2019. https://developer.ibm.com/technologies/blockchain/tutorials/cl-blockchain-basics-intro-bluemix-trs/.
4 Frankenfield, "Crypocurrency," 2019.
5 Teo, Candice. "Could Blockchain Help to Stem the Flow of Conflict Diamonds?" World Economic Forum, 2018, https://www.weforum.org/agenda/2018/06/diamonds-recycling-blockchain-technology-responsible-ethical-businesses/.
6 CB Insights, "Blockchain Trends in Review," 2019, https://www.cbinsights.com/research/report/blockchain-trends-opportunities/.
7 Vaubel, Roland. "The Government's Money Monopoly: Externalities or Natural Monopoly?" Kyklos 37, no. 1 (1984): 27-58.
8 Kuhner, Timothy K. "Citizens United as Neoliberal Jurisprudence: The Resurgence Of Economic Theory." *Va. J. Soc. Pol'y & L.* 18 (2010): 395.
9 Rooney, Kate. "Your Guide to Cryptocurrency Regulations around the World and Where They Are Headed," CNBC, 2018, https://www.cnbc.com/2018/03/27/a-complete-guide-to-cyprocurrency-regulations-around-the-world.html.
10 Yaga, Dylan, et al. "Blockchain Technology Overview," NISTIR 8202, 2018, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.
11 Adkisson, Jay. "The Cryptocurrency Paradox And Why Crypto Is Failing," Forbes, 2018, https://www.forbes.com/sites/jayadkisson/2018/11/28/the-cryptocurrency-paradox-and-why-crypto-is-failing/#598b8cf7c9d0.
12 Comtex. "The Effect of Cryptocurrency on Money Laundering," MarketWatch, 2019, https://www.marketwatch.com/press-release/the-effect-of-cryptocurrency-on-money-laundering-2019-07-15.
13 Rovero Coello, Emilio. "Are cryptocurrencies useful for remittances?," Forbes, 2020, https://coincenter.org/entry/are-cryptocurrencies-useful-for-remittances.
14 Del Castillo, Michael. "Blockchain 50: Billion Dollar Babies," Forbes, 2019, https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchain-50-billion-dollar-babies/#1d4d32957ccb.
15 Mulligan, Cathy. 'Blockchain and Sustainable Growth," UN Chronicle, 2018, https://www.un.org/en/un-chronicle/blockchain-and-sustainable-growth.
16 Fefer, Rachel F., "Blockchain and International Trade," Congressional Research Service, 2019, https://fas.org/sgp/crs/row/IF10810.pdf.
17 Levi, Stuart D. et al., An Introduction to Smart Contracts and Their Potential and Inherent Limitations," Harvard Law School Forum on Corporate Governance, 2018, https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.
18 Alexandre, Ana. "Chinese Internet Court Employs AI and Blockchain to Render Judgment," *Coin Telegraph*, April 25, 2019, https://cointelegraph.com/news/chinese-internet-court-employs-ai-and-blockchain-to-render-judgement.
19 Zmudzinski, Adrian. "Chinese Internet Court Uses Blockchain to Protect Online Writer's Intellectual Property," *Coin Telegraph*, December 8, 2018, https://cointelegraph.com/news/chinese-internet-court-uses-blockchain-to-protect-online-writers-intellectual-property.
20 Global Times, Beijing Courtrooms Turn to AI, Blockchain Technology," 2019, http://www.globaltimes.cn/content/1147520.shtml.
21 Mozur, Paul, et al., "Made in China, Exported to the World: The Surveillance State," *New York Times*, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.
22 Gartner, "Gartner Hype Cycle," 2020, https://www.gartner.com/en/research/methodologies/gartner-hype-cycle.
23 Institute for the Future, "Map of the Decade 2017-2027: Blockchain Futures," 2017, http://www.iftf.org/fileadmin/user_upload/downloads/blockchain/IFTF_BlockchainFutures_Map.pdf.
24 Oracle, "Transformational Technologies: Today," 2020, http://www.oracle.com/us/solutions/cloud/tt-technologies-white-paper-4498079.pdf.
25 De Filippi, Primavera. "Citizenship in the Era of Blockchain-Based Virtual Nations." In *Debating Transformations of National Citizenship*, pp. 267-277. Springer, Cham, 2018.

26 Bitnation, 2020, https://tse.bitnation.co/.
27 Nesta, "The Nation State Goes Virtual," 2017 https://www.nesta.org.uk/feature/10-predictions-2018/the-nation-state-goes-virtual/.
28 Ohlheiser, Abby. "Inside the Online World of 'Incels,' the Dark Corner of the Internet linked to the Toronto Suspect," Washington Post, 2018, https://www.washingtonpost.com/news/the-intersect/wp/2018/04/25/inside-the-online-world-of-incels-the-dark-corner-of-the-internet-linked-to-the-toronto-suspect/.
29 Von Behr, Ines, et al. "Radicalization in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism," 2013, https://www.rand.org/randeurope/research/projects/internet-and-radicalisation.html.
30 Torpey, Kyle. "This Cryptocurrency Just Surpassed Bitcoin in One Key Adoption Metric," Forbes, 2019, https://www.forbes.com/sites/ktorpey/2019/09/30/this-cryptocurrency-just-surpassed-bitcoin-in-one-key-adoption-metric/#64ff93487e2f.
31 Cuthbertson, Anthony. "North Korea Has Amassed $670 Million In Bitcoin and Other Currencies Through Hacking," 2019. https://www.independent.co.uk/life-style/gadgets-and-tech/news/north-korea-bitcoin-cryptocurrency-blockchain-un-report-a8819446.html.
32 Cavegn, Dario. "Deloitte: E-residency Brought €14.4 million to Estonia in First Three Years," ERR, 2017. https://news.err.ee/646254/deloitte-e-residency-brought-14-4-million-to-estonia-in-first-three-years.
33 Casey, Michael J. "Why the U.S. Shouldn't Let China Dominate the Digital Currency Race," Fortune, 2020. https://fortune.com/2020/04/07/china-us-digital-currency-coronavirus/.
34 Rolland, Nadege. "A China–Russia Condominium over Eurasia," 2019. https://www.iiss.org/publications/survival/2019/survival-global-politics-and-strategy-februarymarch-2019/611-02-rolland; Mações, Bruno. "Russia to China: Together we can rule the world," Politico, February 17, 2019, https://www.politico.eu/blogs/the-coming-wars/2019/02/russia-china-alliance-rule-the-world/.
35 Abi-Habb, Maria. "How China Got Sri Lanka to Cough Up a Port," *The New York Times*, June 25, 2018, https://www.nytimes.com/2018/06/25/world/asia/china-sri-lanka-port.html.
36 Mortier, Thierry. "How Blockchain Technology Is Transforming the Distributed Energy World," 2019. https://www.ey.com/en_gl/power-utilities/how-blockchain-technology-is-transforming-the-distributed-energy.
37 Liao, Shannon. "The Marshall Islands Peplaces the US Dollar with Its Own Cryptocurrency," *The Verge*, May 23, 2018, https://www.theverge.com/2018/5/23/17384608/marshall-islands-cryptocurrency-us-dollar-usd-currency.
38 Shin, Laura. "Why Cryptocurrencies Could Push the Dollar from World Reserve Currency Status," *Forbes*, November 7, 2017, https://www.forbes.com/sites/laurashin/2017/11/07/why-cryptocurrencies-could-push-the-dollar-from-world-reserve-currency-status/#89747376a9ed.
39 The Economist, "The search to find an alternative to the dollar," 2020. https://www.economist.com/leaders/2020/01/18/the-search-to-find-an-alternative-to-the-dollar.
40 Casey, Michael J. "Why the U.S. shouldn't let China dominate the digital currency race," Fortune, 2020. https://fortune.com/2020/04/07/china-us-digital-currency-coronavirus/.
41 Detrixhe, John. "China's Ant Financial, thwarted in the US, is expanding rapidly in Europe," *Quartz*, March 15, 2019 https://qz.com/1570052/ant-financials-alipay-is-expanding-rapidly-outside-of-china/.
42 Zhang, Hui. "Blockchain in China," MIT Tech Review, May 2, 2019, https://events.technologyreview.com/video/watch/hui-zhang-blockchain-china/.
43 Roumeliotis, Greg, "U.S. blocks MoneyGram sale to China's Ant Financial on national security concerns," *Reuters*, January 3, 2018, https://uk.reuters.com/article/uk-moneygram-intl-m-a-ant-financial/u-s-blocks-moneygram-sale-to-chinas-ant-financial-on-national-security-concerns-idUKKBN1ET03A.
44 Russell, Jon, Rita Liao, and Ingrid Lunden. "Alibaba's Ant Financial buys UK currency exchange giant WorldFirst reportedly for around $700M," *Techcrunch*, February 14, 2019, https://techcrunch.com/2019/02/14/alibabas-ant-financial-buys-worldfirst/.
45 Engen, John. "Lessons from a mobile payments revolution," *American Banker*, 2017, https://www.americanbanker.com/news/why-chinas-mobile-payments-revolution-matters-for-us-bankers.
46 Brimelow, Ben. "The Short Film 'Slaughterbots' Depicts a Dystopian Future of Killer Drones Swarming the World," Business Insider, 2017. https://www.businessinsider.com/slaughterbots-short-film-depicts-killer-drone-swarms-2017-11.
47 Mitchell, Anna. Diamond, Larry. "China's Surveillance State Should Scare Everyone," The Atlantic, 2018. https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/.
48 Eichengreen, Barry. "Hegemonic Stability Theories of the International Monetary System," Working Paper No. 2193, National Bureau of Economic Research (NEBR) Working Paper Series, Cambridge, MA: 1987.
49 McDowell, Daniel. "The US as 'Sovereign International Last-Resort Lender': The Fed's Currency Swap Programme during the Great Panic of 2007–09." New Political Economy, 2011. https://www.tandfonline.com/doi/abs/10.1080/13563467.2010.542235.

CHAPTER 21

The Significance of 5G for Special Operations of the Future

Toby Redshaw

> *"He will observe also that changes in tactics have not only taken place after changes in weapons, which is necessarily the case, but that the interval between such changes has been unduly long. This doubtless arises from the fact that an improvement in weapons is due to one or two men, while changes in tactics must overcome the inertia of a conservative class; but it is a great evil. It can be remedied only by a candid recognition of each change, by a careful study of the powers and limitations of the new ship or weapon, and by a consequent adaption of the methods and using it to the qualities it possesses, which constitutes its tactics. History shows that it is vain to hope that military men generally will be at pains to do this, but that the one who does will go into battle with a great advantage—a lesson in itself of no mean value."*
>
> ***—Admiral Alfred Mahan,***
> ***The Influence of Sea Power Upon History: 1660-1783***[1]

The Story Line

Military history is a key source for learning how to take advantage of technological changes. Foundationally, the tech matters and always has, but it must be managed intelligently and requires the ability to understand domain and context. To that end, this chapter details the Fourth Industrial Revolution (4IR) and why it matters, and the part 5G plays in it. I drill into what 5G really is, while demystifying it and discussing its pragmatic impacts. The "7Ps"—proactive, predictive, pattern-matched, preventative, permissioned, peer-connected, and precise—define the impact. I also discuss how to keep up with the increasing pace of technological change in a 5G world, including having future-proofing radar. Finally, how does 5G affect special operations? I propose some possibilities and prescriptions and outline some cautionary tales.

The Importance of Technology to Military Operations

I have been stealing from the military my entire career. Military history is a hundredfold richer domain than the history of business to understand strategy, planning, execution, and the value of talent, training, and morale. It is a richer source of learning for offense and defense performed both well and not so well. In this domain, one can clearly observe both successful and failing technology applications. As in business, no amount of talent, great execution, or technology will save you from bad strategy. Mighty Motorola fell in the 2000s because it executed a really bad strategy really well. However, even great strategy will certainly fail if structure is not matched to mission and talent to task. Many companies have failed and battles have

been lost because leaders structured and staffed forces based on the last "war" not the war to come.

My point is that technology matters.

About 3,300 years ago the Hittites pushed across modern-day Turkey with a technological superiority that granted them an overmatch advantage against their enemies. They had some of the the first mobile missile launchers. In actuality, this was a chariot corps with two or three soldiers lobbing javelins, but it was still a technological superiority that won the day.[2]

It is commonly accepted belief that numerical force superiority wins wars most often. While we revel in David beating Goliath, the back story is Goliath killed a hundred Davids and a thousand of David's less-known, less-skilled cousins (for this thought exercise, let's call them "Reginalds"). History, however, is full of examples of Goliaths losing. The CEO of Walmart—the current corporate Goliath—carries a photo of a list of the top-ten retailers for each decade since the 1950s as a reminder that companies that were on previous lists and seemingly undefeatable have either lost their lofty status or disappeared altogether.[3]

Walmart is in the numerical superiority game, while special operations forces (SOF) seek to achieve and maintain relative superiority. Technology matters in both. I would suggest it matters more in the world of relative superiority. So how does this tie into special operations?

In 2012, I was honored and surprised at my good fortune to be asked to participate in a three-day innovation summit with Admiral William McRaven and his direct reports at SOCOM, along with a small group of smart, seasoned industry and academic minds. My first response was, "why would the most innovative fighting force on earth need to spend time with us?" The answer was simple: adversaries were becoming increasingly innovative, and Admiral McRaven realized the time to improve an organization's technology and innovation is when it is still in first place, not after the organization begins to lose ground. Admiral McRaven knew this truth better than most and, early in his career, captured his thoughts on this topic in his master's thesis capstone at the Naval Postgraduate School, in which he wrote about special operations and how their "cutting-edge technology, access to national-level intelligence, high-quality training, and elite troops" combine to "achieve relative superiority."[4] One of the world's best engineers, Alan Kay, from Xerox Parc, is widely credited as saying "context is worth 80 IQ points." You can't delegate understanding context, understanding those all-important atmospherics, because when you do, you lose 80 IQ points. The CEO of Walmart didn't miss this observation, and neither did Admiral McRaven.

Rather than trot out the "answers," divine specific futures, or be prescriptive, my goal in writing this chapter is to explain what is coming now and coming fast in one specific sector: 5G and its environment. I hope to give special operations and 5G some context so deeper, smarter, more practiced people can leverage this knowledge advantageously both at home and overseas.

One important point from Carl von Clausewitz before we dive in: In the special-operations world, maybe more than any other, selection and training are the essential first steps to success, well ahead of any whiz-bang technology. Clausewitz called these the "moral factors," which boil down to an essential synchronized mix of perseverance, smarts, boldness, and bravery. No technology will supplant those attributes. They come from selecting and training the right men and women for each mission. Technology definitely can help, and, in this chapter, we'll see how 5G especially can help, but 5G is the tail, not the dog. Having the right people on the right mission makes all the difference.

The Fourth Industrial Revolution

We are at the start of the Fourth Industrial Revolution. This is massively important and provides the broader context for all things linked to technology now and for the next decade. Yes, context . . . 80 IQ points.

Before we explain 5G, let's explore 4IR a bit more. This concept comes from a 2016 book by Professor Klaus Schwab, founder and executive chair of the World Economic Forum, who runs the much touted annual confab of big shots, innovators, politicians, captains of industry, and luminaries that is Davos.

What is 4IR?

It means these things at a minimum:

- It's a big enough deal to merit being the fourth industrial revolution. The last three changed the world.
- Like the last three, it is not a rising tide, and there will be winners and losers, participants and spectators.
- Unlike past industrial revolutions, this one is purely technological.
- Unlike the previous revolutions that took decades to evolve, this one will take six years, perhaps a bit more or less.
- It is sometimes referred to as the cyber-physical era, which will intertwine and mesh the physical world with the digital world. Everything that can be connected will be connected.
- With connectivity comes intelligence, and with massive connectivity comes pervasive intelligence.

Importantly, just like the last three "revolutions," some areas adopt new technology methods, and do so extremely fast, while others do not and get left behind. Some 700 (yes, 700) automobile manufacturers have ceased to exist in the United States over the last 120 years, many because they did not adopt new technologies. Ever heard of Nyborg or Norwalk Underslung? The Waltham-Orient had a good run for a decade then

disappeared in 1908. These cars were made in Waltham, Massachusetts, near one of Verizon's current big 5G labs. The Riker Electric Car won the New York horseless carriage race in 1896. The cars were built in Elizabeth, New Jersey—just across the river from Verizon's NYC 5G Lab—and the company was dead by 1902. Some of these companies were the Goliaths of their time, others were Davids, others were Reginalds, and some Davids became Reginalds by missing technology shifts.

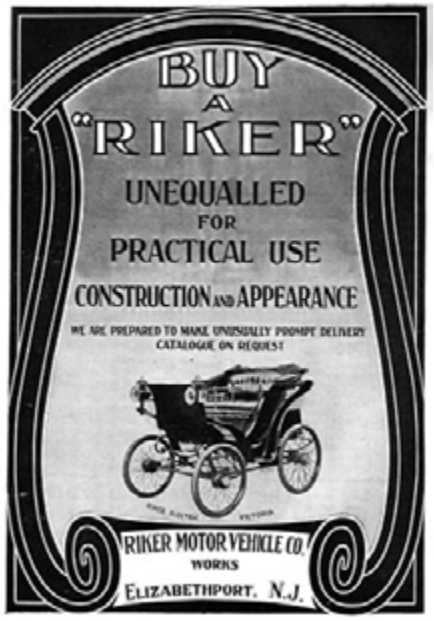


Figure 1: Advertisement for the Riker electric car.

Why Are We Entering 4IR Now? What Is Causing a Sea Change of This Scale?

The 4IR story is anchored in four technologies plus one. If we look back over the past decade, we have seen four technologies grow tremendously in terms of utility, adoption, impact, value, and/or scale. Think back to where cloud computing, artificial intelligence (AI) and big data, augmented reality (AR) and virtual reality (VR), and the Internet of Things (IoT) were in 2010, and it is easy to see we have come an amazingly long way. The original release for containers (the basic Lego of modern cloud computing) was only seven years ago. Global cloud annual revenue is now around $266 billion, and growth is accelerating.[5] There were more than 8 billion IoT devices in 2017.[6] Gartner projected there would be more than 20 billion in 2020; others had predicted more than 50 billion IoT devises by 2020.[7] Released in 2016, Pokémon GO, an AR game, is of no great impact or importance, does not use amazingly deep tech, and is not applicable to business in general and certainly not something special operations would look at. But it had 50 million users in its first 19 days.[8] That sends a noticeably clear signal: Imagine if Pokémon GO was a useful AR platform with real-world applications and a better tech solution—what is that growth curve?

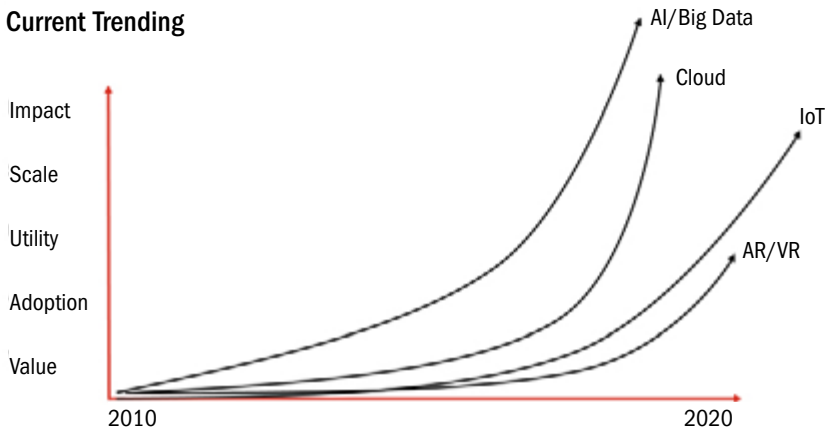


Figure 2: Current trending for artificial intelligence/big data, cloud computing, the Internet of Things, and augmented/virtual reality.

Now imagine these technologies were tied to a software-defined, cloud-native network that was designed for a thousand times more IoT density and ten times better battery life. A network that had compute built in at the edge, massive bandwidth capability, and super low latency. (Latency is telco talk for how quickly an end point can get a desired outcome, which is transmission time plus whatever processing is required.) What I just described is 5G. Together with the other four technologies mentioned, 5G creates a flywheel effect for accelerated growth and new capabilities—"four technologies plus one" driving the 4IR.

This scenario described in the previous chapter is the key premise behind the 4IR and why those four technologies plus 5G—despite the seemingly steep curve of growth since 2010—will experience hockey-stick growth in the 2020s and change everything. Here's a glimpse of the future:

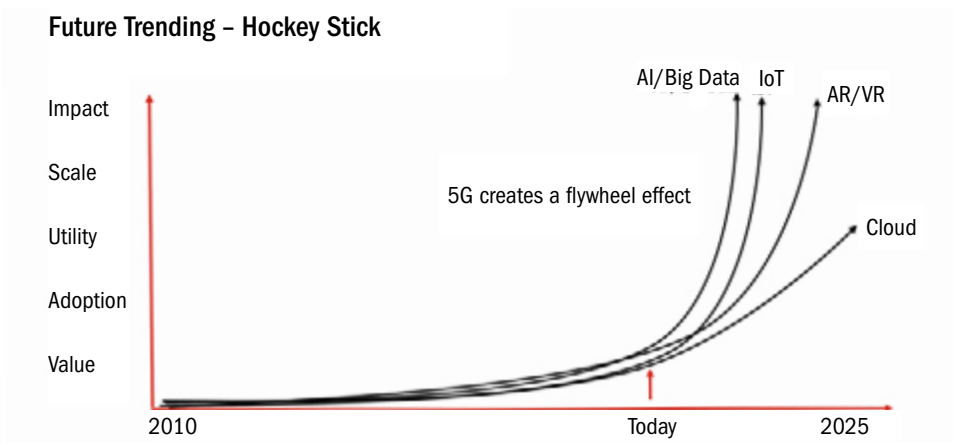


Figure 3: The "hockey stick growth" of 5G and four main technologies of 4IR by 2025.

I have been close to these technologies for a decade, and I am absolutely convinced they are at an inflection point in terms of unit cost, economic impact, and ease of adoption. Those three factors alone create hockey stick growth. The addition of 5G moves all of them into a new dimension around edge computing as they are accelerating. The technologies become more pervasive and intelligent and start to function in real-time environments, meaning in human dimensions, time intervals that are a fraction of a blink of an eye. In turn, these developments fuel many more applications as the unit cost to deploy goes down. A ten times improvement in IoT battery life with a thousand times improvement on IoT density restrictions clearly open up a much bigger total available market (TAM)—that's simply money. The larger TAM, lower unit costs, easier adoption, and high margins drives massive rapid adoption. On the AI/big-data side, emerging platforms exist that may be 50 times better than previous ones. Meanwhile the "legoization" of AI enables the field to move from the domain of data scientists and senior-level experts to second-year computer-science students. Those two factors alone are massive accelerators. Meanwhile, the cloud growth trends look like there will be a ten times growth during the 2020s.

So, let's assume the hockey-stick prediction is right. My favorite question about new tech has always been, "So what, who cares?"

It is fine that smart people all agree these changes will have such a large and broad impact that it has been defined as its own industrial revolution. But what does that really mean? To answer that question, one needs to understand what 5G really is and what kinds of new tech we will get when the four plus one combine. Once we understand those two things, we can begin to see why 5G matters for special operations.

Demystifying 5G

5G is a network technology massively different from 4G. It is not only a 10 to 1,000 times improvement in some of the key things we care about but also produces a binary leap forward. 4G does not have the latency to support real-time computing environments; 5G does. Latency is simply how quickly you go from ask to response in a network. On top of that, because 5G is a software-defined cloud network, it has compute built in all the way to the edge. This is standard cloud-based, containerized compute. A dumb cheap camera can take its pixel input, blast it back to the edge, and return intelligence (an impending crash, anomaly, defect, and identification of foe or friend) in 30 milliseconds, which includes the compute time and the transmission. That is roughly one-tenth the blink of an eye. That is a different world from 4G.

Networks are basically clever sets of wires and pipes. The electricity in your home and the water coming out of your tap are ends of networks. Telecom networks are also "pipes." There are basically two types: "pipes" in the ground or on poles, which are cables (mainly optical fiber). "Pipes" in the air are radio waves, and their size and features are functions of spectrum and the specifications of the equipment. 5G is a globally accepted set of specifications. The spectrum can provide huge capacity to very small capacity, depending on the wave. Millimeter waves from about 26 gigahertz

and up are massively fat pipes. The problem is, the fatter the pipes through the air, the lower the propagation and penetration through structures. This means building out a 5G network is about small cells, and lots of them, placed smartly, instead of the more familiar 4G towers we have all seen miles apart. 5G antennas send out smart, narrow (6-degree) beams targeted to specific receiving points. 5G towers send out broad, noisy waves across 120 degrees.

The diagram below shows what the key attributes of 5G pipes look like through the air. Remember, these attributes are all 10 to 1,000 times more than 4G and have compute at the edge; with that latency, compute and intelligence move into the real-time domain. That is a sea change. Most of the world happens in real time. This is part of the "so what" that comes with emerging 5G networks.

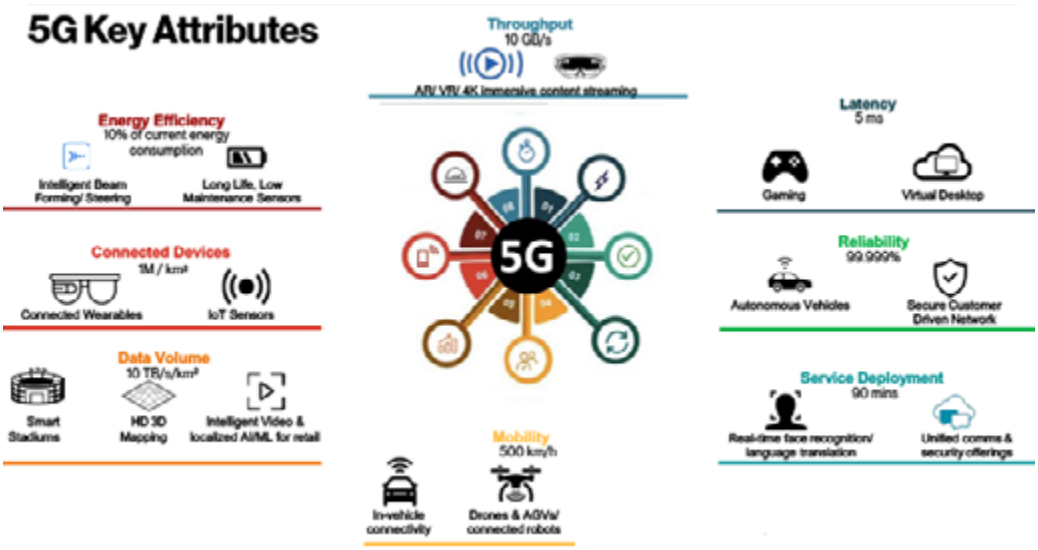


Figure 4: Some of 5G's key atrributes include energy efficiency, reliability, and data volume.

The other half of the 5G story is it is no longer just a network

It is a fabric with embedded, powerful compute at the edge.

A supercomputer in your back pocket that can process intelligence and rich media in real time.

5G's Pragmatic Impact

To show what 5G can do, I'll talk briefly about three major and two minor platforms this technology will enable. All the platforms are in Verizon's labs, and some are already with early test customers in the field. By 2021, these platforms will move toward the mainstream and become broadly available commercially in their early forms on 5G. Devices with 5G chips already exist, and the increasing number of devices these chips can go into are just around the corner (as are more specialized 5G-compatible chips).

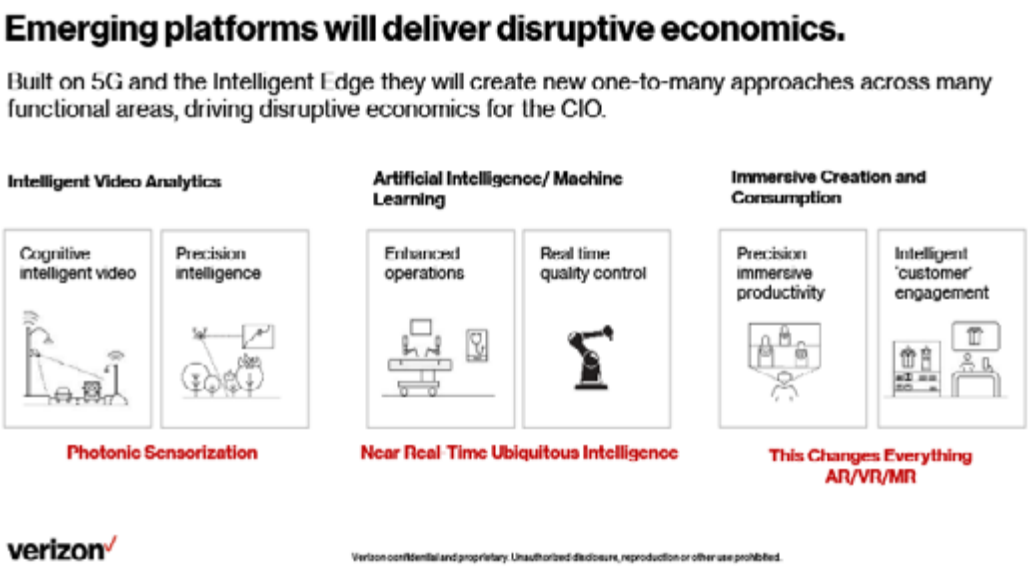


Figure 5: The three major platforms enabled by 5G.

Photonic Sensorization

Over 5G, a relatively cheap camera can send rich video feed at lightning-fast speeds, to be analyzed for patterns, triggers, intelligence, and anomalies. When coupled with AI, it can return a response in a fraction of a blink of an eye. This is all over the air. This could be from a drone, a body cam, or a listening post. AI (more precisely, machine learning [ML]) can be trained to recognize any elements in a flow of pixels relatively easily. Beating the Korean go champion, winning *Jeopardy!*, or modeling cancer molecule behaviors is difficult AI. Recognizing stuff in pictures just isn't. More than that, photons can become sensors.

Near Real-Time Intelligence

This is simply capturing all data available in a localized environment and being able to run it against ML models and get an answer back immediately. Clearly this has applications for the factory floor, venues, healthcare facilities, and distribution centers.

Having this capability could also make downrange ad hoc sensors, sensor nets, and co-opted sensor networks generate intelligence in real time.

Immersive Creation and Consumption

Immersive creation and consumption is the ability to have real-time intelligent AR/VR elements in any environment on a device or a heads-up display (HUD). It can be used to create hyperrealistic interactive immersive environments for training and operational preparation. Not too long ago, I did two ten-minute bursts in an immersive environment to teach employees the five key things to watch for (pattern match) when working the deli counter at a big grocery store. I barely give the exercise any thought, but I can recall these items instantly any time I am at a deli counter, much to the annoyance of the employees. This type of deeply immersive training is sticky, it stays with you, and it makes your team more effective and efficient. Other simulated programs allow you to walk through a space station or fly 100 yards above hot lava to fight storm troopers in a complex environment. These simulations had such high fidelity that the experience felt real. The ability to create realistic digital training environments that are between two to five times better for training and at a functional cost way below any current alternatives is a massive breakthrough.

The platforms that are enabled by 5G make operations, training, engagement and even environments:

Proactive, Predictive, Pattern Matched, Preventative, Permissioned, Peer Connected and Precise

We call those the 7 P's

These also improve agility, cost structure and effectiveness.

Figure 6: The "7Ps" of 5G.[i]

i Whether you are thinking of a consumer experience, a healthcare center, or something more closely tied to the SOF world, which do you want: ones that incorporate the 7Ps or those that do not? Credit to Professor Tim Chou (Stanford Computer Science) who gave me the 7th "P" (Precise—note his great book on IoT *Precision* [2020]). Also credit to John Sviokla, a former Harvard Business School professor who helped me with two of these "Ps" in a two-day "work session," including golf carts at Pebble Beach with cigars and beer.

Evolutionary Intelligence and Agility

Now imagine what happens when you combine these three digital platforms. All these processes and activities will produce mountains of raw data and metadata in real time that can be moved up to the cloud and used to create new models, discover new insights and patterns, solve crucial questions, and identify anomalies, risks, and opportunities. In turn, all this information allows me to update my processing at the edge to take advantage of the new information. I am then existing in an evolutionary environment that, when managed appropriately, can create an overmatch advantage that puts my team on continually more intelligent footing than an opponent, which is what "evolutionary intelligence" is all about.

Minor Platforms

The two minor platforms worth mentioning are volumetric capture, which is taking a huge leap forward, and next-generation presence and collaboration. When coupled with 5G, the end user now has the ability to make hyperrealistic three-dimensional images of anything (even objects in motion) and to create simulated training environments that make the user feel like s/he is actually there. There are many applications here for special operations to consider, such as what these technologies may mean for overwatch or for what overwatch may become in the future.

Special Operations—Possibilities, Prescriptions, Cautionary Tales

In the big picture, 5G is a tech domain that needs proactive engagement, monitoring, and a future-proofing radar to see what is coming up next. These steps can take the form of a series of effective listening posts to capture new tech related to 5G as it emerges and process those signals. The real trick will be to coordinate those listening posts and appropriately bin all signals into one of the following groups:

- **Not Applicable.** No need to pursue or monitor because the technology does not apply. For example, we may build some clever tech for combine harvesters that may not have any dual use for SOF or the Department of Defense.
- **Noted.** Technologies of interest in stages too early to determine exact applications; should be revisited in six months.
- **Interested.** Items that have potential, which you want to get your hands on and learn more about, maybe through a SOFWERX-, Naval X-, AFWERX-, or DARPA-like environment.
- **Obvious.** This is new technology with immediate opportunity to leverage. The Dreyse needle gun is a good historical example for this category (it is also a cautionary tale).

In business, especially information-technology areas, companies adopt new technologies commonly. However, the real challenge comes when dealing with removing legacy systems and architecture. That is often more challenging to replace, not a critical short-term mission, and tends to lead to horrible cost structure and inefficient spaghetti architectures. Complexity is the enemy of successful SOF. Technology and innovation should be used to drive out complexity. Down-range communications and information flows can be challenges of complexity, and usually those challenges are all about the architectures and designs upstream from the operator.Figuring out a good path for swapping out the old for the new deserves our attention. Clearly, an opportunity exists to impact the planning, preparation, and execution areas for special operations. In his book, Admiral McRaven maps out how innovation and new technology can be used to simplify plans, eliminate obstacles, and improve time to achieve relative superiority, core SOF functions.

As the world becomes more digitized, moving to real-time information flows could improve operational effectiveness and shrink the gaps between common operational practice, intelligence, and on-the-ground reality.

Having an over-the-horizon view can help ensure the technology is employed properly in the short and medium terms. More importantly, an over-the-horizon view can help operators manage out complexity. For SOF, this means really understanding the technical information architecture of pervasive technology.

Constant realistic rehearsals matter. The ability to do exactly that in short order, in more detail and with a lower cost structure with immersive real-time technology could make a big impact. I believe leaders in all aspects of training, learning, and performance improvement will adopt 5G technology because it is better and faster and has a better cost structure than 4G.

In my world, we think a lot about security. But, in my nonkinetic world, we do not think about it at the level SOF should. We also do not think much about countermeasures. Both security and countermeasures are issues that will need special attention in a dual-use technology world.

In special operations speed to relative superiority and speed of execution matter more than most environments. As 5G evolves, having cycle times as a guidepost and objective will be important. In the business world some of the biggest winners have not been the early adopters of technology but operators that looked at the new technology and innovated at the business-model level. When telegraphs and railroads started to crisscross the United States, companies like Sears and Standard Oil invented new business models to account for the nascent technology. Uber represents a modern-day example of employing new tech at the model level. The company dominated at a model level without really creating either anything difficult or special technologically.

A parallel tale to how 5G will likely impact special operations and society in general can be seen in Helmuth von Moltke's use of the telegraph and railroads to change the model of a standing army and deployment during the Franco-Prussian War. Moltke not

only made the standing army better and more responsive but also cheaper. Further, he adopted the Dreyse needle gun—the first bolt-action rifle—after both the French and British turned it down. The gun was relatively flimsy and broke more often, by an order of magnitude, than the robust muzzle loaders. From one perspective, the gun was not great technology. From another, it was. It fired five times more often than other guns. In addition, a soldier did not have to stand up (and become a big target) to reload. From a model perspective, even the wobbly first iteration of this tech was a breakthrough. The British and French high command who turned this down were not stupid. Judging new technology is hard.

Other areas that will adopt 5G and 4IR technologies and grow and change will be autonomous and semiautonomous vehicles such as drones and roboticsthat include robotic weapons and munitions. There will also need to be work on future enhancements like rapidly deployable private or isolated ad hoc networks, countermeasures, and the ideas that will come from the extra 80 IQ points deep context delivers.

Conclusion

There are three key things to keep in mind in the discussion about 5G and special operations. SOF must apply 5G and the technologies it will enhance across planning, preparation, and execution. SOF must also think across short-, medium-, and long-term horizons and across broader areas like information architecture to ensure simplicity, manageability, and effectiveness. Finally, SOF must have effective technology radar and future proofing to stay current and ahead of the game. On top of that, all special operations really rests on the selection of the operators and their "moral factors" of perseverance, smarts, boldness, bravery, and training, lots of training. Applying 5G to training will also matter, it could be a game changer.

Endnotes

1 Mahan, A. T. *The Influence of Sea Power Upon History, 1660-1783*, Boston, Little, Brown, 1890.

2 Ruiz, Luis Alberto, "The Hittites' Fast War Chariots Threatened Mighty Egypt," National Geographic, April 30, 2020, https://www.nationalgeographic.com/history/magazine/2020/03-04/hittite-fast-war-chariots-threatened-egypt/.

3 Thomas, Lauren. "Here's the One Photo Walmart's CEO Keeps on His Phone to Stoke 'Healthy Paranoia' in Race against Amazon," CNBC, December 7 2018, https://www.cnbc.com/2018/12/07/walmarts-ceo-says-this-photo-inspires-him-to-stay-ahead-of-amazon.html.

4 McRaven, William H. S*pec Ops: Case Studies in Special Operations Warfare—Theory and Practice.* New York: Ballantine, 1996.

5 Watts, Stephen. "Cloud Revenue and Market Share Trends in 2020," BMC Blogs, April 21, 2020, https://www.bmc.com/blogs/cloud-revenue-market-share-trends/.

6 Van der Meulen, Rob. "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent from 2016," Gartner, February 7, 2017, https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

7 Van der Meulen, "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017," 2017; Nordrum, Amy, " Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated," IEEE Spectrum, August 18, 2016. https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.

8 Desjardins, Jeff. "In the Race to 50 Million Users There's One Clear Winner—And It Might Surprise You," World Economic Forum, June 26, 2018. https://www.weforum.org/agenda/2018/06/how-long-does-it-take-to-hit-50-million-users.

CHAPTER 22

On Being Stretch Armstrong: Innovating Successfully inside Bureaucratic Organizations

Tambrein Bates, Brad Chedister, and Lt Col Jennifer J. Snow

> *"Learning and innovation go hand in hand. The arrogance of success is to think that what you did yesterday will be sufficient for tomorrow."*
>
> ***—William Pollard***

One of the toughest challenges facing the US government and the Department of Defense (DOD) is how to use innovation effectively to solve problems. If you were to ask each of the armed services and each interagency partner what "innovation" means to them, the definitions would be as diverse as the organizations they represent. Accurately defining what innovation means for a specific organization will determine if that organization competes successfully in the future as a national defense asset and if it can help its customers stay ahead of technologically savvy adversaries. As an innovator, navigating the various obstacles and challenges from within government can be a bit like being Stretch Armstrong: you get pulled in a lot of directions. You have to learn how to keep it all moving in the right direction to satisfy your customers' expectations.

Innovation has become the new watchword inside the DOD and the various interagency partners that make up the intelligence and federal law enforcement communities. Everybody wants it, needs it, spends toward it, but why are only a few of these government-founded innovation centers successful? Innovation is not as easy as having a big personality champion an idea, holding a few meetings in a flashy space, and then suddenly success is achieved. Innovation requires a clear purpose, a well-defined strategy, the right expertise, the right processes, and constant customer feedback. Further, innovation is a science, a deliberate effort to grant an organization an advantageous position over a technologically comparable or advanced adversary. Nowhere is this advantage more important than in support of national security. Yet despite millions of dollars invested in hundreds of research-and-development (R&D), science-and-technology, and innovation hubs, the DOD continues to struggle, at best, with incremental change and, more commonly (and dangerously), lags in innovation efforts tied to long-term acquisition plans, decentralized manufacturing, and politics that increase the gaps between national security, capability, and agility.

This chapter explores the challenges facing innovators. By highlighting the struggles and limitations, a more fruitful path can be identified and implemented independent of the current operating constraints. These innovation models and methods can help organizations best structure their efforts, help new innovation teams overcome key obstacles, and ultimately achieve success from within by leveraging the right solutions, metrics, and tools for their mission. It concludes with specific recommendations for leaders faced with securing the United States against diverse emergent futures.

How to Define Innovation

Words matter. How your customer, leadership, or innovation hub chooses to define innovation will impact your work, its structure, and the paths that develop. Getting this part right is important. No single definition of innovation exists, so understanding your mission priorities is central to understanding what innovation means for a specific customer and how to properly address their needs. Some hubs focus on a single technology sector, while others are designed for overall organizational process improvement and agility. Some innvoation hubs may also be designed to develop solutions that combine multiple collaborative areas of focus. Understanding priorities and mission needs and aligning them with the hub's charter is a vital process.

When addressing innovation, one must understand the definition of the word. Often, people confuse innovation with invention. Although the two complement each other, they are not the same thing. Merriam-Webster says, "The words innovation and invention overlap semantically but are really quite distinct." In this case, "*invention* can refer to a type of musical composition, a falsehood, a discovery, or any product of the imagination. The sense of invention most likely to be confused with innovation is 'a device, contrivance, or process originated after study and experiment,' usually something that has not previously been in existence. . . . *Innovation*, for its part, can refer to something new or to a change made to an existing product, idea, or field. One might say the first telephone was an *invention*, the first cellular telephone either an *invention* or an *innovation*, and the first smartphone an *innovation*."[1]

We can expand on the telephone analogy to help define the difference between the invention and innovation. The first bidirectional, electrically transmitted speech over distance was a groundbreaking invention. The method of transmitting speech today via cellular-based smartphones simply changes the way in which we achieve the same effect. Innovative, but not inventive.

Provided the definitions above, we can further define innovation based on generally agreed upon types, or levels, of innovation. Several different innovation models exist, including Jürgen Hauschildt's Four Levels and McKinsey's Three Horizons. More recent thought leadership defines innovative levels as 1) incremental, 2) adjacent, and 3) transformational.[2]

- Incremental: Sometimes called "core" or "Horizon 1," these typically serve existing customers and may involve new, improved or incrementally better products and/or services.
- Adjacent: Often referred to as "Horizon 2"; those innovations that leverage existing expertise but do so in new or innovative ways, typically expanding into adjacent markets or customer segments.
- Transformational: Sometimes called "breakthrough" or "Horizon 3" innovation; involves the creation of entirely new businesses to serve new markets and customers. This is the most radical type of innovation and, traditionally, the hardest to incorporate into existing organizations unless a crises arises to act as a catalyst or strong leadership provides the thrust in support.

The most mature innovation organizations help their customers diversify research funding by distributing efforts across these three kinds of innovation in a 40-30-30 ratio. Forty percent of their time is focused on incremental innovation, and 30 percent each on adjacent and transformational innovation. This practice ensures improvement to and modernization of current products for existing customers. Organizations also use innovation expertise to find and attract new adjacent markets as well as swinging for the fence by developing new products and new markets in anticipation of future challenges and competition in emerging areas.[3]

Why Do Some Innovation Efforts Succeed While Others Fail?

Innovations proliferate quickly, but organizations often struggle to sustain their impact and value. Many innovation labs become resource sinkholes, with little to show for the money spent except a cool space, with geeky furniture and high-tech toys, as evidence the organization is "doing" innovation. These labs vary in model, purpose, staff and experience, mission, and goals as well as the ways in which they connect and serve their customers. Some key questions may be posed: What red flags signal an innovation effort may be set to fail? Conversely, what are some indicators the stage is set for success?[4]

Failing innovation efforts or "innovation theater," defined as "any innovation work [that] is done to show people that innovation is happening, but which doesn't result in a tangible outcome,"[5] usually have several of the following characteristics:

- Flashy spaces with high-tech toys and lighting used for VIP "talk-throughs";
- Lack a clearly defined mission or too broad a mission or scope;
- Staff members unable to clearly articulate priorities, purpose, or overarching strategy;
- Center sits behind guards, gates, and guns or behind government firewalls that limit collaboration and potential flow of ideas and outside perspectives;
- Staff members not easily accessible, responsive, or open to outside ideas or collaboration—"Not Invented Here" syndrome[6] permeates the team;
- Innovation success is thought to derive from achieving a critical mass of funding or ideas or through company participation in "brainstorming" events;
- Innovation events are hosted with little background or defined requirements to guide participants;
- Lack of processes or plans to capture data from collaborative events and provide follow through to apply this information to actual problems and solutions;
- Innovation center has a low or no transition rate on projects to key customers;

- Innovation center has no tangible metrics to measure either innovation efforts or progress to show value or impact;
- Staff cannot articulate clearly their jobs' necessary functions;
- Staff cannot define clearly the structure, models, processes, and tools they use to support innovation requirements;
- The organization does not provide defined steps, plans, phases, processes, or tools for how innovation happens;
- Staff does not have a clear idea of who the customer is, with whom they need to be engaging and why, or who key stakeholders are;
- Staff does not have the right experience or mix of expertise or relies on part-time or additional-duty personnel to accomplish mission;
- Large budgets that allow for the "purchase of solutions" or checklist mentalities that limit creative approaches or outside perspectives;
- Lack of support from senior-level leadership.[7]
- Conversely, successful innovation platforms have the following indicators:
- Open messy spaces where people are working and things are happening; includes flexible, reconfigurable workspaces, meeting and training spaces, prototyping and manufacturing space, demostration space, and digital presence space, and is used daily by multiple users from various sectors;
- A clear mission flexible enough to evolve with the customer;
- Strong support and guidance from leadership to drive innovation and innovation strategy;
- Right combination of expertise necessary for the innovation platform to succeed, which should be a mix of abilities that bring experienced innovators into contact with fresh perspectives and government or agency liaisons;
- Readily available and updated tangible metrics to measure results to provide a measure of success and value;
- Seek to interact with sister services, interagency partners, industry, customers, and nontraditional groups outside the organization to gain fresh perspectives, new ideas, and new opportunities and technologies;
- Have a process, plan, tools, and path to transition projects.
- Well-defined, impactful issues that have a risk-to-reward ratio that justifies their selection and will result in disruptive innovation that complements or advances existing incremental innovation efforts by the sponsor;
- Functions as an additional tool for existing R&D, science and technology (S&T), and acquisitions efforts vice a duplicative or competitive effort;
- Encourages collaborative solutions that bring together diverse groups to take

on complex cross-cutting problems that a single organization or entity would struggle to accomplish;

- Able to proactively, positively, and consistently interact and influence partners and customers across spaces and within the primary service or agency sponsor;
- "Constraint-based" innovation that pushes innovators to go for disruptive instead of incremental and potentially duplicative solutions;
- A culture that emphasizes information sharing, transparency, trust, and shared credit where all participants benefit from participating and someone always wins;
- Rapid movement of innovation into the field for feedback and testing followed by persistent iterations to deploy the solution in support of the customer;
- Act as a friendly front door for innovators to participate and learn how to best team with government and military partners;
- Able to showcase multiple transitions and solutions that have been facilitated by the center and used by sponsor or customers today.[8]

These are not all-inclusive lists but can help organizations identify whether their innovation hub is geared for success. If an innovation hub is not well aligned with the mission it is meant to support, lacks a well-defined strategy or vision, fails to connect with real customers, lacks metrics to show how the center produces value, or has an unbalanced team staffed too heavily with either service members or entrepreneurs, then the probability of failure is high. The primary purpose of establishing an innovation center is to provide a safe space with the right mix of talent to drive innovation and creativity across the service or organization while providing for the strategy, people, and processes described above to enable success. Real change does not happen in a vacuum, and innovation hubs can be the nodes that educate, inspire, and connect everyone to external resources, technology, and tools that can help them solve their biggest problems.[9]

Modeling Innovation

Partnership Intermediary Agreements, Other Transaction Consortiums, and Commercial Solutions Openings

Several innovation lab models exist. Probably the two most recognized are the Other Transaction Consortium (OT Consortium) and the Partnership Intermediary Agreement (PIA). Commercial Solutions Openings (CSO) are another popular format, while hybrid models may bring together a complementary variety of solutions to meet more complex missions. But how can you know which model best supports your organization? How much flexibility do you need to innovate? Are you aiming to solve future problems

or existing gaps that the S&T department is struggling to address? Determining the appropriate model for the service or interagency partner you support is crucial to designing an effective hub. The following describes the most common models in use today and provides an overview of their purposes and how best to use them.[10]

OT Consortium–based models are appropriate for services or interagency partners that focus on prototypes or demonstrations, testing and evaluation, or technology-feasibility studies of innovative capabilities related directly to weapons or weapons systems, the mission effectiveness of people and platforms, or the improvements of platforms or key components. An OT Consortium can help identify and address known gaps in mission effectiveness, and an OT Consortium is a cheap, easy, and effective process when paired with a plan of phased future tasks to achieve innovative improvements. The OT Consortium model works well for mature organizations with established community support looking to expand or modernize missions during changing technology regimes[i] and constrained budgets. The model allows customers to focus on filling known critical mission gaps and acquiring innovative solutions. It primarily will produce incremental innovation solutions and is best set to provide operational to strategic-level solutions.[11]

PIA-based models are appropriate when the service or interagency wants to establish a collaborative community for technology exchange or technology transfers among government, industry, academia, and nontraditional technology partners. The model emphasizes joint collaboration to accelerate delivery of innovative capabilities. A PIA is most useful when leveraging multiple partners in collaborative technology exchanges around the development of relevant mission-enabling technologies, including the joint exploration of innovative solutions to fill key mission gaps (sometimes these may be unknown until external partners get involved) and to define new mission possibilities. A PIA must provide generous access, space, collaboration, information sharing, and transparency to establish the credibility necessary to show both internal and external partners the seriousness and potential value of the endeavor.

The PIA model helps the customer discover both current unknown gaps and shortfalls and what they need to be effective and at an advantage for future missions. The PIA model is appropriate for customers as part of a new, consolidated, or high-growth organization that may have nascent community support and that has to integrate new missions with rapid technology changes across multiple sectors. With the insight of the private sector, academia, or nontraditional experts, it can produce both disruptive and incremental innovation solutions and is best set up to meet critical needs for tactical to operational users.[12]

i Defined as "the set of attributes of a technological environment where the innovative activities of firms take place. Technological opportunity, appropriability of innovations, cumulativeness of knowledge and capabilities, and closeness of knowledge base to basic sciences (versus applied sciences) are attributes of technological regime" (Song, Michael, et al., "How Does Technological Regime Affect Performance of Technology Development Projects?" Journal of Product Innovation Management, June 16, 2014 https://doi.org/10.1111/jpim.12192).

In both OTA Consortium and PIA models, organizations may use pilots, prototypes, or demonstrations to express innovation and prove their relevance. Both models bring high value quickly, through innovation and outreach beyond the traditional vendor community. A PIA model has more internal flexibility to explore problem sets and to conduct neutral facilitation as a non-Federal Acquisition Regulation (FAR)–based entity, which sets a clear boundary to prevent conflict of interest and favoritism. (PIA staff do not select or award contracts or funding and can help direct technology to the right customers for a variety of competitive events, testing, and validation.)[13]

While PIA and OT Consortium are both effective models, there are key distinctions. First, the participants of each are derived from different sources. OT consortiums draw from a pay-to-play reservoir of participants, usually aligned by sectors (e.g., manufacturing), and are typically more traditional memberships that routinely seek government contracts as part of their business model. PIA models draw from a low-barrier-to-entry, or free, model that typically broadcasts challenges to a wide audience, followed by targeted research and marketing designed to deliberately increase nontraditional offerings.

Second, PIA and OT Consortium models differ in expertise. When sourcing and contracting technologies, the lines of effort (LOE) fall into two categories: LOE 1 and LOE 2. LOE 1 includes the collaboration, prioroitization, and events processes that lead to a specific down-selected technology in preparation for a contract award. LOE 2 includes the negotiation, contract award, and program-management functions that develop and/or purchase the capability for fielding decisions. While the process required to field innovative technologies requires both LOEs, PIAs tend to be much better at LOE 1, as their open participation approach attracts nontraditional entities. However, PIAs do not have the authority to assist with or issue government OT awards, so they are not well suited to LOE 2. On the other hand, OT Consortiums are specifically designed for LOE 2 because they are chartered to assist with government contracting efforts. However, during LOE 1, OT Consortiums do not attract many fast-moving nontraditionals or technology sectors because of their consortium participation models. In the future, hybrid models that combine these two types will reap the benefits of both.

The CSO-based model is appropriate for customers seeking to fulfill specific standing requirements, fill known capability gaps, or advance specific technology areas. This non-FAR model uses a merit-based approach that evaluates individual solutions using a streamlined process requiring only minimal corporate and technical information. It seeks to solicit nontraditional government partners under a process similar to a Broad Area Announcement (BAA) that allows for the acquisition of technologies relevant to a specific program or project. It has embedded processes designed to fast-track technology briefings and allow for notifications to be made within a 30-day window, encouraging feedback from service and interagency customers. The model also potentially allows for follow-on funding and sponsorship to move technologies to the next stage. Organizations typically pair CSO-based projects

with an OTA or PIA model but may use them alone to augment existing acquisitions processes. CSO projects allow for incremental and adjacent innovation.[14]

Other Innovation Tools and Models

Cooperative R&D agreements (CRADAs) also facilitate collaboration among the private sector, academia, and nontraditional technology partners with government agencies to develop technologies with both military and commercial applications. The DOD or interagency partners typically use CRADA with one or more of the models discussed in this section, allowing for the sharing of either in-kind resources or funding to develop specific technologies. Thus, the customer can access expertise to shape the technology in ways that best support its specific requirements. Commercialization lowers price points for the government and also supports industry partners in a manner that enhances the overall DOD mission. Technologies developed under a CRADA may lead to breakthrough solutions that grant the DOD and its partners technological advantage over adversaries. CRADAs also drive competition, ensure high-quality technological development inside the United States, and allow the government to team with unique experts. It also allows the government to gain access to sectors it previously may not have viewed as relevant to national security and expand its organic capabilities by teaming with industry, academic, and nontraditional tech partners to pursue technological foreign internal defense initiatives (Tech FID).[15]

In a skunkworks model, the innovation team sits in a separate space from the larger organization and pursues highly disruptive technologies and processes intended to revolutionize how services or organizations operate either daily or during specific wartime or crisis situations. These types of innovation efforts focus on long-term strategic-level initiatives and typically have resources and the freedom to test new ideas. A skunkworks-type effort's primary challenge is ensuring good communication with the primary sponsor or customer. Without consistent communications and feedback, this form of innovation may be viewed as too separate from the primary organization or a potential threat to other incumbents. If the service leadership does not have a clear understanding of a project's mission and vision, these efforts may be seen as unnecessary or expendable; therfore, a skunkworks model requires persistent engagement to promote understanding and alignment and may be used with one or more of the above models to promote rapid acquisitions of key technologies.[16]

Toward Innovation with Purpose

> *"Collaboration is not just technical. It's the cultural willingness to share and win as a team using the right technologies and the assumption that everyone can add value."*
>
> ***—Wayne Kurtzman***

With all of its complexity, putting innovation into practice is challenging. However, examining existing tech hubs, talking to their teams, participating in events, and digesting their lessons learned can help any service or organization determine the right model and tools. The SOFWERX PIA model provides an applicable case study for SOF.

Founded in 2015 by then USSOCOM acquisition executive James "Hondo" Geurts, SOFWERX provides a non-FAR-based innovation space outside government for cross-cutting collaboration and experimentation with less government restriction. The SOFWERX vision was to create a platform designed and operated to help solve challenging warfighter problems through increased collaboration and innovation. It focuses specifically on accelerating the delivery of innovative capabilities to USSOCOM customers and refining capability through exploration, experimentation, and assessment of promising technology to support agile acquisitions for the warfighter.[17] In order to achieve this, SOFWERX adopted a "big tent" philosophy designed to be transparent and inclusive and to encourage collaboration that benefited all participants, not just the government. The model rapidly resulted in an extended ecosystem of over 40,000 individuals and organizations from across government, industry, academia, and bespoke technological "tribes of expertise" that do not typically collaborate with the government.

A simple and expeditious process exists to accomplish SOFWERX's goals. SOFWERX provides neutral facilitation to support USSOCOM SOF Acquisitions and Technology (SOF AT&L) and Program Executive Offices (PEOs) missions to accelerate their warfighter support, focusing their efforts on acquisitions. SOFWERX provides technology, expertise, testing and evaluation, and rapid prototyping, while working with the end user to provide constant feedback to guide and shape technology. This becomes a force multiplying capability for the end user, saving lives, resources, and time while granting a tangible advantage or solving a critical challenge.[18]

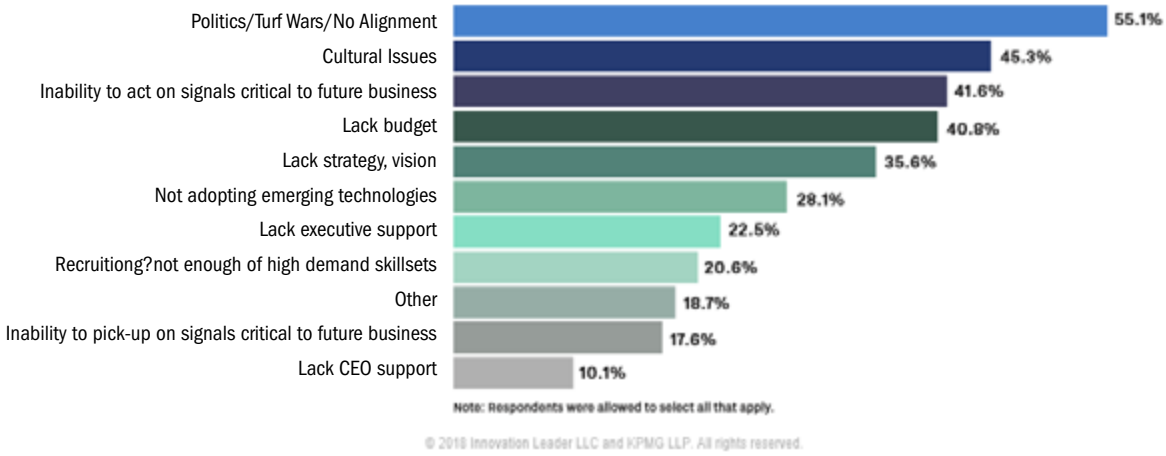
SOFWERX receives project nominations from the individual warfighter, the components, SOF AT&L, and HQ USSOCOM JCodes. Additionally, the SOFWERX PIA has leeway to explore transformational technologies by tracking technology forecasts, highlighting risks, and providing low-risk/high-yield opportunities to the command.[19] The SOFWERX team leverages ten primary activities to assess technologies for the end user, including collaborative project orders, rapid prototyping events, hackathons, capability assessment events, technology expos, combat evaluations, capability collaboration events, prize challenges, expert tech talks, and projects identified by USSOCOM stakeholders.[20]

The final component of the SOFWERX process is capturing the metrics of all outcomes. SOFWERX documents every nomination and activity to support these metrics. Impact categories include agreements, knowledge transfers, consignments, validations, and actual transitions to programs of record. Consignments allow tactical customers to leverage low cost, commercial-off-the-shelf (COTS) solutions to meet a critical need in a deployed or crises environment. Validations allow the USSOCOM

stakeholder to evaluate whether a technology can meet or solve a need and indicate if, not a good fit now, it might work in the future, allowing both successes and failures to be seen as positives. Agreements may include CRADAs or other collaborative orders that allow the government to access technologies and expertise it otherwise could not access, while knowledge transfers encourage the sharing of solutions across spaces and partners. Finally, SOFWERX can also assist with transitions to programs of record for PEO's by establishing assessment events that evaluate, downselect, and award agreements for promising capabilities. Metrics from these types of transitions benefit not only SOF but also the larger joint and conventional forces, and congressional and Senate offices frequently seek these metrics to evaluate success.[21]

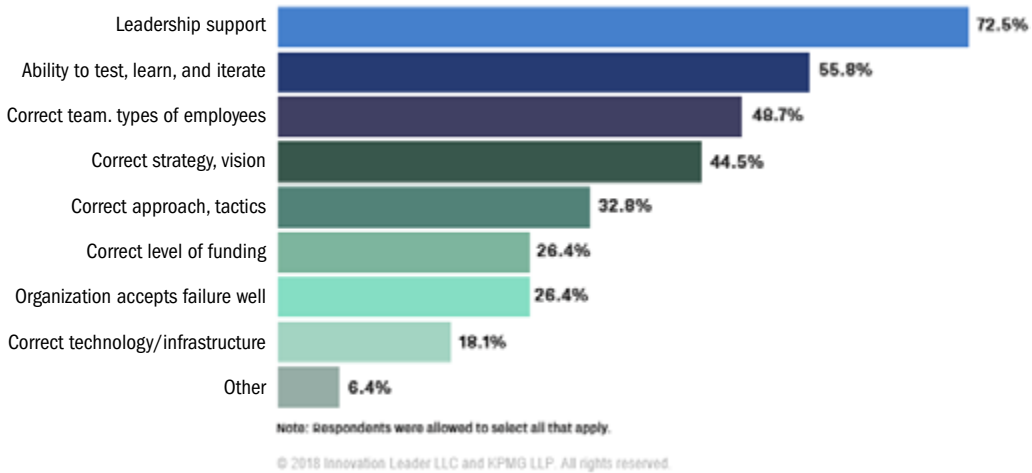
What Are the Barriers to and Enablers of Innovation?

Successful innovation requires understanding the barriers to innovation and how to most effectively enable innovation. In 2018, the Innovation Leader team surveyed over 500 chief innovation officers (CIOs), resulting in the "Bench Marking Innovation Impact 2018" report. Based on CIO feedback, the team found the following factors to be the biggest barriers to innovation:



After coordinating with fellow government innovators, beyond this survey, none of those teammates within the Department of Defense disagreed with either the barriers or their import. Most interesting, we have found that those that do not work in the innovation space often assume funding is the most prominent barrier. However, for those who do work in the space, funding rarely (if ever) is the barrier to innovative ideas or capabilities.[22]

If barriers exist, then conditions can be established to allow innovation to flourish. CIOs and government innovation teammates agreed the following metrics represented the enablers necessary for innovation success:



A large majority of those polled designated leadership support as the key component to successful innovation. Senior leadership can help align innovation goals and quickly resolve conflicts that arise from middle management. Leaders must ensure adequate alliances and consistent communication exist between the innovation team and the customer to continue positive momentum.[23]

How to Measure Innovation

Most organizations measure themselves through either financial or nonfinancial means. The Innovation Leader report indicated roughly 60 percent used "revenue generated from innovation products" as a metric, while only 25 percent do not track the financial impact of their innovation. Financial data can track tangible quantitative metrics, but what if the innovation space is mostly providing nonfinancial qualitative impact? According to Innovation Leader, the most mature innovation teams focused on customer touch points, insights generated by their center, and progress metrics, while the 25 percent of the least mature innovation hubs did not rely on metrics at all.[24] The following chart compares these metrics for most and least mature innovation teams:

Non-financial metrics by maturity

Metric	Least Mature	Most Mature
Customer Touch-Points	23.3%	63.0%
Learnings/Insights Generated	34.9%	54.5%
Progress Metrics	44.2%	45.5%
Patent Applications	18.6%	27.3%
Other Non-Financial Metrics	4.7%	27.3%
Brand Building/ Market Perception	20.9%	27.3%
Employee Participation Rates	27.9%	27.3%
Hypotheses Tested	18.3%	27.3%
Number of Ideas Generated	39.5%	18.2%
Media References or Press Mentions	14.0%	18.2%
None	25.6%	0.0%

While the DOD continues to fund disparate innovation organizations, many do not use innovation metrics or capture the most impactful metrics associated with their innovation goals and responsibilities. The MITRE Corporation conducted a holistic survey of government innovation organizations and found some interesting aspects of innovation efforts by organizational characteristics:[25]

Type	Definition	Primary Role	Percentage of Participating Organizations*
Networker	Facilitates connections and partnerships amongst parties with the purpose of creating community or collaboration.	Creating interactions.	67%
Educator/ Advisor	Propagates innovative techniques and activities to encourage innovation.	Imparting knowledge and disseminating guidance.	56%
Acquisition Facilitator	Expedites delivery of solutions through contracts between government and other entities.	Increasing the speed and efficiency of acquisition.	46%
Investor	Provides funding to advance innovation.	Effectively allocating funding.	46%
Incubator	Provides guidance and resources for early-stage innovations that are not ready for adoption.	Maturing technologies, products, and processes.	41%
Accelerator	Guides a proven solution to higher growth and adoption.	Increasing adoption of technologies, products, and processes.	23%
Developer	Creates or builds innovative technology, products, or other solutions.	Building new technologies and products.	15%

Table 2. Types of Innovation Organizations
Note: The total number of participating organizations was 39. Organizations can belong to multiple categories.

Of those organizations surveyed, multiple types of innovation structures existed, and each type played multiple roles. SOFWERX is a networker, although the team also conducts outreach and STEM programs for local schools, facillitates expert panels for government customer awareness, and acts as a neutral facilitator for acquisitions, helping to speed up the process and streamline acquisition timelines.[26]

Within each of the various kinds of organizations, MITRE broke out individual activities and impacts. The table on the following page assesses additional organizational activities, which helps one understand in which ways each kind of innovation organization excels. The breakdown of activities helps provide a starting point to develop both quantitative and qualitative metrics.[27]

While metrics can be an important place to start, there is concern about the inadequacy of metrics. Specifically, organizations should focus on the goals associated with each project. That way, regardless of an organization's associated level of innovation (incremental, adjacent, or transformational), specific goals can be quantified and measured objectively. Further, many DOD organizations point to "Transitions to Programs of Record" as a leading metric, which does not allow for the ideal 40-30-30 split of effort across innovation spaces to ensure the DOD gains a competitive advantage against adversaries while also allowing teams to look for and apply transformational levels of technology.[28]

Activity Category	Definition	Subcategory	Percentage of Organizations Reporting Activity*
Networking and Outreach	Increase engagement and collaboration within and across organizations and domains, through events, social media, partnership agreements, etc.	Organize and/or participate in networking events	64%
		Reach out to vendors that do not traditionally work with government	25%
		Build cross-functional teams to accomplish an objective	13%
		Arrange fellowships and exchange programs	10%
Funding	Provide funding to innovators, often through competitive selection process (e.g., "Shark Tank")		59%
Education and Training	Advance innovative approaches and thinking in government organizations through coaching, workshops, strategic guidance, etc.		46%
Product Evaluations and Assessments	Help innovators test and improve their solutions through technical assessments, red teaming, focus groups, etc.		44%
Contracting and Licensing	Assist innovators with identifying users and reaching contractual agreements	Facilitate pilot contract awards	41%
		Facilitate technology transfer (e.g., licensing government technology for commercial use)	5%
		Administer government Requests for Information (RFIs)	3%
Technical Events	Organize events around solving specific problems using hackathons, challenges, design sprints, etc.		38%
Research and Publications	Investigate and report on topics such as technological developments, markets, and best practices for innovation	Publish innovation playbooks, case studies, market research reports, etc.	36%
		Scout technologies on near-term and long-term horizons	13%
Prototyping	Build prototypes in-house and/or provide prototyping capabilities to others (e.g., maker space)		26%

Table 3. Activities Performed by Innovation Organizations
*The total number of participating organizations was 39.

What Should the DOD Do to Implement Innovative Ideas and Principles Effectively?

The biggest innovation challenges for the DOD include:

- US government debt. Redundancy and duplication of effort must be removed and lower cost, joint service, and unifying strategies must be implemented.
- The US private sector innovation base regards the US government as slow, onerous, and inflexible, scaring away partners, especially start-ups.
- US government funding, expertise, and requirements are scattered and invisible to ~90 percent of the marketplace.
- DOD technology analysis, acquisition, and implementation is fragmented and lags adversary decision/adaptation cycles, resulting in ever increasing capability gaps.

- National-level communities of interest do not have centralized locations for purposeful collisions, interagency and joint service collaboration, or positive competitive thought.[29]

To overcome these challenges effectively, senior governmental leaders should apply an immediate, comprehensive solution. The US government already has the tools necessary to "go fast." However, it does not have the organization, priorities, or authorization to leverage technology advancements effectively. It must pursue a flexible, high-velocity model to identify, assess, and deploy operationally relevant, low-cost technologies rapidly and at scale. Only then can our SOF forces keep pace with their adversaries.

One option for the government to explore would be to establish an accelerated synergistic group of business activities around specified technologies and their associated communities of interest. By creating five technology-focused hubs, the government and DOD will be able to streamline and strengthen the US innovation base and create a unified network, increasing both funding visibility while also drawing in the best ideas to provide cross-cutting solutions that prevent duplicatious effort for the nation. A basic model for this ecosystem might look something like this:[30]

• Cyber Security • Electronic Warfare • Near Peer CI • Sensors • Logistics	• Microelectronics • FNC3/C4I • AR/VR • Modeling, Sim & Training (MS&T) • IOT • Adv. Electronics • Materials and Manufacturing • Engineered Resilient Systems	• Human Performance • Human Factors Sciences • Biotechnology • Biomedical	• Data Science • Autonomy& Remote Control • Robotics and Human Machine Teaming • Air, Ground and Sea Platforms • Multi-Domain Operations (MDO)	• Hypersonics • Space • Directed Energy • Nuclear Modernization • Weapons Technologies • Counter IED • Counter WMD • Energy and Power Tech

Based on USD R&E Priorities and Reliant 21 Communities of Interest.
Locations TBD by the future Government Sponsor.

The five hubs should combine with 1) a nonprofit intermediary to execute day-to-day operations, 2) a proven innovation and collaboration processes, 3) a senior leader backing the process to ensure it is created holistically and used appropriately by the enterprise, and 4) an experienced OT developer that can award and manage the follow-on contracts.[31]

Reducing competition among the services and incentivizing collaboration on cross-cutting areas of interest for acquisitions and innovation will also help to optimize spending and solutions, prevent duplication of effort, and create increased agility. Limiting contract lengths is also imperative. Large-scale long-term contracts (10 years or longer) do not suit a world in which emerging technologies generate new threats perpetually. Shorter, more flexible contracts with early out options will force companies

to stay competitive and to remain in tune with technology advances or risk losing their place. Short-term contracts will also benefit SOF, as companies are incentivized to respond quickly to technology changes to create capabilities to beat adversaries in multidomain operations.[32]

The US government faces many innovation headwinds, but they can be mitigated by the five-hub concept, incentivizing armed services to collaborate on shared challenge areas and prioritizing acquisition and contract agility. Short of this type of holistic approach, the government will continue to waste precious resources by standing up more "silos of excellence" that neither communicate effectively nor share resources, requirements, goals, and objectives. A change in approach will ensure the full potential of the US innovation base is unleashed to best benefit our SOF forces, our nation, and US national security.

Bibliography

Ahmed, P. (1998, March 1). "Benchmarking Innovation Best Practice." Retrieved November 14, 2014, https://www.emerald.com/insight/content/doi/10.1108/14635779810206803/full/html.

Ahuja, S. B. (2019, September 9). "Why Innovation Labs Fail, and How to Ensure Yours Doesn't." Retrieved November 14, 2019, https://hbr.org/2019/07/why-innovation-labs-fail-and-how-to-ensure-yours-doesnt.

Atkinson, R. D. (2019, August 28). "How the US Government Falters on Support for Innovation." Retrieved November 14, 2019, from https://itif.org/publications/2019/08/28/how-us-government-falters-support-innovation.

Bates, T. (2019). "SOFWERX Executive Briefing." Retrieved November 14, 2019, https://www.sofwerx.org/.

Blank, S. (2019, October 7). "Why Companies Do 'Innovation Theater' Instead of Actual Innovation." Retrieved November 14, 2019, https://hbr.org/2019/10/why-companies-do-innovation-theater-instead-of-actual-innovation.

Brunelle, J., et al. (2019) "Measuring the Impact of Innovation Activities in Government." MITRE Corporation. Technical report for US Government FA8702-19-C-0001.

de Jong, M., Marston, N., & Roth, E. (2015, April). "The Eight Essentials of Innovation." Retrieved November 14, 2019, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/the-eight-essentials-of-innovation.

Drucker, P. (2018, April 19). "HDI." Retrieved November 14, 2019, from https://www.thinkhdi.com/library/supportworld/2018/how-to-measure-innovation.aspx.

Emprechtinger, F. (2018, April 27). "What Is the Degree of Innovation?" Retrieved November 14, 2019, https://www.lead-innovation.com/english-blog/degree-of-innovation.

Evans, N. D. (2017, May 3). "Four Considerations for Navigating 'Innovation Antibodies' and 'Innovation Theater.'" Retrieved November 14, 2019, https://www.cio.com/article/3193609/4-considerations-for-navigating-innovation-antibodies-and-innovation-theater.html.

Fact Sheet: The White House Releases New Strategy for American Innovation, Announces Areas of Opportunity from Self-Driving Cars to Smart Cities. (2015, October 21). Retrieved November 14, 2019, https://obamawhitehouse.archives.gov/the-press-office/2015/10/21/fact-sheet-white-house-releases-new-strategy-american-innovation.

Howieson, S. V. (2013, January 1). Policy Issues for Department of Defense Technology Transfer. Retrieved November 14, 2019, https://www.ida.org/-/media/feature/publications/p/po/policy-issues-for-department-of-defense-technology-transfer/p-4958.ashx.

"Innovation Labs: Getting Started and Delivering Results." (2016, February 29). Retrieved November 14, 2019, https://www.innovationleader.com/research-reports/innovation-labs-getting-started-and-delivering-results/970.article.

Innovation Leader. (2017, April 25). "The Corporate Innovation Ecosystem: Map & Discussion Guide." Retrieved November 14, 2019, https://www.innovationleader.com/downloadable-documents/the-corporate-innovation-ecosystem-map-and-discussion-guide/924.article.

Innovation Leader. (2018, February 5). "Best Practices in Scouting Trends and Emerging Tech." Retrieved November 14, 2019, https://www.innovationleader.com/downloadable-documents/best-practices-in-scouting-trends-and-emerging-tech/718.article.

Innovation Leader. (2018, March 1). "Innovation Illustrated: Measuring Innovation." Retrieved November 14, 2019, https://www.innovationleader.com/innovation-illustrated/innovation-illustrated-measuring-innovation/327.article.

Innovation Leader. (2018, August 16). "Blueprints for Corporate Innovators." Retrieved November 14, 2019, https://www.innovationleader.com/research-reports/blueprints-for-corporate-innovators/954.article.

Innovation Leader. (2018, June 12). "Benchmarking Innovation Impact 2018." Retrieved November 14, 2019, https://www.innovationleader.com/research-reports/benchmarking-innovation-impact-2018/963.article.

Invest in Canada. (2019). "Innovation Superclusters Initiative." Retrieved November 14, 2019, https://www.investcanada.ca/innovation-superclusters-initiative.

Kirsner, S. (2017, June 26). "Six Types of Innovation Lab: The Pros and Cons." Retrieved November 14, 2019, https://www.innovationleader.com/innovation-labs-and-spaces/six-types-of-innovation-lab-the-pros-and-cons/528.article.

KPMG International Cooperative. (2019, September 17). "Benchmarking Innovation Impact 2020." Retrieved November 14, 2019, https://home.kpmg/us/en/home/media/press-releases/2019/09/new-survey-data-indicates-increased-confidence-and-investment-in-innovation-among-fortune-1000.html.

Kuznicki, M. (2018, April 13). "Three Signals of 'Innovation Theatre' to Watch Out For." Retrieved November 14, 2019, https://medium.com/the-moment-is/3-signals-of-innovation-theatre-to-watch-out-for-8c2e29d4dcf3.

Leonard, H., et al. (2018). "SOFWERX: Innovation at US Special Operations Command." Harvard Business School Case. Retrieved November 14, 2019, https://lish.harvard.edu/publications/sofwerx-innovation-us-special-operations-command

Manning, B. (2018, December 21). "Commercial Solutions Opening." Retrieved November 14, 2019, http://acqnotes.com/acqnote/careerfields/commercial-solutions-opening.

Manning, B. (2019, February 23). "Cooperative Research and Development Agreement (CRADA)." Retrieved November 14, 2019, http://acqnotes.com/acqnote/tasks/cooperative-research-and-development-agreement.

Manning, B. (2019, August 15). "Other Transaction Authority (OTA)." Retrieved November 14, 2019, http://acqnotes.com/acqnote/careerfields/other-transaction-authority-ota.

Milliken, K. (2019, August 22). "The Five-Step Approach to Disruptive Thinking." Retrieved November 14, 2019, https://www.innovationleader.com/innovation-methodologies/the-five-step-approach-to-disruptive-thinking/1148.article.

Milliken, K. (2019, September 13). "How Customer-Centric Innovation Can Lead to Big Wins. Retrieved November 14, 2019, https://www.innovationleader.com/open-innovation-/-co-creation/how-customer-centric-innovation-can-lead-to-big-wins/1166.article.

Minister of Innovation Science and Economic Development. (2018, September 4). Innovation Superclusters Initiative. Retrieved November 14, 2019, from https://www.ic.gc.ca/eic/site/093.nsf/eng/h_00000.html.

Obama, B. (2011, October 28). Presidential Memorandum—Accelerating Technology Transfer and Commercialization of Federal Research in Support of High-Growth Businesses. Retrieved November 14, 2019, https://obamawhitehouse.archives.gov/the-press-office/2011/10/28/presidential-memorandum-accelerating-technology-transfer-and-commerciali.

Pisano, G. P. (2019, February). "The Hard Truth about Innovative Cultures." Retrieved November 14, 2019, https://hbr.org/2019/01/the-hard-truth-about-innovative-cultures.

"Seven Benefits of Workplace Collaboration." PLANBOX. (2019, October 17). Retrieved November 14, 2019, https://www.planbox.com/7-benefits-of-workplace-collaboration/.

Quinn, B. (2015, November 11). "Why Measuring Innovation Matters." Retrieved November 14, 2019, from https://www.forbes.com/sites/brianquinn/2015/11/05/why-measuring-innovation-matters/#2eb142946cd8.

Reperi Analysis Center. (2019) "Eight Reasons Why SOF Will Operate under Increasing Risk." Government Futures Report. Available from team@reperi.com.

Swearingen, W. D., & Dennis, J. (2009). "US Department of Defense Technology Transfer: The Partnership Intermediary Model." *International Journal of Technology Transfer and Commercialisation, 8*(2/3), 270. doi: 10.1504/ijttc.2009.024389.

"What is a CRADA?" (2016, June 11). Retrieved November 14, 2019, https://tier7.us/what-is-crada/.

Wright, T. (2018, April 20). "McKinsey's Three Horizons of Growth Can Help You to Innovate." Retrieved November 14, 2019, https://www.executestrategy.net/blog/mckinseys-three-horizons-of-growth.

Endnotes

1 Merriam-Webster. (2019, November 5). Invention. Retrieved November 14, 2019, from https://www.merriam-webster.com/dictionary/invention.
2 Emprechtinger; Wright.
3 Wright.
4 Ahuja; Blank; Evans; Kuznicki.
5 "Is Your Company Just Performing 'Innovation Theatre'"? Idea to Value, February 12, 2019, https://www.ideatovalue.com/inno/nickskillicorn/2019/02/is-your-company-just-performing-innovation-theatre/.
6 Pop, Oana-Maria, "Does Your Organization Have the Not Invented Here Syndrome?" Hype Innovation, March 26, 2015.
7 Ahuja; Blank.
8 de Jong, Marston, Roth; Innovation Leader "Innovation Labs: Getting Started"; Innovation Leader, "Blueprints for Corporate Innovators"; Innovation Leader, "Benchmarking Innovation Impact 2018"; Pisano; "Seven Benefits of Workplace Collaboration"; Quinn.
9 Milliken, "Five-Step Approach"; Pisano; "7 Benefits of Workplace Collaboration"; Quinn.
10 Kirsner.
11 Kirsner; Swearingen, Dennis.
12 Kirsner; Manning, "Other Transaction Authority"; Swearingen, Dennis.
13 Kirsner; Manning, "Other Transaction Authority"; Swearingen, Dennis.
14 Manning. "Commercial Solutions Opening"; Manning, "Other Transaction Authority"; Swearingen, Dennis.
15 Manning. "Cooperative Research and Development Agreement (CRADA)"; Swearingen, Dennis.
16 Kirsner; Manning, "Other Transaction Authority"; Swearingen, "US Department of Defense Technology Transfer," 2009.
17 Leonard, et al.
18 Leonard, et al.; Bates.
19 Leonard, et al.; Bates.
20 Leonard, et al.; Bates.
21 Leonard, et al.; Bates; Innovation Leader, "Benchmarking Innovation Impact 2018."
22 Innovation Leader, "Benchmarking Innovation Impact 2018."
23 Innovation Leader, "Benchmarking Innovation Impact 2018."
24 Innovation Leader, "Benchmarking Innovation Impact 2018."
25 Brunelle, et al.
26 Brunelle, et al.
27 Brunelle, et al.
28 Brunelle, et al.; Innovation Leader, "Benchmarking Innovation Impact 2018."
29 Atkinson; "Fact Sheet: White House Releases New Strategy"; Howieson; Obama.
30 Invest in Canada, "Innovation Superclusters Initiative."; Minister of Innovation Science and Economic Development, Innovation Superclusters Initiative; Obama.
31 Invest in Canada. "Innovation Superclusters Initiative"; Minister of Innovation Science and Economic Development, Innovation Superclusters Initiative.
32 "Eight Reasons Why SOF Will Operate under Increasing Risk."

CHAPTER 23

Special Operations Forces as a Rapid Prototyping Laboratory

Leo Blanken and Philip Swintek

Introduction

The US military's once-secure technological lead is slipping away. Peer competitors have developed clever strategies to exploit the US lead, while making significant progress in their own right.[1] Further, the technology landscape is moving away from large, centralized research efforts toward small, diffused networks of technological innovation. The Department of Defense seems to be finally waking up to the fact that it needs to develop novel strategies for navigating the relationship between emerging technology and national security.[2]

We propose one such strategy in this chapter. In brief, we argue the unique nature of special operations forces (SOF) offers a rich opportunity to be leveraged as a "rapid prototyping laboratory" (RPL). This laboratory could serve the development of SOF-specific capabilities, as well as more wide-ranging capabilities that may be scaled up to the general-purpose forces.[3]

In an RPL construct, SOF units and activities could serve as a test bed for new technologies, concepts, and practices. These activities could easily be conducted by employing the logic of inductive inquiry, natural experimentation, and field experimentation to provide structure and rigor to the prototyping activities. The proposed innovation challenges for testing could be curated from across the joint force. Professional military education (PME) institutions are the perfect locations for the curation and refinement of such research questions, as well as for designing and executing the RPL processes.

SOF have many attractive qualities that make them ideal living laboratories for the rapid prototyping of innovation challenges. First, SOF forces are continuously distributed to the most operationally relevant locales around the globe. No matter the topic one is interested in—from peer competitors, nonstate threats, partner force operations, or any of a host of irregular challenges—SOF units are deployed to such an environment. Second, SOF forces are the most capable of weaving research activities into their operations. Through their careful selection and training processes and lean organizational design, SOF possess the cognitive and operational flexibility to integrate prototyping nimbly and responsibly. Through thoughtful planning that leverages a dedicated network of PME-based researchers and "customers," the joint force could fruitfully utilize SOF units as a global laboratory for innovation.

In this chapter, we first set the stage by discussing the Department of Defense's legacy system of innovation, and how it fit appropriately with the technological and strategic landscape of the Cold War through the example of the "Second Offset." We then sketch the current technological and strategic landscape, showing how the

Second Offset legacy innovation system can no longer keep pace with demands. Next, we explicate our argument in two steps: explaining the logic of rapid prototyping and showing its natural fit to a partnership between SOF and PME entities. Finally, we provide some concrete examples that deliver a robust "proof of concept" of SOF operators who have—through their own entrepreneurship—already started the rapid prototyping endeavor called for above. Our proposal seeks simply to scale up, systematize, and hyperenable such entrepreneurship.

Legacy System of the Cold War, and Why It No Longer Works

World War II taught the United States that success in modern warfare is inextricably linked to applied science and technological innovation.[4] The total nature of the conflict made clear that systems needed to be built to access expertise from across the entire society to produce the innovation necessary for the nation's security.[5] The system designed to generate innovation for US national security reflected the scale and centralization of the industrial-age warfare in which it was born[6] and proved to be a useful tool in offsetting the size advantage enjoyed by Warsaw Pact conventional forces throughout the Cold War.[7]

The centralized structure of innovation during the Cold War can be likened to a lighthouse: a tall vertical structure from which a single beam emanates at the top. In such a construct, the leadership at the top of the lighthouse surveys the strategic environment to drive innovation requirements. The leadership then, in turn, directs the subordinated structure of the lighthouse to provide the needed innovations.

This approach to innovation worked during the Cold War for a number of reasons. First, military and political leaders understood their opponent well. The United States well understood the force and bureaucratic structures, Warsaw Pact alliance, and political goals of the Soviet Union, as they largely mirrored those of the United States. This provided a useful framework from which force planning, intelligence, and doctrinal needs could be deduced.[8] Second, the US national security apparatus had a firm grasp of the trajectory and nature of the technologies that would be relevant on the battlefield. Nuclear weapons aside, all force structures during the Cold War were improved versions of the platforms and doctrine of World War II. In fact, the Cold War period maintained the uninterrupted track record of the US defense establishment driving the technological landscape, as every single major technological advance in the United States to that point had relied on Defense dollars for the basic research.[9] More specifically, to control technological innovation in this period, the Department of Defense funded universities, government laboratories, and the relevant units and organizations within the services.[10]

The crowning achievement of this era of US military innovation, the "Second Offset" wedded doctrine and technologies designed to prevent numerically superior Warsaw Pact forces from swamping NATO defenses in central Europe.[11] Through a carefully orchestrated combination of primary research, applied research, and field experimentation wedded with coevolved doctrinal concepts, the United States solved

this problem. Stealth aircraft, advanced sensors, and precision-guided munitions were the technological innovations necessary to enable the AirLand Battle doctrine of the 1980s.[12] This series of technical achievements constituted an innovative solution to a well-understood and highly salient military scenario. In this case, the "lighthouse" discerned the strategic problem and effectively generated the innovations necessary to answer it.

None of the conditions that enabled the "lighthouse" to work during the Cold War holds true anymore. Rather than facing a single, well-understood threat, the United States faces a large number of heterogeneous and poorly understood challenges, which range from the enduring scourge of violent nonstate actors to emerging regional threats and peer competitors determined to contest the United States in asymmetric and nontraditional ways.[13] Further, the pace of technological change vastly outstrips that of the Cold War, and, for the first time in American history, basic technologies are being developed outside the control of the Department of Defense.[14] Finally, while the United States has been focused on its global war on terrorism, its chief rivals on the global stage—namely China and Russia—have begun to outpace US military innovation and technology.[15]

Therefore, the legacy "lighthouse" model of innovation is no longer sufficient. Future innovation efforts should look more like a "Christmas tree." In this metaphor, the bright star at the top of the Christmas tree would fulfill the function of the original lighthouse beam; it would focus on well-understood and agreed-upon requirements. The rest of the tree, however, is also strung with lights. These strings of Christmas lights represent innovation efforts diffused throughout the enterprise. Rather than innovation being compartmentalized in a reductionist division of labor, innovation efforts can be encouraged and enabled throughout the force. Further, given the inherent asymmetric and decentralized structure of SOF, these units are perfectly suited to the Christmas-tree model of innovation and could constitute the first string of lights on the tree.

What a Rapid Prototyping Laboratory Looks Like

The Secretary of Defense's advisory Defense Innovation Board (DIB) recommends the following changes to foster innovation:

> *Test various possibilities of employing different practices to seek out empirical evidence, . . . [to be] rapid, iterative, and risk-tolerant. Instead of giving processes pride of place . . . focus on outcomes, and how to get there most efficiently. These practices should be generalized, and not only to products and services, but potentially to strategies and operations as well.*[16]

There are a number of such voices calling for fast, iterative feedback loops between operational experiences on one hand and providers of material solutions

on the other. Such an approach to military innovation can generally be labeled "rapid prototyping."[17] Actionable plans to instantiate rapid prototyping, however, remain lacking. Some refer to rapid prototyping as a "mindset" or "culture" that needs to be inculcated throughout the force.[18] Others seek to rely on nascent technologies to make the process work: "Immediate feedback will pour into a data lake where the latest methods in machine learning and artificial intelligence can improve operational effectiveness."[19] We propose a specific set of established methodologies, married to a specific set of operationally deployed units to implement rapid prototyping immediately and effectively.

The first task is to concretize "rapid prototyping," turning it from a buzzword to specific and well-established research techniques. We offer three such analytic tools that can be implemented readily: *field experimentation, natural experimentation,* and *inductive reasoning.*

Experiments are designed to establish control. In other words, experiments allow the researcher to isolate the independent effect of various factors upon some outcome. *Field experimentation* refers to conducting such research in "a naturalistic setting and manner . . . as a hedge against unforeseen threats to inference that arise when drawing generalizations from results obtained in laboratory settings."[20]

The common usage of "field experimentation" across the joint force does not fit this definition, as it usually refers to the observation of nascent technologies being demonstrated in an empty field on some US military base. Often, by the time innovations are actually integrated into field exercises for conventional forces, they have been acquired and integrated into force structure. Actual field experimentation would allow the researcher to contend with all the potential confounding factors created by *actual* encounters with opposing forces in the **actual** settings in which innovations are designed to operate,[21] which would require as many aspects of a "down range" setting as possible. Globally deployed SOF missions provide a perfect locale for such field fermentation.

Natural experiments can be considered a subset of field experiments. In these cases, control over potential confounding factors occur naturally in the environment. For example, if US forces are operating in two provinces of Afghanistan that are strikingly similar across a number of attributes, an innovation may be tested in only one of those provinces (rather than multiple iterations of costly tests in multiple areas). Such a design would not only be economical but also provide a large degree of control, thereby generating stronger inferences regarding the impact of the potential innovation under scrutiny. Given restrictions on "random assignment" within military operations, sensitivity to naturally occurring experimental opportunities is paramount in leveraging this logic.[22]

Finally, *inductive reasoning* refers to the process of inferring general laws or principles from the observation of particular instances (as opposed to relying on preexisting theory to derive conclusions, as is done through deductive reasoning).[23] In other words, inductive reasoning relies on discerning trends or patterns within

naturally occurring data. Though this seems the simplest of the three methods discussed here—colloquially referred to as "lessons learned"—the US military has struggled to learn systematically from things that it has experienced and observed.[24] This is because of the inherently conservative inclinations of military organizations[25] but also their poor understanding of these two modes of reasoning.[26]

SOF are an attractive force of choice for implementing a model of this sort for the same reasons they are often selected for unique and high-risk missions—their maturity, education levels, and rigorous selection processes.[27] SOF units are often more comfortable with risk simply based on the nature of SOF missions.[28] Furthermore, SOF are also consistently deployed across the globe, with forces spread across each of the six geographic Combatant Commands. Finally, special operators conduct a wide array of missions—from near-peer competition, to direct-action counterterrorism and working closely with partner forces—ergo, they are postured to explore an equally wide range of innovation challenges.

Collaborative partners will be necessary to conduct rapid prototyping endeavors. While forward deployed SOF offer an ideal environment to conduct rapid prototyping, additional labor and expertise will be necessary to execute these activities. PME students may prove to be the ideal partners. As military professionals, they would understand the organizational, operational, and strategic contexts in which the protyping activities are nested. As graduate students, they could employ research techniques they are currently learning in the classroom. Finally, they could serve to connect the research to the relevant actors (academic, industry, and interagency) across the wider innovation ecosystem.[29] Through such a partnership, the professional development of PME students would be directly tied to the transformation of the force through operationally relevant research projects.[30]

In the following section we show some examples of specific innovations that have been prototyped by special operators. These "naturally occurring" innovation efforts show the untapped potential that our proposed endeavor seeks to harness.

SOF's Natural Affinity for Innovation Prototyping

In recent decades, US SOF has already demonstrated itself as an RPL for emerging technology, albeit an unintended one. The benefits of pairing SOF with the development, testing, and implementation of emerging or untested technology has been shown in a number of cases. We briefly survey three here. First is the use of Global Positioning Systems (GPS)–based technology and satellite communication (Satcom) during the initial invasions of Iraq and Afghanistan during both the Persian Gulf War and the war on terrorism, respectively. Second are the ongoing challenges around countering unmanned aerial systems (CUAS). Third is the development of the Android Tactical Assault Kit (ATAK), an innovation spearheaded by PME students, to enable collaboration with partner forces. We offer these three examples to show a latent rapid prototyping capability that could easily be systematized and expanded to great effect.

One of the most influential technological advances for the US military in recent memory has been the use of GPS technology across all aspects of the Department of Defense. GPS technology is not new. As early as the 1960s, the US military used a rudimentary version of the technology to guide both ships and aircraft. In 1978, the United States increased its GPS capabilities by launching the first Navstar satellite constellation, but the system was largely untested in combat until Operation Desert Storm, during which US SOF were vital to testing the system in the laboratory of combat.[31] Specifically, SOF deployed behind enemy lines used GPS technology to navigate across the barren desert, conducting special reconnaissance deep in enemy territory.[32]

Undoubtedly, mistakes were made while using a largely untested technology, but these mistakes were used to improve techniques and equipment. For example, after the Persian Gulf War, the Army dictated that all armored vehicles would carry GPS receivers, and the demand for handheld devices, which were primitive by today's standards, surged across the force.[33] This increase in demand and utility was partially based on the successful use of GPS technology during the ground and air wars waged by US forces during this short, but influential, conflict. With these lessons, among others, the implementation of GPS technology and its satellite constellation grew and improved, and the improved US GPS infrastructure greatly enabled SOF during the subsequent conflicts across Afghanistan and Iraq, paving the way for another RPL for GPS and SOF.

As detachments of US SOF waged unconventional warfare in the mountains of northern Afghanistan, their mission was to advise and assist the freedom fighters of the Northern Alliance struggling to resist the Taliban on their own. A key component of their mission was to increase the lethality and survivability of the Northern Alliance through combat-multiplying technologies such as GPS. Primarily, GPS served two purposes during the initial invasion of Afghanistan in 2001: map the front lines and provide guidance to smart bombs. US SOF and operatives from the Central Intelligence Agency (CIA) traveled along the scattered northern frontlines and used GPS to pinpoint friendly and enemy positions in conjunction with laser-guided bombs to mark high-value enemy targets for pilots flying overhead.[34] This data provided valuable intelligence to senior US officials as they planned the larger campaign to ouster the Taliban and defeat al-Qaeda. More important, it also demonstrated the combat power provided by a handful of secure portable handheld GPS devices to senior military leaders and policy makers. Today, handheld GPS technology is ubiquitous across the US military. Once again, SOF, and its partners in the interagency, served as an RPL to validate technology in a combat laboratory.

Just over a year later in Iraq, the US military used the same GPS technology during Operation Viking Hammer. As soldiers from the Tenth Special Forces Group (Airborne) blazed their way through Kurdistan and into northern Iraq, they relied heavily on GPS to coordinate their efforts.[35] SFOD-As from Tenth Special Forces Group (Airborne) were spread across the Iraqi frontier as they led their Kurdish partner forces to defeat

Saddam Hussein's army. This swift campaign required precise knowledge of friendly positions. Relying on handheld and vehicle-mounted GPS systems, commanders could see the positions of their subordinate units with high accuracy. While GPS technology supported a highly precise bombing campaign in Afghanistan, in Iraq, it increased the freedom of maneuver for friendly forces by supporting decentralized operations. Commanders understood the battlefield with a new level of clarity that supported the dispersion of forces across large geographic areas—further validating GPS as a combat multiplier via a SOF RPL.

Similar to GPS, SATCOM was not new technology during the invasions of Iraq and Afghanistan. Though widely used throughout the military prior to 2001, it was largely untested in combat prior to the war on terrorism. During the onset of combat operations in Afghanistan in 2001, SATCOM was pervasive as a form of communications across the battlefield. The SFOD-As and CIA operatives fighting alongside the Northern Alliance in Afghanistan utilized SATCOM to coordinate the efforts of their intricate bombing campaign with major ground offensives.[36] Using man-portable radios on their backs, US forces sent messages via satellites to their headquarters located on the other side of the globe. This space-based technology was undoubtedly a combat multiplier across the offensive in northern Afghanistan, as it directly supported decentralized operations with near-instantaneous global connectivity to execute a precision bombing campaign, once again validating technology in a combat laboratory via SOF.

In Iraq, the invasion also required constant communications to coordinate Operation Viking Hammer. SATCOM allowed US forces to coordinate the efforts of an intricate bombing campaign with the unconventional war they were waging on the ground.[37] SATCOM enabled small and isolated units to coordinate their efforts and synchronize combat power. It also allowed for greater geographic dispersion of forces across the battlefield, which proved vital as the United States invaded Iraq. During the invasions of both Afghanistan and Iraq, SATCOM enabled decentralized, lethal, and precise operations that minimized friendly casualties and helped define the new American way of war. The value of SATCOM and the operations it fostered was evident to leaders at the highest level thanks to an accidental RPL, with SOF leading the way.

Today, SOF continue to fill the role of an RPL for emerging technology across the globe. This has increasingly become the case as US operations have become more decentralized, with SOF often in the lead, facing technologically savvy enemies and adversaries, from extremist organizations with drones to near-peer competitors waging electronic warfare. SOF's value in the process of developing, testing, and fielding innovative and emerging technology has only increased in recent years.

While drones and unmanned aerial vehicles (UAVs) have played a key role in the last two decades of conflict across the globe, until recently, they consisted mostly of large drones used to drop munitions on remote targets or observe the battlefield. However, drone technology has improved, miniaturized, and become more pervasive across the globe, as have the threats posed by UAVs. As a result, US adversaries and

enemies use commercial off-the-shelf UAVs to disrupt and attack US forces in remote corners of the globe. Typically, the forces facing these threats are SOF.

The emerging threat from UAVs has created a demand for counter-UAV (CUAV) technology to enable military and law-enforcement personnel to defeat UAV threats. Consequently, the market is flooded with CUAV solutions. While the companies touting these wares attest to their value and effectiveness, the testing is all limited to controlled scenarios often lacking real-world variables (meaning field experiments only). However, for the SOF units in Afghanistan, Syria, and elsewhere facing these threats, the threat is real and must be defeated. This paradigm has created a perfect SOF RPL, with units on the battlefield fielding and testing CUAV equipment, attesting to the validity of said equipment, and ordering more of the successful systems and avoiding the ineffective or overly expensive technological blunders. Meanwhile, large organizations such as Special Operations Command (SOCOM) or the Asymmetric Warfare Group (AWG) oversee the procurement of systems and programs of record to counter this threat. To conceptualize this with an earlier example, SOCOM and AWG are the light on top of the Christmas tree, guiding the overall process. The SOF detachments, on the other hand, are the Christmas lights strung around the tree, facing the threat and driving innovation toward the correct solution—an SOF RPL.

However, the CUAV example is missing an important piece of the model we developed. While there is an adequate amount of experimentation in the innovation of CUAV solutions, it needs to be tied into PME—into field experimentation shepherded by SOF professionals as part of their academic professional development. ATAK represents one such example. The ATAK is an Android-based operating system installed on tablets, cell phones, and other handheld devices that provides real-time awareness on the modern battlefield, fosters communication, leverages SATCOM, and uses GPS technology. It has proven to be an invaluable tool for SOF across the globe. Interestingly, given the ATAK's success and value, many SOF officers have looked to its further development, testing, and implementation while attending PME. Two such examples include supporting the development of remote advise-and-assist ATAKs for partner forces separated geographically from their American SOF advisors and ways to tie the ATAK better into joint-operations centers.[38]

Taking it one step further, the same SOF students have since completed PME and are now using the devices they helped improve on the battlefield, completing the cycle of innovation. The innovation and integration of the ATAK by SOF professionals—both on the battlefield and during PME—is an example of a successful SOF RPL that has supported combat success directly, from testing to field experimentation and natural experimentation.

Conclusions

We can now return to the Defense Innovation Board's recommendations and highlight the specific ways in which our proposed initiative satisfies their key points:

> *Test various possibilities of employing different practices to* ***seek out empirical evidence****, . . . [to be]* ***rapid, iterative, and risk-tolerant****. Instead of giving processes pride of place . . . focus on outcomes, and how to get there most* ***efficiently****. These practices should be generalized, and* ***not only to products and services, but potentially to strategies and operations as well***[39] *(emphasis added).*

By using SOF as the laboratory for rapid prototyping, our proposal leverages the military community most comfortable with the necessary rapidity, cognitive flexibility, and risk tolerance. Marrying the SOF laboratory with PME research teams produces gains in efficiency, as well as the required analytic rigor for valid empirical testing. Finally, these operators and military graduate students are fully capable of applying these techniques to endogenize strategic and operational concepts, not just the technological "shiny objects" that take precedent in most discussions around innovation.

Endnotes

1 Atkinson, Robert D., and Caleb Foote. "Is China Catching Up to the United States in Innovation?" *Information Technology and Innovation Foundation*, 2019, http://www2.itif.org/2019-china-catching-up-innovation.pdf.

2 Harrison, Adam Jay, Bharat Rao, and Bala Mulloth. 2018-19. "Innovation Tradecraft: Sustaining Technological Advantage in the Future Army." 48 (4):45-52.

3 This argument is developed further in Blanken, Leo, Philip Swintek, and Justin Davis. 2020. "Special Operations as an Innovation Laboratory." *War on the Rocks*. https://warontherocks.com/2020/02/special-operations-as-an-innovation-laboratory/.

4 Zachary, G. Pascal. 1999. *Endless Frontier: Vannevar Bush, Engineer of the American Century*. Cambridge, MA: The MIT Press.

5 Coletta, Damon V. 2016. *Courting Science: Securing the Foundation for a Second American Century*. Stanford: Stanford University Press.

6 Thomas, William. 2015. Rational Action: *The Sciences of Policy in Britain and America, 1940-1960*. Cambridge, MA: The MIT Press; Wolfe, Audra. 2013. *Competing with the Soviets: Science, Technology, and the State in Cold War America*. Baltimore: Johns Hopkins University Press.

7 Tomes, Robert R. 2007. *US Defense Strategy from Vietnam to Operation Iraqi Freedom: Innovation and the New American Way of War,* 1973–2003. New York: Routledge.

8 Blanken, Leo J., and Justin Overbaugh. 2013. "Are we Assuming the Worst about Assumptions? Induction, Deduction, and Military Intelligence in Counterinsurgency." *Inteligencia y Seguridad* 13 (January-June): 193-220.

9 Ruttan, Vernon W. 2006. *Is War Necessary for Economic Growth?* New York: Oxford University Press.

10 Wolfe, Audra. 2018. *Freedom's Laboratory: The Cold War Struggle for the Soul of Science*. Baltimore: Johns Hopkins University Press.

11 Pedlow, Gregory W. 2018. "The Development of NATO Defense Plans for Central Europe in the Last Decades of the Cold War," in D. Kruger and V. Bausch, (eds) *Fulda Gap: Battlefield of the Cold War Alliances*. Lanham, MD: Lexington.

12 Coletta, Damon V. 2017-18. "Navigating the Third Offset Strategy." *Parameters* 47 (4):47-62.

13 Cancian, Mark F. 2019. The US Military Forces in FY2020: The Struggle to Align Forces with Strategy. *CSIS Briefs*. https://www.csis.org/analysis/us-military-forces-fy-2020-struggle-align-forces-strategy.

14 The US Department of Defense funded 36 percent of global research and development in 1960. In 2016, that number had fallen to 3.7 percent. See Sargent, John F., Marcy E. Gallo, and Moshe Schwartz. *Global Research and Development Landscape and Implications for the Department of Defense*. Washington DC: Congressional Research Service, 2018.

15 Carter, William. 2018. Statement Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities "Chinese Advances in Emerging Technologies and their Implications for US National Security". *Center for Strategic and International Studies*. https://docs.house.gov/meetings/AS/AS26/20180109/106756/HHRG-115-AS26-Wstate-CarterW-20180109.pdf

16 Defense Innovation Board. 2019. "Recommendations." https://innovation.defense.gov/Recommendations/.

17 Kozloski, Robert. 2017. "The Path to Prototype Warfare." *War on the Rocks*. https://warontherocks.com/2017/07/the-path-to-prototype-warfare/.

18 Whitmarsh, Toby, and David Arnel. 2019. If You Are Not First You Are Last: Gaining an Adaptive Edge through Rapid Prototype Warfare. *War Room*. https://warroom.armywarcollege.edu/articles/if-you-are-not-first-you-are-last-gaining-an-adaptive-edge-through-prototype-warfare/.

19 Carleton-Smith, Mark. 2018. "New British Way of War." *Global Defence*. http://edition.pagesuite-professional.co.uk/html5/reader/production/default.aspx?pubname=&edid=fc50d232-0df5-4759-bfaa-05e5761e5701.

20 Gerber, Alan S., and Donald P. Green. 2012. *Field Experiments: Design, Analysis, and Interpretation*. New York: W.W. Norton and Co.

21 Kapiszewski, Diana, Lauren M. Maclean, and Benjamin L. Read. 2015. *Field Research in Political Science: Practices and Principles*. New York: Cambridge University Press.

22 Dunning, Thad. 2012. *Natural Experiments in the Social Sciences: A Design-Based Approach*. New York: Cambridge University Press.

23 Losee, John. 1993. *A Historical Introduction to the Philosophy of Science*. Vol. Third. London: Oxford University Press.

24 Dyson, Tom. 2019. "The Military as a Learning Organization: Establishing the Fundamentals of Best-Practice in Lessons-Learned." *Defence Studies* 19 (2):107-129.

25 Hasselbladh, Hans, and Karl Yden. 2019. Why Military Organizations are Cautious About Learning? *Armed Forces and Society*. https://journals.sagepub.com/doi/abs/10.1177/0095327X19832058.

26 Blanken, Leo J., and Justin Overbaugh. 2013. "Are we Assuming the Worst about Assumptions? Induction, Deduction, and Military Intelligence in Counterinsurgency." *Inteligencia y Seguridad* 13 (January-June): 193-220.

27 Tucker, David, and Christopher Lamb. 2007. *United States Special Operations Forces*. New York: Columbia University Press.

28 Mulhern, Brian G. 2014. "Risky Business: Risk Tolerance in US Army Special Forces." Master's thesis, Naval Postgraduate School. https://calhoun.nps.edu/bitstream/handle/10945/42694/14Jun_Mulhern_Brian.pdf?sequence=1&isAllowed=y

29 See Kulczycki and Hampton chapter in this volume.

30 Tran, Thang, Michael Oliveira, Josh Sider, and Leo Blanken. 2018. "Ignorance and Professional Military Education: The Case for Operational Engagement." *War on the Rocks*. https://warontherocks.com/2018/11/ignorance-and-professional-military-education-the-case-for-operational-engagement/.

31 Jerry J. Sellers, *Understanding Space: An Introduction to Astronautics*, ed. Douglas H. Kirkpatrick (New York: McGraw Hill, 2005), 31.

32 Linda Robinson, *Masters of Chaos: The Secret History of the Special Forces*, (New York: Public Affairs, 2004), 63.

33 "Evolution of GPS: From Desert Strom to Today's Users," Space and Missile Systems Center, March 24, 2016, https://www.af.mil/News/Article-Display/Article/703894/evolution-of-gps-from-desert-storm-to-todays-users/.

34 Robinson, Linda. *Masters of Chaos: The Secret History of the Special Forces*. New York: Public Affairs, 2004; Gary C. Schroen, *First In: An Insider's Account of How the CIA Spearheaded the War on Terror in Afghanistan*, (New York: Random House, 2005), 112.

35 Spencer C. Tucker, ed., *US Conflicts in the 21st Century, Afghanistan War, Iraq War, and the War on Terror*, (Santa Barbara: ABC-CLIO, 2016), 959.

36 Schroen, Gary C. *First In: An Insider's Account of How the CIA Spearheaded the War on Terror in Afghanistan*. New York: Random House, 2005.

37 Tucker, Spencer C, editor. *US Conflicts in the 21st Century, Afghanistan War, Iraq War, and the War on Terror*. Santa Barbara: ABC-CLIO, 2016.

38 Bandy, Daniel W., Eric A. Mitchell, Aaron L. Goldan, Jay D. Parsons. 2018. "Joint Operations Center Tactical Assault Kit: Evolution Toward Scalable Multilateral SOF C4I." Master's thesis, Naval Postgraduate School. https://calhoun.nps.edu/handle/10945/61230.

39 Defense Innovation Board. 2019. "Recommendations." https://innovation.defense.gov/Recommendations/.

SECTION 5

DIGITAL DOMAINS: THE SOF ROLE

CHAPTER 24

Special Operations Forces and Cyber-Enabled Influence Operations

Herbert Lin and Trisha E. Wyman

Introduction

This chapter focuses on opportunities for influence operations in a rapidly changing and disruptive information environment, in which both US special operations forces (SOF) and enemy forces have increased access to both global populations and systems and a variety of cyber tools to facilitate and enhance such operations. SOF are the readied forces—adaptable, small, and capable of sensitive operations—and have a long history of achieving influence in the information environment. Historically, SOF have pioneered the successful navigation and operation of the most technologically advanced systems and methods, their future should be no different.

In the future, cyber-enabled influence operations (CEIO) will be integral to the success of efforts to influence, recruit, and engage people, systems, and forces around the world. To do so, they must take advantage of insights from social and cognitive psychology, marketing, social media, and the arts of influence and persuasion (as commercial and enemy entities have done). They must also employ technological capabilities that shape and manipulate hardware and software infrastructures to improve US SOF access to denied areas and marginalized populations.

A Special Operations Framing for Influence Operations

US SOF operate in a rapidly evolving and contested information environment that requires learning from previous experience, adaptation, and an understanding of peer nation-state activities, commercial competitors, and opportunities for cyber-enabled influence operations. This chapter is concerned with influence operations, and adopts a definition of influence operations inspired by that of psychological operations contained in several Department of Defense (DOD) publications. DOD regards psychological-operations soldiers as its primary influence-focused force.[1] Furthermore, this chapter presents influence concepts that can and should be considered for use by, and could be used against, US SOF operations.

US SOF operate primarily in small teams and in sensitive and hostile environments in which signature management and social engineering may be required for mission success. Furthermore, although employed throughout all levels and phases of conflict and throughout the full range of military operations, US SOF are often the first forces employed both to create favorable environmental conditions and in crisis operations.[2] Influence operations provide US SOF opportunities for improving signature management, socially engineering audience and local perceptions, and promoting US SOF objectives.

The concepts discussed in this chapter are applicable not only for US special operations but also to understand the opportunities available for nation-state competitors to target US forces and audiences. Peer competitors actively use cyber-enabled influence operations to target US SOF, conventional US forces, and other US audiences. They spread their influence efforts across varying internet platforms, addressing various military exercises and operations, and target groups and individuals. Russia, for example, has demonstrated its capability and inclination to use entities such as the Internet Research Agency to plan and execute influence operations using social media and human networks to encourage activities and attitudes favorable to its national goals.[3] Russian media has shared falsehoods about SOF activities and their real intent. For example, citing an article on a Russian website, the *New York Times* reported on a false Russian claim that the Ukrainian government had issued US service members Ukrainian passports, the possession of which would allow American forces to infiltrate Russia. The article was shared over multiple Russian social media platforms, according to American officials.[4] China views Russia's robust media effort as a success, which is reflected in the increase in China's development and funding of its media efforts.[5] Both countries have employed internet influence measures and clickbait to garner attention to their content.[6]

Influence Operations and SOF Missions

This chapter regards influence operations as activities designed to convey to a target audience (whose size may be as small as a single individual) both information and indicators selected for their potential to influence emotions, motives, objective reasoning, attitudes, understanding, beliefs, or behavior in ways that advance the interests of the operator.[i]

Influence operations can be conducted throughout all phases of conflict, from the prewar phase to a postwar phase. They may be aimed at friendly, neutral, and adversary audiences to publicize the beneficial reforms and programs to be implemented after defeat of the adversary; to instill and sustain popular belief in and support for US and multinational political systems (including ideology and infrastructure) and associated political, social, and economic programs; to explain US policies, aims, and objectives; to amplify economic sanctions or other social or political action taken against an adversary; to shape foreign public opinion; or to increase the psychological impact of US and multinational combat power.

All military activities are ultimately intended to influence adversary behavior. However, if such activities are not planned and executed specifically to convey such

i This list of desired effects is derived from both the current DOD definition of military support operations (Joint Publication 3-13.2, Military Information Support Operations, Washington, D.C. 2014, II-6.) and an earlier DOD definition of psychological operations promulgated in 1984 (http://documents.theblackvault.com/documents/psyops/OvertPsyOps.pdf) as "planned political, economic, military, and ideological activities directed toward foreign countries, organizations, and individuals in order to create emotion, attitudes, understanding, beliefs, or behavior favorable to the achievement of US political and military objectives." JP 3-13.2 Military Information Support Operations, 2011, page vii; also see JP3-13 Information Operations, 2014, II-9.

information or indicators to influence the perceptions and the subsequent behavior of a target audience, they do not constitute influence operations in the lexicon of this chapter.[7]

Influence operations may be declared truthfully, undeclared, or declared falsely.[ii] Truthfully declared influence operations identify the originator clearly and correctly, so that an influence operation publicly associated with Nation A is in fact conducted by Nation A. Undeclared influence operations are not publicly associated with any actor at all. Nation A may originate an influence operation, but if the operation is gray, it does not identify a national actor. Falsely declared influence operations—also known as false-flag operations—are associated publicly with a nation or actor other than that of the true operator, so that an influence operation appearing to be publicly associated with Nation B will in fact have been conducted by Nation A.

Influence operations act as force multipliers that use nonviolent means in often violent environments.[8] They seek to persuade rather than to compel, using logic, fear, desire, or other mental factors to promote specific emotions, attitudes, or behaviors. Many influence operations take advantage of local knowledge about political, cultural, ethnic, and religious factors at play in target audiences to influence perceptions and facilitate desired behavior.[9]

Target audiences for influence operations may consist of governments, organizations, groups, or individuals. The size of the audiences can vary, ranging from entire national populations, geographically delimited populations, specific demographic groups, audience leaders, or social media influencers. In cases in which an audience may view the US government as a suspicious source of information, SOF operators may have to rely on (and, thus, must cultivate) trusted local sources to deliver the same information, possibly to greater effect.

Influence operations can be used to induce adversaries to take (or fail to take) specific actions that will advantage the originator and/or disadvantage the adversary. Influence operations may seek to reinforce the adversary's preconceived (though inaccurate or incomplete) beliefs,[iii] focus the adversary's attention on unimportant activities so that important activities go unnoticed, create the illusion of strength where weakness exists, overload the adversary's information collection and analytical capabilities, or reduce the adversary's situational awareness.

The act of providing truthful and contextually accurate information to inform target populations is an influence operation. Influence operations to inform are serious, thoughtful, and balanced attempts to change hearts and minds and are not intended to be disingenuous. As far as is possible, they are unbiased, unslanted, and not misleading. Most important, the intent of an attempt to inform is to enable target

ii These definitions correspond roughly to DOD doctrine distinguishing between white, gray, or black operations. See Appendix A, FM 3-05.30, Psychological Operations, Army Field Manual, 2005, https://fas.org/irp/doddir/army/fm3-05-30.pdf.

iii Magruder's principle states that it is generally easier to induce an enemy to maintain a preexisting belief than to present notional evidence to change that belief. Thus, under many circumstances it is more useful to examine how an enemy's existing beliefs can be turned to advantage than to attempt to change his or her beliefs. See FM 90-2 BATTLEFIELD DECEPTION, 1988.

audiences to reach their own conclusions, as opposed to the conclusions desired by another party. (Of course, other parties—for example, adversaries competing for the loyalties of the same target population—may view such operations as misleading, unbalanced, biased, or slanted.)

The definition provided above for influence operations emphasizes *selected* information and indicators. Such information—which may be mostly false, mostly true, or some mix of the two—may be selected for reasons other than its potential for contributing to a fair, balanced, or objective presentation in which the audience can decide for itself. Thus, a host of other possible purposes for influence operations exist, including:

- **Operations to distract,** which seek to shift the attention of a target audience to another topic, entity, or issue and can be used to bury unfavorable information.
- **Operations to overwhelm,** which seek to spread the attention of the target audience to many focal points; taken together, the disparate foci serve a similar purpose to that of jamming operations in electronic warfare that increase noise and lower the signalø-to-noise ratio, making detection of real targets more difficult. Such operations may make use of multiple, mutually inconsistent narratives and ideas. Such inconsistency is not necessarily a disadvantage, as different segments of a large target audience may gravitate toward one idea or another, potentially generating confusion and disorientation in the overall target audience.
- **Operations to mislead,** which seek to introduce additional information into the environment. Such information may be entirely false, partially misleading or slanted, or entirely unfalsifiable (i.e., opinion that seems to be fact, either superficially or overtly). Such operations can be used to introduce alternative narratives or interpretations that are more favorable for the operator than others already in circulation.
- **Operations to provoke and outrage,** which seek to evoke or amplify emotional responses in the target audience to events or conditions. An audience in such a state is manipulated to take action they might not otherwise consider in their interests.

Often, influence operations use assets and resources indigenous to the operational environment,[10] including local broadcast and print media, as well as social media and other computer-based communications mechanisms. The use of such assets may help to facilitate credibility of the indigenous government, allies, and other agencies.

In a given geographical region, influence operations conducted by SOF may focus on a variety of tasks.[11] To be optimally effective, these tasks also require synchronization and coordination with the activities of joint, interagency, civil,

and foreign partners, such as military-civil affairs units, the State Department, local nongovernmental organizations, and foreign governments. For friendly or neutral audiences in denied areas, influence operations may seek to improve access to accurate and timely information about past and present circumstances. When successful, such operations build support from the local populace. If such audiences are disorganized or isolated physically or psychologically, influence operations may be able to provide useful guidance, instructions, or reassurance. For example, they may help to sustain or boost the morale of friendly resistance fighters. They may also mobilize popular support for US and multinational military operations or encourage empathy between friendly host-nation armed forces and the civilian populace.

For adversary audiences, influence operations can be used to diminish morale, reduce their will to resist, or give them alternatives to continued conflict. For ostensibly neutral audiences skeptical of US motives, influence operations may seek to reduce tensions by instilling favorable or positive views of the United States or its indigenous partner. As part of ongoing military actions against adversary forces, influence operations can also support deception or the exploitation of ethnic, cultural, religious, or economic differences in ways that cause confusion or hostility among rival adversary factions. Influence operations may be conducted to lower the morale of or diminish local support for adversary forces, undermine confidence in adversary leadership, counter information disseminated by adversaries, or attack the legitimacy of adversary political systems.

The Complexities of the Current and Emerging Information Environment

The information environment—which consists of the individuals, organizations, and systems that collect, process, disseminate, or act on information—has evolved rapidly over the last few decades providing increased interconnectedness and ease of influence.[12] This environment has three dimensions:

- **Physical:** consisting of command-and-control systems and supporting infrastructure and roughly corresponding to cyberspace hardware (e.g., computers and network technology interconnected through the internet).
- **Informational:** consisting of where and how information is collected, processed, stored, disseminated, and protected and roughly corresponding to the information carried and stored within cyberspace.
- **Cognitive:** encompassing the thinking minds and feeling hearts of those who transmit, receive, respond to, and act on information.[iv]

iv The DOD definition of "cognitive" dimension does not explicitly account for affect, making reference only to "minds." But because how people feel affects how they receive, respond to, and act on information, we will use "cognitive dimension" to include both thought and affect. For simplicity, we will refer to the cognitive dimension while intending to encompass both cognition and emotion.

Two examples can illustrate how the rapidly changing information environment may affect SOF operations. The first example is the increasingly popular Fitbit, a wearable device that tracks the physical activity (e.g., running) of a user and can monitor the user's location in real time through the use of GPS. Such information can be uploaded to sites and shared with others, allowing for the aggregation of many users location profiles. In 2018, a private citizen noticed that a public-facing global map of all Fitbit users choosing to share their location information showed the locations of Fitbit-using active-duty military personnel on deployment,[13] revealing US deployments abroad that were not widely known. Some commentators raised concerns that specific individuals could be associated with various deployments[14] to the obvious detriment of operational security.

Second, electronically mediated gaming, an activity with which tens of millions of people worldwide engage voluntarily and avidly and which is expected to increase in popularity,[15] will provide previously unimagined opportunities to engage with target audiences. Various technological developments, from the deployments of 5G wireless technology to increased visual and audio fidelity and low-latency responses, haptic technologies that provide tactile inputs, and AI-driven image and audio creation, will increase the realism of the immersive experience. Consider, then, the utility of high-fidelity, multisensory gaming as a way to gain the attention of certain target audiences, providing channels through which influence of various kinds may be exercised.

The nature of cyberspace is also changing rapidly. Nations around the world, and nonstate actors in some cases, seek greater degrees of sovereign control over their own cyberspace. For example, Russia is endeavoring to build an internet that can be disconnected from the global internet at times the Russian government deems appropriate.[16] China's "Great Firewall"—and its associated practices of preventing certain foreign sources from delivering internet content to China—is well-known as an element of China's assertion of cyber-sovereignty.[17] India shuts down the internet, at least regionally, with some frequency—in 2019, India experienced at least 95 such shutdowns.[18] Since the majority of such nations and nonstate actors are authoritarian rather than democratic,[v] there will be growth in the number and size of areas that are denied both physically and in cyberspace. Operating effectively in such areas will require US SOF to understand the systems and processes in play and will demand SOF expertise in penetration and unconventional warfare.

The cognitive dimension is where human judgment and perception apply information and where people process, react to, and make decisions based on information. Modern marketing and advertising techniques for shaping audience perception go beyond the use of audio and visual selectors and indicators. Indeed, all

v Freedom House produces an annual ranking of the world's nations according to its judgments of "internet freedom," a composite index that account for internet access, freedom of online expression, and privacy issues on the internet. In the 2019 report (Freedom House, *Freedom on the Net*, 2019), this ranking can be found on page 24-25, and a causal perusal will show that nations with the lowest internet freedom scores tend to be those with authoritarian governments.

sensory perception should be considered as influencing the cognitive domain. Modern-day advertisers and marketers purposely activate touch, smell, and auditory signals to shape audience perception of a situation or product.[19] In a real-world example, Dunkin' Donuts used coffee scent on buses in Seoul, South Korea, in concert with visual marketing, resulting in a 16 percent increase in attendance at Dunkin' Donuts stores near bus stations and a 29 percent increase in coffee sales.[20]

The Psychology of Influence Operations

Highly effective influence operations often take advantage of human psychological factors that have remained relatively unchanged for millennia. This section discusses three critical factors in understanding the psychology of influence operations: social identity, cognitive economy, and dual-system cognition. We then apply these factors to the process of narrative and perception development. The impact of these factors on societal interaction, discourse, persuasion, and decision-making have been studied widely.[21]

Cognitive Economy

Cognitive economy refers to the inherently limited human cognitive-processing capability. For example, the number of unrelated items that human beings can remember for a short period of time is finite. Thus, when individuals are under time pressure to make decisions, they often select the first satisfactory solution rather than the optimal (best possible) one.[vi] People can "use up" the resources needed for thoughtful and deliberate decision-making; thus, their capability for such decision-making in a limited time is restricted.

The finiteness of a person's cognitive resources has profound implications for how people approach decision-making tasks that involve information processing. The phrase "cognitive miser" has often been used to describe human beings who preferentially operate in accord with a principle that might be called "cognitive economy"—the use of thinking strategies that minimize the effort used in performing mental tasks so cognitive resources are conserved.[22]

Dual-System Cognitive Theory

A preference for low-effort thought does not mean that humans can only engage in such thought. Dual-system cognitive theory posits the existence of some thinking

vi The tendency to choose satisfactory solutions in favor of optimal ones is known as "satisficing" and was the subject of two papers by Herbert Simon ("A Behavioral Model of Rational Choice," *Quarterly Journal of Economics* 69 (1955): 99–118; "Rational Choice and the Structure of the Environment" Psychological Review (1956) 63: 129–138). The resulting theory of "bounded rationality" was the basis for Simon's 1978 Nobel Prize in Economics. Simon described the contrast between optimizing and satisficing as the difference between "looking for the sharpest needle in the haystack" (optimizing) and "looking for a needle sharp enough to sew with" (satisficing) (Simon H. A. "Satisficing." In New Palgrave: A Dictionary of Economics, Eatwell J., Millgate M., Newman P., eds., Vol. 4: Stockton Press: New York; 243–245, 1987). For an interesting example of decision-making under extreme time pressure, see Hannah Oh, et al, "Satisficing in Split-Second Decision-Making Is Characterized by Strategic Cue Discounting" (Journal of Experimental Psychology: Learning, Memory, and Cognition, 42(12):1937-1956, 2016, https://doi-org.stanford.idm.oclc.org/10.1037/xlm0000284.)

strategies that operate at low cognitive cost and others that operate at higher cost. The low-cost system—often known as System 1—is a fast, intuitive, reflexive, and emotionally driven mode of thought. The higher-cost system—often known as System 2—reflects a slower, more deliberate, analytical mode of thought.[23]

Known by a variety of names in the psychological literature—spontaneous, heuristic, peripheral, reflexive, and intuitive— System 1 thinking is implicit, unconscious, "from the gut," and responsive to visual and other perceptual cues. It is based on principles (called heuristics) highly suited for making quick judgments and snap decisions.[24] (An example of such a heuristic is that loud noise signifies immediate danger.) Most important, System 1 thinking is the way human beings process information under most circumstances, and it is always operative (that is, it is never not functioning).

For most situations that people encounter in everyday life, System 1 thinking is mostly adequate to produce outcomes that are good enough for everyday use. But it tends to be inadequate when situations call for complex inferences or deep understanding of nuance and subtlety. For such situations, System 2 thinking is more often useful, even though it is generally effortful, consumes cognitive resources, and operates relatively slowly. Known by a number of different terms in the psychological literature—central, systematic, deliberate, and analytical—System 2 thinking involves a variety of thought processes associated with formal logic, reasoning and rationality, symbolic abstraction, serial rule-based processing, and language and conscious thought. System 2 thinking is slower but tends to be less prone to error than System 1.

Reliance on heuristic thinking is not a tendency limited to less educated or less intelligent individuals. All people—regardless of level of education, intelligence, profession, or political persuasion—rely on such thinking to some degree, to their detriment under some circumstances. Consider the profession of intelligence analysis, which has been defined as "the process by which the information collected about an enemy is used to answer tactical questions about current operations or to predict future behavior."[25] Richard Heuer's now classic 1999 volume on the psychology of intelligence analysis[26] makes the point forcefully that intelligence failures are often not the result of inadequate or incomplete information but rather faulty "going-in" assumptions about the situation under review—assumptions that can and are often driven by heuristic thinking. Such assumptions frame the mental model within which the analyst places various pieces of information and the logic with which these pieces relate to each other. Faulty assumptions often yield unreliable conclusions.

Social Identity

Human beings are social, and social identity—that is, one's identity as a member of one or more groups—is important to most individuals. People form groups on the basis of similarities with others (a phenomenon known as homophily). Such similarities may include ethnicity, gender, age, religion, social class, employment

status, geography, or political party. They may also include personal beliefs, values, attitudes, and aspirations, such as moral values, shared recreational activities, and attitudes toward sexual activity. People in groups are highly motivated to establish a shared reality to validate their identity and experiences, and that shared reality may well include shared attitudes, feelings, and emotions.[27]

A person's sense of group identity can be threatened by information that contradicts or casts doubt on any important aspect of that group's shared reality. Such information is likely to activate identity-protective psychological mechanisms. Such mechanisms typically involve the rejection of threatening information, by ignoring, disbelieving, or discrediting it, or by finding error in it. Most importantly, the invocation of these mechanisms is not necessarily (or even often) conscious.

One particularly powerful method for rejecting threatening information has been described as motivated reasoning,[28] which refers to a person's desire to reach a particular conclusion. When engaged in motivated reasoning, people choose a selective set of cognitive processes for strategies for accessing, constructing, and evaluating beliefs, and they search their memory for beliefs, rules, and knowledge to support their desired conclusions. That is, they are likely to be rationalizing a conclusion (via System 2 thinking) that may have emerged from System 1.

Narrative, Framing, and Perception Management

Humans use narratives and stories to understand and explain the actions of others in the groups of which they are a part.[29] How a narrative is framed strongly influences how people perceive events—a person walking on water can be praised for her miraculous skills and talent (a positive framing) or criticized for not being able to swim (a negative framing). Framing depends on cultural, societal, and psychological factors that may vary from audience to audience,[30] and the ability to frame a narrative in favorable terms is an enormous advantage in shaping the perceptions of an adversary.

An example of using psychological biases in framing narratives is the exploitation of the "availability heuristic" in social media. The availability heuristic is a cognitive shortcut that relies on the ease with which information can be accessed as an indicator of the significance or importance of that information.[31] Consistent with the use of this heuristic, surveys indicate most people read only headlines of online media postings prior to sharing the content.[32] Accordingly, malign actors often use headlines to induce unwitting users to click on, forward, or share misleading information.

The leaks to the public of emails from John Podesta, director for Hillary Clinton's 2016 presidential campaign demonstrate the use of the availability heuristic. Over the one-month period of October 2016, Wikileaks released publicly 33 tranches of Podesta's private emails, which had been stolen by the GRU intelligence service of the Russian armed forces.[33] The periodic release of these tranches enable Russian influencers to keep the emails in front of the American public for an extended period of time, thus crowding out, or at least competing with, coverage of other election-

related stories. The release also helped to shape a negatively tinged narrative about Clinton's candidacy.

Cyber Tools for Cyber-Enabled Influence Operations

Cyber-enabled influence operations are those conducted with or supported by cyber tools. Such cyber tools fall into two categories: those accessible to the general public and that can be used legally (e.g., Facebook or Google; called Category 1 cyber tools for the purposes of this chapter), and those that the public cannot use legally (e.g., hacking tools used to conduct cyberattacks; Category 2) and which actors generally use clandestinely.

Influence Operations Enabled by Category 1 Cyber Tools

The modern information technology (IT) infrastructure—including the internet, the availability of virtually all internet applications on mobile devices, and broadband services adequately equiped to carry audio and visual traffic—and IT-based applications—including, but not limited to, social media, search engines, and data mining—can be used to extend the reach and effectiveness of influence operations in ways unimaginable before the advent of the internet and personalized computing. We labelInfluence operations enhanced in such a manner "cyber-enabled influence operations" (CEIOs).

CEIOs take advantage of Category 1 cyber tools in the information environment, an environment that is loud and chaotic with large amounts of information being transmitted at high speeds. People encounter increasingly more information and have less time to process it. Thus, as the principle of cognitive economy would suggest, people go into cognitive overload and increase their reliance on intuitive processing.

Moreover, many internet-based applications and internet business models have features and characteristics that can be exploited by those seeking to leverage System 1 processing to pursue an influence campaign. For example:

- Search engines return highly visible results for queries based in large part on the popularity of those results and the algorithmically inferred desires of the user for specific information rather than their factual relevance to those queries,thus playing to confirmation bias[vii] based in System 1.[34]
- Search engine optimization (SEO) techniques enable search algorithms to be manipulated to enhance the visibility of false, misleading, or worthless information.
- The internet hosts numerous content providers that supply information to willing and receptive users. These providers may be single individuals or automated bots, government agencies, large media companies, and everything in between. As important, these providers are mostly free to

vii Confirmation bias: when a person seeks or interprets "evidence in ways that are partial to existing beliefs, expectations, or a hypothesis in hand" (Nickerson).

distribute whatever information they wish. Because of the heterogeneous nature of these providers, people can find support for virtually any point of view or idea, no matter how outlandish or irrational.

- Affinity groups with substantial public reach can be created easily in today's information environment. Modern cyber tools also allow individuals to find others who have similar points of view easily, which facilitates the rapid growth of groups of like-minded individuals. Therefore, once societally marginalized views can now find expression and voice in easily accesible online groups and, by extension, can be mainstreamed into society at large.
- Groups of like-minded individuals often recirculate their views in echo chambers. People are more likely to believe information circulating in their affinity groups because access to such information is more readily available,[35] even if the same message comes from (apparently) different sources from within the group. This conclusion is worrisome in light of the finding that false information tends to come back multiple times after the initial publication on social media; true information does not.[36] Although this study did not focus on repetition on social media as a whole rather than within specific groups, it seems reasonable to suggest a greater exposure to false information would characterize the information flows within affinity groups—and thus that false information is more reinforced.
- Video imagery is much more emotionally evocative than text, and social media such as YouTube and TikTok provide easy access to online video. Since anyone can publish a video on these platforms and make them accessible to any audience, such media channels provide may opportuntiies for emotional manipulation.
- Tablet devices and smartphones allow for immediate access to the internet, and media applications often notify individuals when new content is available. Because people are psychologically predisposed to seek novel inputs (a characteristic of System 1 thinking), they are likely to respond to such notifications. To increase ad revenue, media applications take advantage of such notifications to increase user engagement and continue the flow of incoming information.
- Tweets of 280-character messages do not allow for much nuance; indeed, they are ideally suited for the distribution of simplistic messages. Features such as "retweet" and "like" allow recipients to pass along the message (be it text or video) or their sentiments to wide audiences rapidly.

Perhaps most important from the perspective of nation-state adversaries, the physical borders of nations are highly permeable to information. Compared to controlling the entry of people and physical objects through national borders,

nations have to work hard to prevent the entry of information from outside. It is essentially impossible to be 100 percent successful at such prevention efforts. Internet-based companies trafficking in information of various kinds take advantage of border permeability to increase market sizes—and, thus, borders are a poor differentiator between foreign and domestic actors.

Influence Operations Enabled by Category 2 Cyber Tools

Category 2 cyber tools—that is, hacking tools—are used by adversaries to compromise IT-based products and services by taking advantage of vulnerabilities in their design, implementation, or configuration. Their use is generally regarded as the key element in what DOD describes as offensive cyberspace operations (OCO).[37] Certain kinds of OCOs can support, facilitate, and enhance influence operations (whether cyber-enabled or not) and may even be the primary means through which an influence operation is conducted.

As one example, *NPR* reported US Cyber Command (CYBERCOM) conducted a variety of offensive cyber operations under the rubric of Operation Glowing Symphony intended to degrade and disrupt online ISIS propaganda, communications, fundraising, and recruitment efforts.[38] According to *NPR*, much of this effort focused on creating an endless series of technology annoyances and time-wasting interruptions that degraded and disrupted the workflow of ISIS network operators significantly.

The NPR report referred to these activities as "psychological operations with a high-tech twist" because US CYBERCOM intended them to cause high levels of emotional frustration for ISIS operators. Indeed, the description of this event aligns with the definition of influence operations provided earlier: These operations conveyed to ISIS network and cyber operatives malware and other technology disruptions selected for their potential to cause frustration and anger, compromising ISIS operators' objective reasoning and reducing their efficiency and effectiveness in ways that advanced the interests of the United States.

Connections between Cyber-Enabled Influence Operations and Offensive Cyber Operations

In the wake of Russian interference in the 2016 US presidential election, Dick Cheney described the activity as an "act of war," while Hillary Clinton called it a "cyber 9/11."[39] But, although Russian actions clearly violated US sovereignty, they did not rise to the threshold of armed attack or a use of force against the United States. No one died; no property was destroyed. Russian interference did include the conduct of certain offensive cyber operations, but in retrospect, it appears that a substantial portion, if not the bulk, of Russian activities were influence operations aimed at various segments of the US populace.

OCOs target adversary computing and communications capabilities to destroy, damage, or disrupt those capabilities or other systems and processes dependent on

those capabilities. As such, the success of an OCO depends on the exploitation of vulnerabilities in the computer hardware and software and the system configurations that undergird those capabilities. Cyber tools that exploit such vulnerabilities are Category 2 cyber tools.

Influence operations—even if cyber-enabled—do not conform to this understanding, except perhaps incidentally. As noted previously, influence operations are designed to convey specific information to target audiences. That is, they target *human* audiences. While Russian hackers did manage to penetrate the private email accounts of Democratic National Committee campaign officials in 2016, the damage came not from the hacking itself but from the coordinated release and amplification of formerly private emails. Both were part of a Russian influence operation using cyber tools to influence the emotions, motives, objective reasoning, attitudes, understanding, beliefs, or behavior of American citizens.[40] Russia used social media cyber tools *exactly as they were intended to be used* to achieve psychological and behavioral effects in the targeted population. Where OCOs relate to hacking into machines, CEIOs concern the hacking of human minds. CEIOs take advantage of Category 1 cyber tools.

However, we do not mean to imply CEIO and OCO have no similarities. They do have some high-level similarities akin to the similarities between ground and air combat. Just as ground and air combat allow nations to project power in physical space, OCOs and CEIOs project power using cyberspace. Both OCOs and CEIOs use digital technologies to accomplish their missions. Like all other aspects of foreign relations and international conflict, they both rely on good intelligence collection and analysis. But their similarities do not continue at lower levels of abstraction.

Moreover, there is no reason to suppose that Category 2 cyber tools and OCOs cannot support CEIOs. OCOs can be used to compromise the confidentiality, integrity, and availability of targeted computing resources and the information handled with such resources. Thus, they can extract information from or implant information in data-storage devices and communications channels; CEIOs can take advantage of information obtained in such a manner or use implanted information to help achieve their goals.

Importantly, CEIO can be a tool to influence audiences and shape favorable societal perceptions and conditions for future OCO. The Russian elections meddling proved to be at least partially successful in developing and disseminating a narrative via social networks, leading to social unrest, protest, polarization of audiences, and distrust in the political system. Although it may be some time before experts determine the full impact of Russia's meddling, an investigation of their activities is an opportunity to examine consequences and outcomes for CEIO as a long-term progression toward deliberately well-planned OCO.

How Cyber-Enabled Influence Operations Can Support SOF Missions

As noted previously, SOF operators often depend on the actions of indigenous parties to accomplish their missions. CEIOs can play important roles in persuading these other parties to act accordingly. We base the vignettes below on a set of examples of military information support operations provided in Joint Publication 3-13.2. Each vignette describes how CEIOs could contribute to these activities.

- **Influencing the development of adversary strategy and tactics.** An adversary government may employ tactics that, if widely known, would cause foreign or domestic blowback to its public image. CEIOs can be used to draw negative international or domestic attention to these tactics in ways that could result in condemnation and, thus, pressure the adversary to change its tactics. First-person reports of condemnation-worthy events in text and video carried over social media may be particularly effective for such purposes.
- **Amplifying economic and other nonviolent forms of sanctions against an adversary.** An adversary government may be propped up by corrupt or malicious commercial activities. CEIOs can be used to organize activities that damage these activities . For example, group communications enabled by social media and other communications applications can be used to organize strikes or boycotts against corrupt merchants.
- **Undermining confidence in adversary leadership and attacking the legitimacy and credibility of adversary political systems.** Discrediting a rigged election helps to undermine an adversary government, and CEIOs can play a role in doing so. For example, spreading rumors over social media may sow doubts in the population about its leadership. Social media is also well-suited for organizing protests and is better-suited than traditional media for maintaining the operational security that may be needed to go from organization to execution. Capitalizing on the idea that secret documents are often more believable than public documents, hack-and-leak operations combine OCO with CEIO, the former to obtain such documents and the latter to publicize them.
- **Countering hostile information activities.** Adversary information operations, often using social media networks, may be damaging to US interests. Most social media networks have key influencers that play outsize roles in determining information flows and content,41 and eliminating or compromising those influencers can impact network operations significantly. CEIOs can be used to discredit influencers, for example, by exposing unsavory histories.
- **Mobilizing popular support for US and multinational military operations.** Generating popular support for US operations usually requires a nuanced and subtle understanding of the political and social environment among

the relevant population, which may include tracking popular sentiment by monitoring important social networks (though not an influence operation, strictly speaking). Being tied into such networks also provides entry for CEIOs that can counter misleading adversary messages.

- **Gaining and sustaining popular belief in and support for US and multinational political systems and political, social, and economic programs.** To accomplish this task, the effectiveness of communications rhetorically hostile to the United States must be reduced. The conversational center of such groups can sometimes be shifted by determined actors, but such shifts are possible only slowly.
- **Shifting the loyalty of adversary forces and their supporters to friendly (or perhaps neutral) powers.** Provoking hostilities between two rival groups that are unfriendly to the United States can be one element of such a shift. CEIOs—especially falsely attributed ones—offer opportunities for false-flag operations delivered to each group implicating the other.

In the context of these vignettes, a few general considerations can be offered. First, many of the CEIOs described rely on the availability of trusted influencers. One approach to cultivating trusted influencers is for SOF to build personal relationships with them; such relationships require in-person presence and take a long time to develop.

SOF operators themselves can become trusted influencers in online social media networks. Such an outcome may be possible because online interaction does not require in-person interaction. On the other hand, working oneself into such a position requires infiltrating a group and the paitence to integrate oneself into the proceedings of that group by building followers and contributing to the group dialogue. If SOF operators can build such relationships and establish credibility, opportunities could arise for the SOF operators to engage the networks or individuals face-to-face.

SOF operators can also assume the identity of a trusted influencer. Such an approach would generally rely on OCOs directed at such an outcome, which would enable an SOF operator to impersonate the trusted influencer and also to prevent the person from recovering his or her online identity. Even if successful, the SOF impersonator will have to be wary of arousing suspicion and refrain from saying anything that is distinctly out of character.

A second consideration is that the availability of deepfake technology for generating realistic-but-false video and text (e.g., emails or tweets) with a look-and-feel of authentic text documents is likely to prove particularly useful in sowing confusion and breeding doubt in adversaries, especially among media-naive populations.

To undertake these or similar types of CEIOs, several policy issues would have to be resolved. Most important, standing DOD policy prohibits activities that are "directed at or intended to manipulate audiences, public actions, or opinions in the United States."[42] Although, strictly speaking, this prohibition is applicable to

activities "directed at" or "intended" for US audiences, it appears to have been extended to influence operations directed at foreign audiences, at least from time to time, because of the concern that US citizens might somehow be exposed to the information content of such operations through news media or the internet.[viii]

The online environment presents nontraditional opportunities for conducting influence operations. Because of the online environment's fundamental anonymity, distinguishing between humans and automated "bots" can be difficult. Today, bots can be used to flood selected information spaces, augment follower counts, and amplify content through retransmissions and "likes." In the future, bots will be able to engage in wide-ranging real-time conversations with human beings that will be indistinguishable from comparable human-to-human conversations, at least for limited content domains. Indeed, bots will likely be able to engage in persuasive conversations at least as well as some people,[43] providing SOF operators with opportunities for extending influence.

Finally, the lack of face-to-face interaction facilitated by the internet means SOF operators can engage with a broader range of adversaries. For example, given the paucity of Asian Americans in SOF,[44] most SOF units would likely find it difficult to operate inconspicuously while on the ground in many Asian nations. If an SOF operator can engage remotely, his or her ethnicity need not be apparent. An additional advantage of remote engagement is the ability to refer to large databases quickly to augment gaps in knowledge, which can build credibility and trust.

viii The origin of these concerns seems to be the 1948 Smith-Mundt Act, which prohibited the State Department from domestic dissemination of its international information materials and products. (Matthew C. Weed, *U.S. Public Diplomacy: Legislative Proposals to Amend Prohibitions on Disseminating Materials to Domestic Audiences*, Congressional Research Service, Washington DC, Report R42754, September 21, 2012, https://fas.org/sgp/crs/secrecy/R42754.pdf). Although the act applied only to the State Department, these provisions have been widely interpreted to mean the intentional or unintentional propagandizing of the American populace *by any element of the US government*. The Smith-Mundt Modernization Act of 2012 made the materials prepared for foreign audiences available to members of the interested domestic public—nevertheless, concerns remain about DOD propagandizing of the US public, and, thus, DOD policy continues to prohibit the activities described above (112th Congress. Smith-Mundt Act of 2012. May 10, 2012. Accessed at https://www.congress.gov/bill/112th-congress/house-bill/5736).

Conclusion

The evolution of 5G networks, independently developed internet infrastructures, and tactile internet technology will increase the opportunity and improve the ability of US SOF to shape perceptions in various populations. However, these same opportunities, particularly independent internet infrastructures, will challenge the conventional mindset of CEIO and US SOF's ability to conduct cyber operations. Virtual reality and deepfake technology already exist, but will be more readily available and more deceptive than today.

This chapter suggests many possible opportunities for SOF to take advantage of influence operations enhanced by cyber tools. DOD appears to assign some responsibilities for influence operations to both SOCOM and CYBERCOM. SOCOM and CYBERCOM should maintain their existing efforts, but also consider developing a concrete joint strategy.[45]

There has been ongoing discussion within the DOD—specifically the US Army—about the scope of US Army Cyber Command responsibilities. In 2019, *Army Times* reported that US Army Cyber Command has proposed changing its name to Army Information Warfare Command.[46] Lt. Gen. Stephen Fogarty, commander of US Army Cyber Command, was quoted as saying, "sometimes, the best thing I can do on the cyber side is actually to deliver content, deliver a message. . . . Maybe the cyberspace operation I'm going to conduct actually creates some type of [information operation][ix] effect."[47] True enough. But the expertise of US Army Cyber Command, and of CYBERCOM, is on the information *delivery* side of influence operations.

By virtue of long experience in executing influence operations, US SOCOM has developed its extensive psychological and cultural expertise on the information *content* side of influence operations. Bringing to bear the respective expertise of each command should enhance the synergies possible between cyber-enabled influence operations and offensive cyber operations, and it would be most desirable if the two commands could partner on, rather than compete over, the cyber-enabled influence operations mission.

ix In context, the term "influence operations" as it is used in this chapter would have been a more proper substitute than "information operations."

Endnotes

1 U.S. Department of the Army, ADP 3-05: *Army Special Operations* (Washington, D.C., July 2019), https://fas.org/irp/doddir/army/adp3_05.pdf, page 2-8.
2 Joint Chiefs of Staff, "Joint Publication 3-0: Joint Operations" (Washington, D.C., October 22, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910; Joint Chiefs of Staff, "Joint Publication 5-0: Joint Planning" (Washington D.C., June 16, 2017), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf
3 Robert S. Mueller, III., *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, D.C.: U.S. Department of Justice, March 2019), https://www.justice.gov/storage/report.pdf, page 448.
4 Eric Schmitt, "American Commandos Gear Up for New Shadow War with Russia," New York Times, July 12, 2019, edition, https://www.nytimes.com/2019/07/12/us/politics/us-russia-hungary.html.).
5 Michael J. Mazarr et al., *Hostile Social Manipulation: Present Realities and Emerging Trends* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2713.html.
6 Michael J. Mazarr, et al., 2019.
7 U.S. Department of the Army, ADRP 3-05: *Special Operations* (Washington, D.C., January 2018), https://fas.org/irp/doddir/army/adrp3_05.pdf, pages 2-7.
8 "Chapter 2: Special Operations Force Structure," in *SOF Reference Manual*, Version 2.1, Academic Year 1999-2000 (Army Command and General Staff College, 1999), https://fas.org/irp/agency/dod/socom/sof-ref-2-1/SOFREF_Ch2.htm
9 U.S. Army Special Operations Command Public Affairs Office, "Military Information Support Operations Command (Airborne) (Provisional) Fact Sheet" (Fort Bragg, NC: U.S. Army Special Operations Command, n.d.), https://www.soc.mil/MISOC/MISO%20fact%20sheet.pdf.
10 Joint Chiefs of Staff, *Joint Publication 3-13.2: Military Information Support Operations* (Washington D.C., January 7, 2010 incorporating Change 1 20 December 2011), https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C1_JP_3-13-2.pdf, 1–6.
11 Much of this description is informed by *op. cit.* "Chapter 2: Special Operations Force Structure"; "ADP 3-05"; Joint Chiefs of Staff, "Joint Publication 3-13.2: Military Information Support Operations" (Washington D.C., December 20, 2011), https://info.publicintelligence.net/JCS-MISO.pdf, Fig IV–1, p. IV–8.
12 Joint Chiefs of Staff, Joint Publication 3-13, "Information Operations," ed. Department of Defense (Washington, D.C., 27 November 2012 Incorporating Change 1 20 November 2014), I-1, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf .
13 Nick Turse, "Fitness Tracker Data Highlights Sprawling US Military Footprint in Africa," *The Intercept*, January 29, 2018, https://theintercept.com/2018/01/29/strava-heat-map-fitness-tracker-us-military-base/.
14 Jeremy Hsu, "The Strava Heat Map and the End of Secrets," *WIRED*, January 29, 2018, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.
15 Kevin Anderton, "The Business Of Video Games: Market Share For Gaming Platforms in 2019 [Infographic]," Forbes, June 26, 2019, https://www.forbes.com/sites/kevinanderton/2019/06/26/the-business-of-video-games-market-share-for-gaming-platforms-in-2019-infographic/.
16 Tracy Staedter, "Why Russia Is Building Its Own Internet," *IEEE Spectrum,* January 17, 2018, https://spectrum.ieee.org/tech-talk/telecom/internet/could-russia-really-build-its-own-alternate-internet.
17 James Griffiths, The Great Firewall of China: How to Build and Control an Alternative Version of the Internet, Zed Books, 2019, London.
18 Shadab Nazmi, "Why India shuts down the internet more than any other democracy," *BBC*, December 19, 2019, https://www.bbc.com/news/world-asia-india-50819905.
19 Aradhna Krishna, Luca Cian, and Tatiana Sokolova, "The Power of Sensory Marketing in Advertising," *Current Opinion in Psychology* 10 (August 1, 2016): 142–47, https://doi.org/10.1016/j.copsyc.2016.01.007.
20 Sarah Korones, "Dunkin' Donuts Experiments with 'Smell-Vertising' in South Korea," ZDNet, August 12, 2012, https://www.zdnet.com/article/dunkin-donuts-experiments-with-smell-vertising-in-south-korea/.
21 See, for example, Dan Ariely, *Predictably Irrational: The Hidden Forces That Shape Our Decisions*, Revised and expanded (New York, NY: Harper Perennial, 2010); Daniel Kahneman, Paul Slovic, and Amos Tversky, eds., Judgment Under Uncertainty: Heuristics and Biases (Cambridge: Cambridge University Press, 1982); Jonathan Baron, Thinking and Deciding, Fourth edition (Cambridge: Cambridge University Press, 2008); Robert B. Cialdini, Influence: The Pscyhology of Persuasion, Revised edition (New York, NY: Harper Business, 2006); Thomas Gilovich, Dale Griffin, and Daniel Kahneman, eds., Heuristics and Biases: The Psychology of Intuitive Judgment (Cambridge: Cambridge University Press, 2002).
22 See, for example, Susan T. Fiske and Shelley E. Taylor, Social Cognition (Reading, MA: Addison-Wesley Pub. Co., 1984).
23 For a primer on System 1 and System 2 thinking, see Daniel Kahneman, *Thinking, Fast and Slow* (Farrar, Straus and Giroux, 2011); and see also the discussion of Type 1 (i.e., System 1) and Type 2 (i.e., System 2) thinking in Keith E. Stanovich, What Intelligence Tests Miss: The Psychology of Rational Thought (Yale University Press, 2009). For other variants of dual-system cognitive theory, see Richard E. Petty and John T. Cacioppo, "The Elaboration Likelihood Model of Persuasion," in Advances in Experimental Social Psychology, ed. Leonard Berkowitz, vol. 19 (Academic Press, 1986), 123–205,

https://doi.org/10.1016/S0065-2601(08)60214-2; and Shelly Chaiken, "The Heuristic Model of Persuasion," in Social Influence: The Ontario Symposium, Vol. 5., Ontario Symposium on Personality and Social Psychology (Hillsdale, NJ, US: Lawrence Erlbaum Associates, Inc, 1987), 3–39. For a contrary view on dual-system cognitive theory, see Arie W. Kruglanski and Erik P. Thompson, "Persuasion by a Single Route: A View from the Unimodel," Psychological Inquiry 10, no. 2 (1999): 83–109, https://doi.org/10.1207/S15327965PL100201.

24 Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (September 27, 1974): 1124–31, https://doi.org/10.1126/science.185.4157.1124.

25 RAND Corporation, "Intelligence Analysis," RAND Corporation Website, n.d., https://www.rand.org/topics/intelligence-analysis.html.

26 Richards J. Heuer, *Psychology of Intelligence Analysis* (Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency, 1999).

27 Michael A Hogg and Mark J Rinella, "Social Identities and Shared Realities," Current Opinion in Psychology, Shared Reality, 23 (October 1, 2018): 6–10, https://doi.org/10.1016/j.copsyc.2017.10.003.

28 See, for example, Ziva Kunda, "The Case for Motivated Reasoning," *Psychological Bulletin* 108, no. 3 (1990): 480–98, https://doi.org/10.1037/0033-2909.108.3.480.

29 John A. Robinson and Linda Hawpe, "Narrative Thinking as a Heuristic Process," in *Narrative Psychology: The Storied Nature of Human Conduct* (Westport, CT, US: Praeger Publishers/Greenwood Publishing Group, 1986), 111–25.

30 Stephen D. Reese, "Prologue—Framing Public Life: A Bridging Model for Media Research," in *Framing Public Life: Perspectives on Media and Out Understanding of the Social World*, ed. Stephen D. Reese, Oscar H. Gandy Jr., and August E. Grant (Mahwah, NJ: Lawrence Erlbaum, 2001), https://doi.rg/10.4324/9781410605689-7; Cynthia Gordon, "Framing and Positioning," in The Handbook of Discourse Analysis, ed. Deborah Tannen, Heidi Ehernberger Hamilton, and Deborah Schiffrin (John Wiley & Sons, 2015), 324–45, https://doi.org/10.1002/9781118584194.ch15.

31 Kahneman, *Thinking, Fast and Slow, op. cit.*

32 Caitlin Dewey, "6 in 10 of You Will Share This Link without Reading It, a New, Depressing Study Says," *Washington Post,* July 16, 2016, Digital edition, https://www.washingtonpost.com/news/the-intersect/wp/2016/06/16/six-in-10-of-you-will-share-this-link-without-reading-it-according-to-a-new-and-depressing-study/.

33 Mueller Report *op. cit.,* 448.

34 Raymond S. Nickerson, "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises," *Review of General Psychology* 2, no. 2 (June 1, 1998): 175–220, https://doi.org/10.1037/1089-2680.2.2.175.

35 David N. Rapp, The Consequences of Reading Inaccurate Information, Current Directions in Psychological Science 25(4):281-285, 2016, https://journals.sagepub.com /doi/10.1177/0963721416649347.

36 Jieun Shin, Lian Jian, Kevin Driscoll, François Bar, "The diffusion of misinformation on social media: Temporal pattern, message, and source," Computers in Human Behavior, 83:278-287, 2018, http://www.sciencedirect.com/science/article/pii/S0747563218300669.

37 Joint Publications 3-12, "Cyberspace Operations", June 8, 2918. Accessed from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

38 Dina Temple-Raston, "How The U.S. Hacked ISIS," National Public Radio, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

39 On Cheney, see Morgan Chalfant, "Cheney: Russian Election Interference Could Be 'Act of War,'" The Hill, March 27, 2017, https://thehill.com/policy/cybersecurity/325928-cheney-russian-election-interference-could-be-act-of-war; on Clinton, see Sofia Lotto Persio, "Hillary Clinton Compared the Russian Interference in the U.S. Election to 9/11," Newsweek, October 15, 2017, https://www.newsweek.com/clinton-compares-russian-interference-election-911-685474.

40 See indictments in United States v. Netyksho et al., 1:18-Cr-00215-ABJ (U.S. District Court for the District of Columbia, July 13, 2018), https://www.justice.gov/file/1080281/download.

41 Karen Freberg et al, "Who are the social media influencers? A study of public perceptions of personality," *Public Relations Review* 37(1):90-92, 2011, http://www.sciencedirect.com/science/article/pii/S0363811110001207.

42 See item 3(k) in U.S. Department of Defense, "Directive 3600.01: Information Operations," May 4, 2017, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/360001p.pdf, 2.

43 Weiyan Shi et al, "Effects of Persuasive Dialogues: Testing Bot Identities and Inquiry Strategies", to appear in the Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems,2020. Preprint available at https://arxiv.org/pdf/2001.04564.pdf.

44 See Figure 5 in Mike Copenhaver, *The Integration of Minorities into Special Operations: How Cultural Diversity Enhances Operations* (Carlisle, PA: U.S. Army War College, 2014), https://apps.dtic.mil/dtic/tr/fulltext/u2/a620551.pdf.

45 See, for example, Herb Lin, "On the Integration of Psychological Operations with Cyber Operations," *Lawfare*, January 9, 2020, https://www.lawfareblog.com/integration-psychological-operations-cyber-operations.

46 Kyle Rempfer, "Army Cyber Lobbies for Name Change This Year, as Information Warfare Grows in Importance," *Army Times,* October 16, 2019, https://www.armytimes.com/news/your-army/2019/10/16/ausa-army-cyber-lobbies-for-name-change-this-year-as-information-warfare-grows-in-importance/.

47 Rempfer, "Army Cyber Lobbies for Name Change," *op. cit.*

CHAPTER 25

The New COIN of the Realm: The Future of Technology and Insurgency

P.W. Singer

Introduction

Long before the military convoy arrived in the muggy town of Dara Lam, news of the meeting between the US Army colonel and the unpopular governor of Kirsham province had seeped into social media.[1] Angry with both the American presence and the governor's corruption, local citizens organized for a demonstration. Their trending hashtag—#justice4all—soon drew the attention of international media and the online world. It also drew the eyes of some less interested in justice: the notorious Fariq terror network. Using sockpuppet accounts and bots to steer the course of online and real-world sentiment, the terrorists fanned the flames, calling for the protesters to confront the American occupiers.

But this was not the full extent of Fariq's plan. Knowing where a massive crowd of civilians would soon gather, the terrorists also set an ambush. They planned to fire on the US soldiers as they exited the building, and, if the soldiers fired back, the demonstrators would be caught in the crossfire. Pre-positioned cameramen stood ready to record the bloody outcome: either dead Americans or dead civilians. A network of online proxies was prepared to drive the event to virality and use it for future propaganda and recruiting. Whatever the physical outcome, the insurgents would win this battle.

Luckily, other eyes were tracking the flurry of activity online: those of a US Army brigade's tactical operations center. The center's task was to monitor the environment in which its soldiers operated, whether the battlespace was dense cities, isolated mountain ranges, or, now, clusters of social media influencers. The tactical operations center detected the fast-moving online developments and immediately passed them up the chain of command. A generation earlier, the officers might have discounted what was playing out online as mere internet chatter, but now they understood its importance. Receiving word of the protest's growing strength and fury, the colonel cut his meeting short and left discreetly through a back entrance. Fariq's plan was thwarted.

Try as you might, you won't find any record of this event in the news—not because it takes place in the distant year of 2030, but because Dara Lam is a fake settlement in a fake province of a fake country, one that endures a fake war that breaks out every few months in the very real state of Louisiana.

The Joint Readiness Training Center at Fort Polk holds a special place in military history. It was created as part of the Louisiana Maneuvers, a series of massive training exercises held just before the United States entered World War II. When Adolf Hitler and his blitzkrieg rolled over Europe, the US Army realized warfare had begun operating by a new set of rules. It had to figure out how to transition from a world of horses and telegraphs to one of mechanized tanks and trucks, guided by wireless

communications. At Fort Polk, American soldiers, including such legendary figures as Dwight D. Eisenhower and George S. Patton, learned how to fight in a way that would preserve the free world.

Since then, Fort Polk has served as a continuous field laboratory where the army trains for tomorrow's battles. During the Cold War, the army used Fort Polk to prepare for feared clashes with the Soviet Red Army and then to acclimatize troops to the jungles of Vietnam. After 9/11, the 72,000-acre site was transformed into the province of Kirsham, replete with twelve plywood villages, an opposing force of simulated insurgents, and scores of full-time actors playing civilians caught in the middle: in short, everything the army thought it needed to simulate how war was changing. Today, Fort Polk boasts a brand-new innovation for this task: SMEIR.[2]

Short for Social Media Environment and Internet Replication, SMEIR simulates the blogs, news outlets, and social media accounts that intertwine to form a virtual battlefield atop the physical one. A team of defense contractors and military officers create a version of the internet activity of a small city—rambling posts, innocuous tweets, and the occasional bit of viral propaganda—challenging the troops fighting in the Kirsham counterinsurgency to navigate the new digital terrain. For the stressed, exhausted soldiers dodging enemy improvised explosive devices (IEDs) and bullets, safeguarding the local population and fighting the evil insurgents is not enough; they must also be mindful of the ebb and flow of online conversation.

The project illustrates just how rapid—and surreal—technology change can be for military training and the broader political environment. A generation ago, the internet was a niche plaything, one that the US military itself had just walked away from, handing off control to a global consortium of volunteers. Only the most farsighted futurists at RAND suggested it might one day become a crucial battlefield.[3] None imagined the future military would have to pay millions of dollars to simulate a second, fake internet to train for war on the real one.[4]

In this way, what played out at Fort Polk serves not just as a training moment but also a warning for those wrestling to understand the future of war. Despite hopes to the contrary, there will likely be a consistent need to prepare for insurgency, not just because of the continuing issues of failed states and collapsed governance, but the likelihood that, as in the Cold War, great-power competition could express itself through proxy warfare.[5] Yet while the essence of insurgency—a rebellion against authority that targets the effectiveness and legitimacy of the pillars of society[6]—remains the same, advances in science and knowledge can reshape it. Just as they can change the society within which insurgency takes place, new technologies can also introduce key shifts in everything from tactics used in battle to the overall dynamics of the conflict itself.

The following chapter first explores the technologic changes that loom in the years leading toward 2030 and beyond. It then proposes a series of their potential implications, most especially for counterinsurgency, a core task for special operations forces from their beginning to today to 2030 and beyond.

The Technology That Matters

When modern US counterinsurgency strategy was first codified in 1962 under the idea of "Overseas Internal Defense Policy,"[7] it was typed on a machine without digital components. Computers were then used only as massive calculators for a small number of government agencies and businesses. Personal communications devices were little changed versions of the telephone that had been developed by Alexander Graham Bell almost a century earlier, still hardwired into your office or home. The internet would not even be conceived for another year (in a memo written by J. C. R. Licklider and Robert W. Taylor, first describing it as the "Intergalactic Computer Network"),[8] while the first mobile telephone would not be invented until 1973 (and even then, the three-pound Motorola monstrosity did not go on sale for another decade, for the modest price, in today's dollars, of $10,000).[9] As we see in the fictional training at Dara Lam to ISIS's all-too-real rise and recruiting through its deft use of social media, these technologies have since proven crucial to the story of modern insurgency.[10]

In weighing the potential impact of technology on insurgency in the future, we should similarly seek to identify the technologies that will truly matter, in a manner like the computer and its networking did. That is, our focus should not be on mere evolutionary improvements, such as a gun that shoots a bit faster or a missile that goes slightly farther, but the technologies that change the game. These go by various catchphrases. A generation ago in the Pentagon, "revolutionary" was the popular term.[11] Today, the buzzword is "disruptive." Ironically, outside the military, the descriptor is "killer app." Whatever the preferred term, the next most important technologies are akin to the steam engine in the 1820s, the airplane in the 1920s, or the computer in the 1980s–already real and poised to change the world.

What makes such technologies so revolutionary, however, is not that they will somehow magically solve all our problems or lift the fog of war as once claimed by acolytes.[12] Rather, it is the opposite. What truly defines technologies as game-changers is they present new questions, to which we do not have the answers. Disruptive technologies introduce two types of questions : First, "What is *possible*, that was not possible just a generation before?" Second, "What is *proper,* that we were not wrestling with before?" These questions may have to do with the right and wrong way to recruit, organize, train, or equip. Or, they might be related to right and wrong, in terms of raising real legal and ethical issues that were recently only the stuff of science fiction.

A few years back, I helped develop a project for the Pentagon called NeXTech,[13] where we conducted research to determine the pending technologies that might have the aforementioned effect, that is, those in the position now that the computer was in 1980. We interviewed a diverse set of subject-matter experts, ranging from people working at government defense labs and university research centers to experts in industry, ranging from defense contractors to Silicon Valley firms such as Apple, Google, and Facebook. These experts helped us understand the looming change did

not center on any one technology but a cluster of new technology areas. From the hardware of robotics to the "wetware" of human performance enhancements, these technology clusters are poised to change the landscape of what is viewed as possible and proper, including for war and insurgency.

Hardware

In our lifetime, robots, arguably the most celebrated of science fiction technologies, have finally become reality. The US military force that entered Afghanistan after the 2001 attacks used zero robotic systems; as of 2019, the force had over 22,000 in its inventory, while civilian drones are used in an ever-growing number of industries, from agriculture to real estate.[14]

Moving forward, we will see even more automation. Increasingly, autonomous robotics will come in two primary forms, each of which mimics intelligence in nature. In the first type of system, intelligence is centralized. In robotics, these tend to be physically large-scale systems that mimic or directly replace human tasks; examples include driverless cars and unmanned planes. In the second type of system, the intelligence and resulting tasks are decentralized. These systems work via networks, akin to insects, allowing the tasks to be disaggregated into parts, often operating via "swarms" in mass scale.[15]

The changes brought on by both types of systems will be incredibly disruptive to both war and work. An Oxford University examination of 702 different jobs found that 47 percent of total US employment risks change, reduction, or even replacement by automation within the next two decades.[16] The automation of jobs will most affect developing world economies, which support often fragile politics. As just one illustration, according to International Labour Organization estimates, over 137 million salaried workers in five Southeast Asian countries—Cambodia, Indonesia, the Philippines, Thailand, and Vietnam—are "at high risk of being replaced by machines."[17]

These statistics point to an important impact of true technological change: It affects society on multiple levels and in multiple issue areas. For instance here we can expect that technology that simulates and replaces humans will not just alter the various roles that humans play in insurgency but also may spark the kind of anger and unrest that can lead to it.[18]

Software

Major changes are also taking place in what runs our digital technology and software and the networks that connect it. The rise of the "network of networks" has shaped insurgency to such a degree that ISIS, for example, is literally a creature of the modern internet,[19] both recruiting through and operating on it. Yet, the internet itself is changing. One change is to its scale. Only half the world is online, meaning half is still to join. Importantly, however, this shift will take place in many of the areas considered most fragile politically and, thus, susceptible to mass violence. Another change is in its form and function. The internet is shifting from a system of communications among

human beings to running the systems of our increasingly digital world. As of 2019, roughly 10 billion devices were online. By 2026, the number of networked devices is estimated by some to reach 64 billion, reflecting over $3 trillion annual spending.[20] In the new Internet of Things (IoT), most of the new contact points will shift from desktop computers and smartphones to "things" such as cars, thermostats, and power plants.

These changes will shift the internet's impact on and relationship with the world beyond it, particularly in the urban environment. Over the last half century, the global urban population grew by roughly four billion. Over the next decades, most of the global population growth will continue to be in cities; the United Nations projects more than two-thirds of population will be urban by 2050.[21]

As war is a human endeavor, driven by human causes, this trend projects that future wars will see more and more urban operations. It will also shape all the other military tasks, from humanitarian disaster relief to counterterrorism, to take place in more urban settings, especially given the growing number of megacities that eclipse the scale of past urban operations. (Fallujah, for instance, had a population that was less than 250,000, which had fled in significant numbers, and no true high-rise buildings; imagine the battle in a city two orders of magnitude greater in scale and filled with high-rises and skyscrapers.)

These cities will be wired in a way they were not before by IoT, changing not just operations in this space, but what is known in them. All of the new "things" coming online carry "sensors," a system for gathering information about the world beyond the computer, technologies lacking from the computers used by the Advanced Research Projects Agency Network (ARPANET) and even the one with which Mark Zuckerberg created Facebook. Some sensors are self-evident, such as a smartphone or a traffic-light camera. Others hide in the background, like the magnometer and Global Positioning Systems (GPS) that provide information about direction and location. Further, any information online comes with "metadata," akin to digital stamps that provide underlying details about the point of origin and movement of the data. These billions of internet-enabled devices, each carrying multiple sensors, are on pace to create a world of almost a trillion sensors. So, whether the setting is a dazzling "smart city" or the sprawling slums of a megacity, there will be mass connection and collection, making surveillance nearly omnipresent. Indeed, the best parallel for the emerging urban space may be the industrial revolution concept of a "panopticon," where someone or, now, something potentially monitors your every move.[22]

This massive growth will not only empower the internet economy and gather information on scale but also allow the internet to become more of a threat vector than it already is. The IoT will not just merely grow the attack surface, the potential points of vulnerability that cyber threats will go after. Unfortunately, the construction of the IoT is replicating all the original cybersecurity mistakes, baking in insecurity. With no clear security responsibilities and almost no regulation or even basic liability, these devices often lack basic security features, while customers are largely unaware of what they can and should do. Up to 70 percent of IoT devices have

known vulnerabilities,[23] and compromised devices have already become a key part of botnets.[24]

The shift to the internet connecting and running things will play out simultaneously with another core shift, the use of distributed ledger technologies (DLT), using blockchain and other related technologies, to share files, records, and knowledge of how the system works. Already, the impact of DLT has been felt in areas such as finance, where bitcoin and other cryptocurrencies have created a new form of money and method for transferring value. Yet, the model of peer-to-peer distribution may lead to even greater change as it is applied across fields and into recordkeeping. It may even lead to a fundamental reordering of the web, as Chris Meserole and Alina Polyakova put it in *Foreign Policy* magazine, "outside the control of major corporations and states."[25] Such a decentralized model would empower weaker and nonstate actors. Or, like in other spaces of the web, it may prove to be another means for authoritarian states to exert control, such as China's recent efforts targeting blockchain developers.[26] The fact that both scenarios represent potential futures of which we do not yet know the outcome illustrates the scale of shift at hand.

The shift in the internet itself, though, might be minuscule in impact compared to that of the coming intelligence of software. The Chinese military describes the significance as the move in societies, as well as their wars, from the industrialization of the twentieth century to the informatization of the turn of this century to a looming "intelligentization."[27]

The field of artificial intelligence (AI) encompasses work on everything from machine learning to neural networks. Arguably, no other technology area has as much political and economic anticipation and financial investment. Governments around the world, ranging from the US to the Russian, Singaporean, and Israeli, are engaging in an AI "arms race." This arms race, though, is unlike those in the past; the participants do not include only competing nations. All the world's major technology companies and even most traditional business corporations have also focused on AI, spending roughly $153 billion in this space, "with an estimated annual creative disruption impact of $14-33 Trillion."[28] Google and Microsoft, for example, each fund robotics and AI research to an amount of roughly $10 billion a year. General Electric, the company founded by Thomas Edison in 1892, has begun repositioning itself for a robotics and AI market,[29] while John Deere, known for its tractors, bought one of the most promising AI firms in the world.[30] The majority of new entrants to the marketplace also focus on AI. As the founder of *Wired* magazine describes, "AI is already here, it's real, it's quickening. . . . I think the formula for the next 10,000 start-ups is to take something that already exists and add AI to it."[31]

Thought leaders and business luminaries wrestling with the importance of AI seemingly cannot overstate its significance. Masayoshi Son, the founder of the megaconglomerate Softbank, says:

> *Every industry that mankind created will be redefined. The medical industry, automobile industry, the information industry, of course. . . . Even agriculture will be redefined. Because the tools that we created were inferior to mankind's brain in the past. Now the tools become smarter than mankind ourselves. The definition of whatever the industry will be redefined.*[32]

Baratunde Thurston, a director's fellow at the Massachusetts Institute of Technology's Media Lab, goes further, "Every area of life will be affected. Every. Single. One."[33] Insurgency falls within this categorization.

Wetware

Another historic change is afoot in technology in terms of its relationship to humans themselves. "Wetware," or, more technically, "human performance modification," is about using technology to change us. Think of this as combining the science fiction of *Iron Man* and *Captain America* and the Russian Olympic athlete program.

We are seeing revolutions in fields from medicine to synthetic biology, a new discipline encompassing everything from genome-editing tools such as CRISPR to biologic computers.[34] In this space, discoveries and breakthroughs are outpacing "Moore's Law," the IT field standard for changes in processing speed. These are rewriting what is possible for the human species, altering everything from susceptibility to disease to bodily endurance to the workings of the brain.[35]

In turn, new technologies in brain-machine interface will rewrite the entire history of how humans have connected to their technology. From the first stone tools to the drone and iPhone, we have used our monkey fingers. This is being challenged by technologies that have allowed test subjects to control mentally advanced technologies like aircraft[36] and "telepathy tech," conducting database queries and process product orders without ever writing or vocalizing them.[37]

Synergy

A variety of other technology areas could be as disruptive as the three above. For instance, new forms of both energy generation and storage are either coming online or being distributed in new ways, which could shift the nature of geopolitics, battlefield logistics, and other realms of interest to special operations forces. Such technologies could redefine the roles and purposes of already revolutionary systems. For instance, an autonomous drone is game-changing enough as a plane; an autonomous drone that mixes solar and hydrogen energy to stay in the air for 12 months[38] perhaps ought to be understood as something else, as it would have attributes more akin to a space satellite than a plane.

Indeed, that these new technologies cross with and shape one another may be their most exciting and game-changing aspect. For example, direct digital manufacturing, popularly known as "3D printing," turns a bit, a computer design,

into an atom, a created substance. 3D printing is thus a story of both hardware and software revolutions. As such, it holds the potential promise of altering fundamental business models, doing for defense firms what the iPod did to the music industry, changing not just profit margins but also the path to profit itself, as anyone would be able make their own systems and spare parts. In turn, it yields new threats. Indeed, in Great Britain, a country that effectively bans gun sales, police have had to deal with 3D printed guns,[39] while ISIS used fairly advanced injection molding techniques to make its own drones.[40]

What Will These Tech Trends Mean for Counterinsurgency?

With so much change, it is too early to know all that will shake out from these new technologies. But we can identify a few key meaningful trends for war and beyond and resulting questions with which future counterinsurgents will likely have to wrestle.

The End of Nonproliferation

Common among these diverse technology areas is that they are neither inherently military nor civilian. Government and civilian organizations will both research and develop these technologies and buy and use them. Organizations and individuals will apply them to conflict but also to business and family life. Also, these technologies will not require the deployment of massive logistics systems, and, as machine intelligence increases, they will be relatively easy to learn and use, not requiring large training or acquisitions programs. Therefore, insurgent groups will be able to make more rapid gains in technology and capability than previously possible.

In short, the game-changing technologies of tomorrow are most likely to have incredibly low barriers to entry, which means they will proliferate. In addition, some technologies, such as 3D printing, will complicate nonproliferation approaches such as arms embargos and blockades. Weapons interdiction will be altered drastically by the widespread ability to manufacture components and even overall systems onsite.

This issue is not one merely of hardware, but also the spread of ideas. As vexing as the extent of terrorist ideology and "how-tos" have been in a world of social media, Twitter, Facebook, and others still control their platforms. However, the move toward decentralized applications reduces companies' power to censor for legal or public-relations reasons.[41] This problem is beyond a YouTube clip showing how to build an IED or a cleric inspiring someone who watches a linked video to become a suicide bomber. Decentralization, crossed with crowd- and open-sourcing, empowers *anyone* on the network to new scales. For example, Tensorflow,[42] an existing open-source project, allows any actor to tap into AI resources that were science fiction just a decade ago.

Key Resulting Questions

- How will US and allied forces prepare for insurgent adversaries that have access to many of the same technologies and capabilities?
- Will lower barriers to entry make it easier for insurgencies to gain the capability needed to rise?
- Will ease of manufacture and proliferation make it more difficult to defeat insurgencies, if they can rapidly re-create capability?

Multi-Domain Insurgencies

A century ago, Marines battling the rebel forces in Haiti pioneered the earliest of close air-support missions. Today, Marines battling the Taliban, enjoy that same crucial advantage of counterinsurgents. In enjoying unfettered access to the air, they have been able to operate more effectively on the land, not only conducting surveillance and strikes that prevented insurgents from effectively massing forces but also moving their own forces to almost anywhere they wanted.

The monopolization of power may not be the case in the future. Indeed, ISIS, without any state sponsor, has already been able to utilize the air domain (via a self-made air force of drones) to conduct both ISR of US and allied forces and several hundred air strikes.[43] Its "air force" may be ad hoc but still has achieved goals at a minimal cost. More important, ISIS's use of drones points to a change in the overall story of air power and insurgency. Now, the insurgents can fly and fight back.[44]

This ability to cross domains is not limited to air power but also is applicable to other new domains that technology is opening up to battle. Insurgencies will be able to tap into the global network of satellites that have given US forces such advantage in ISR and communications, or even potentially be able to launch and operate cheap microsatellites, either via proxy aid or on their own. (If college students can do it already,[45] why not insurgents?).

More important, the "cyber war" side of insurgency will likely move well past what has been experienced so far.[46] The proliferation of capability through both dark markets and increasing automation, combined with the change in the internet's form to more and more "things" operating online, points to insurgents being able to target command-and-control networks and even use Stuxnet-style digital weapons causing physical damage.[47]

The ability to operate across domains also means insurgents will be able to overcome the "tyranny of distance." Insurgents will be able to observe, target, and reach once-secure bases, and even a force's distant homeland, through malware or unmanned aerial systems. This dynamic has to alter how we think of intervention in conflicts previously characterized as "small wars." More than 75 nations have cruise missiles and over two dozen nations have armed drones; pretty much every nonstate actor has cyber capabilities.

If small nations and nonstate actors can more easily strike back—be it with drones, missiles, or cyberspace hacks—the lure of easy wars fought from afar without consequence is even more of a false notion than it was in the past. Perhaps the most graphic recent illustration of this is the Saudi-United Arab Emirates (UAE) intervention into the Yemeni civil war. When these states launched "Operation Decisive Storm" in 2015, it had an expectation of an easy, airpower-driven win that would "shock and awe" the Houthis into capitulation. Four years and 70,000 casualties later, the Saudi-UAE coalition found itself not just stuck in a grinding ground war but also the victim of a series of drone and missile attacks on sites inside their own countries that, at one point, took half of Saudi oil production off line.[48] If the other side can more easily hit back, be it at a base or the homefront, one must rethink intervention. A future insurgency may not see a Tet-style offensive attack in Hue, but rather in Houston.

Key Resulting Questions

- Is the United States prepared for multidomain warfare, against not only peer states but also insurgents?
- What capabilities utilized in counterinsurgency today might not be available to forces in 2030?
- Just as US forces have used capability in one domain to win battles in another, how might insurgents do so?
- Does the lower barrier to entry for new war technologies demand a higher barrier to entry for joining one?

UnderMatch

In the final battles of World War II's European theater, US forces had to contend with an adversary that brought better technology to the fight. Fortunately for the Allies, the German "wonder weapons," which ranged from rockets and jets to assault rifles, entered the war too little and too late. For the last 75 years, US defense planning has focused on making sure this experience was not repeated to ensure it stayed ahead of its foes technologically. Having a qualitative edge to "overmatch" our adversaries became baked into everything from our overall defense strategy to small-unit tactics. This edge allowed the US military to deter the Red Army in the Cold War, despite having a much smaller military, and to invade Iraq with a force one-third the size of Saddam Hussein's (inverting the mantra that the attacker's force should be three times the size of the defender's).[49]

While this tech overmatch did not always deliver easy victories in painful insurgencies, such as in Vietnam and the post-9/11 wars, it still shaped both tactics, docrine, force size, and even the worldview of the combatants. A Marine officer once told me that if 100 Taliban soldiers attacked his unit of 30 men, he

would have no fear that his unit might lose; indeed, he described how it would almost be a relief to face the foe in a stand-up fight, as opposed to the fruitless hunts, hidden ambushes, and roadside bombs of insurgency. The reason for his confidence was not just his force's training, but that in any battle, his side alone could call down systems of technology that the insurgency could not dream of having, from pinpoint targeting of unmanned aerial systems controlled via satellite to hundreds of GPS-guided bombs dropped by high-speed jet aircraft able to operate with impunity.

Yet US forces cannot count on that overmatch in the future, and not only because of the mass proliferation discussed above, driven by the lower barriers to entry and availability of key tech in the marketplace. Our future counterinsurgency thinking must also recognize geopolitics have changed, with effect on the availaibility of systems. As challenging as the Taliban and ISIS have been, they were not supported by a comparable peer-state power, both developing its own game-changing technology and supplying it to the world.

Mass campaigns of state-linked intellectual property theft means we pay much of the research-and-development costs of China's weapons development. At the same time, China has begun to invest massively in becoming a world leader in revolutionary technologies.[50] For instance, China has a dedicated national strategy to become the world leader in AI by the year 2030,[51] with an array of planning and activity to achieve that goal, while it has displayed novel weapons programs in areas that range from space systems to armed robotics.[52]

Such trends matter not just in the space of great-power conflict, but also in how great powers often contend with each other through much of their rivalry period, such as through proxy warfare, an arena that frequently connects to special operations. During the Cold War, the United States and Soviet Union repeatedly supported and countered insurgents, supplying rebels and governments alike with arms, training, advice, and combat support. It is not unreasonable to expect some repeat of this as the US-Chinese rivalry goes global. Additionally, just as in the Cold War, an arms-trade component of this competition has emerged, with China supplanting Russia as the alternative supplier of choice to the United States.

Therefore, in a future deployment, be it great-state conflict or small-scale insurgency, whether from purchases off the global market or proxy warfare supplies, the United States might not have its expected edge. Indeed, American soldiers could even face the same kind of shock that Soviet helicopter pilots had in Afghanistan in the mid 1980s, when the Stinger missile showed up in the hands of the mujahideen. A US force could one day find itself fighting a guerrilla force that brings *better* technology to the fight.

Key Resulting Questions

- What tactical changes are needed for counterinsurgents when they do not enjoy technology "over-match?"
- How does the growing geopolitical environment shift counterinsurgency? Are US tactics and doctrine ready for great-power–supported insurgents?

Information Underload and LikeWars

> *"It is like sipping from a fire hose."*

This is how a US military officer described a core problem in their job to me at the Combined Air Operations Center at Al Udeid Air Force Base, where US forces coordinated the massive scale of operations in support of counterinsurgencies in Iraq and Afghanistan. They felt most challenged by the amount of data coming at them, from full-motion video to chatroom posts, sent by people ranging from soldiers in the midst of a firefight to intelligence analysts back in the United States. The officer not only had trouble keeping up with the flow, but also, in constantly servicing their inbox, thinking and acting strategically.

Some believe that mastering the problem of "too much information" actually holds the solution to ending insurgency as a phenomenon. In a world of mass surveillance, goes the thinking, if we can sift through the information rapidly enough, insurgents will not be able to operate effectively. AI algorithms will not just identify insurgents instantly via facial recognition[53] or gait detection analysis,[54] but even move to predict their activities. Indeed, various projects already mine open-source intelligence, such as social media posts, to predict the outbreak of violence, riots, and insurgencies.[55]

We should not be so quick to declare victory against "rebel scum" of the future. Like all conflict, insurgency involves a thinking adversary, reacting to each and every move and technology. For instance, we are already seeing the rise of tactics to counter mass surveillance, such as face paint[56] and even stealth clothing.[57] The 2019 street protests in Hong Kong represented a literal battle lab of this back and forth. In turn, the spread of autonomous drones and cars will render whole swaths of current counterterrorism/insurgency defenses obsolete.

The counter tactics may be about more than merely deceiving sensors, but also about altering our relationship with information itself. The systems on which we rely are only as reliable as the information that goes into them. The connection points of this information can be attacked. Communications signals to drones have already been blocked and manipulated in tests, while merchant ships in the Black Sea off Russia experienced a suspected hack in which their GPS started to tell the ship captains they were sailing miles inland.[58] In these situations, someone or something was cutting off or tampering with the information. But what also bodes is a kind of

poison to the overall system, targeting the people behind the networks, in a way that blends old lessons of terrorism with new possibilities of social media.

"Terrorism is theater," declared RAND Corporation analyst Brian Jenkins in a 1974 report that became one of the foundational studies of terrorism and insurgency.[59] Command enough attention and how weak or strong you were did not matter; you could bend populations to your will and cow the most powerful adversaries into submission. This simple principle has guided insurgents and terrorists for millennia. Whether via assassination in the town squares of ancient Judea, marketplace bombings in colonial wars like the one in Algeria, or ISIS's carefully edited beheadings in Syria, the goal has always been the same: control what people think (and fear).

Already, we have seen the power of online networks to shape news and narrative, perhaps most illustratively with the ISIS invasion of Mosul, where an insurgent force did not hide from but, instead, embraced surveillance. Indeed, ISIS even branded its 2014 offensive with the hashtag #AllEyesOnISIS, to ensure the world was watching.

Increasingly, we can use technology to disseminate false information that overwhelms not only our political systems but also our human senses. Bots, algorithms that perform automated tasks, such as acting like humans online, represent one eaxmple of how we can be overwhelmed by false information. The early versions of social media bots could drive what people thought, knew, and even argued about during some of the most influential elections of the last few decades. Bots drove one-third of online conversation on Brexit. In the final six weeks before the 2016 US election, approximately half the American population was unknowlingly exposed to Russian propaganda via Facebook, while Twitter concluded that bots helped drive Russian-generated propaganda to users 454.7 million times.[60] Subsequently, the similar use of artificial accounts appeared not only in elections in places ranging from Mexico to Brazil and Italy but also in attacks on corporate brands and stock share prices and in campaigns to boost the spread of antivaccine conspiracy theories.[61]

Artificial intelligence, available to all actors, will compound this problem exponentially with the creation of "deepfakes." Artificial neural networks mimic how the human brain works, using individual nodes that activate (or not) to a single point of information and carry out incredibly complex tasks by layering the connections together. Through this, machines can study a database of images, words, and sounds to learn to mimic a human speaker's face and voice almost perfectly. An early example of the potential political impact of this came in the creation of an eerily accurate, entirely fake conversation between Barack Obama, Hillary Clinton, and Donald Trump.[62] Drawing only from the data of two-dimensional photographs, these systems can build photorealistic, three-dimensional models of someone's face. In one example, AI transformed a single photograph of the late boxing legend Muhammad Ali into "photorealistic facial texture inference," essentially able to rewrite what he actually did and said when he was alive, at least in our online records of him (which will be the source of "truth" to the vast majority).[63]

Neural networks can also be used to create deepfakes that are not copies at all. Rather than study images to learn the names of different objects, these networks learn how to produce new, never-seen- before versions of the objects in question, called "generative networks."[64] As an example, computer scientists unveiled a generative network that could create photorealistic synthetic images on demand, all with only a keyword. Ask for "volcano," and you got fiery eruptions, as well as serene, dormant mountains—wholly familiar landscapes that had no earthly counterparts. Another system created faces of people who did not exist but whom real humans would most likely mistake as Hollywood movie stars.[65] Such networks can do the same thing with video to create new moments in time that never happened.[66] These networks have produced eerie, looping clips of a "beach," a "baby," or even "golf." They have also learned how to take a static image (a man on a field; a train in the station) and generate a short video of a predictive future (the man walking away; the train departing). In this way, events that never took place may be presented online as real occurrences, documented with compelling video evidence.

Finally, there are neural-network–trained chatbots—also known as machine-driven communications tools, or MADCOMs.[67] This technology—an AI essentially indistinguishable from a human operator—is being built to help companies replace their help desks and sell products online. As in every technology, deepfakes also could be misused terribly and weaponized. Versions have already been used in "revenge porn" that places victims into acts they never committed, while hackers have already used the faked voice of a CEO, hyperaccurate down to the subtle accent of his German background, to trick his subordinate into the fraudulent transfer of $243,000.[68]

Today, savvy internet users can still distinguish "real" people from automated botnets and even many sockpuppets (the combination of Russophied English and a love for red #MAGA hats often gives them away). Soon enough, even this uncertain state of affairs may be recalled fondly as the "good old days"—the last time it was possible to have some confidence that another social media user was a flesh-and-blood human instead of a manipulative machine.

Combine all these pernicious neural-networks applications—mimicked voices, stolen faces, real-time audiovisual editing, artificial image and video generation, and MADCOM manipulation—and it is tough to shake the conclusion the long-feared "cyberwar" of hacking networks will prove less important than what one might conceptualize as the "LikeWar" side of battle: hacking people on networks by driving ideas virally through a mix of likes, shares, and lies.[69]

As an outcome of these technologies, the insurgencies of 2030 will be fought by not only people but also highly intelligent, often inscrutable algorithms that will speak convincingly of things that never happened, producing "proof" that does not really exist. They will seed falsehoods across the social media landscape with an intensity and volume that will make the current state of affairs look quaint. For instance,

as futuristic as the counterinsurgency training on the SMEIR at Fort Polk seems, it captures a point in time soon to passed by technology and tactics.

Thwarted by the eagle-eyed US Army tactical-operations officers, terrorists might not just fade back into the crowd. They might instead shoot the civilians anyway and simply manufacture compelling online evidence of US involvement. Or, maybe they never even show up in the first place, manufacturing the massacre using neural networks that would produce hyperrealistic imagery, distributed outward by armies of AI-infused bots, manipulating the algorithms of the web itself. In turn, the role of the tactical-operations officer might be replaced by the only entity able to effectively battle back: another artificial intelligence. The result will be algorithms battling over the hearts and minds of humans.

It is easy to downplay the effects of these online battles, but to do so ignores how the lessons of counterinsurgency are likely to cross with the new features of LikeWar. As the former head of Joint Special Operations Command General Stanley McChrystal told a conference of military officers in the Middle East, "For the foreseeable future," the online space of social media will be as crucial a domain to any war as that of the air, land, or sea. The reason, he explains, is, "There is a war on reality. . . . Shaping the perception of which side is right or which side is winning will be more important than actually which side is right or winning."[70]

Key Resulting Questions

- What aspects of our relationship to information will change in future insurgencies?
- What will the LikeWar battles between insurgents and counterinsurgents look like in the future? Are we prepared to fight and win them? How will we even know?

Conclusions

The most powerful evidence that we are in a time of historic change is that these technology trends, and their resulting effects on the world, are so diverse they can be a bit overwhelming. Their challenge is not merely that they ripple out in many different directions, but that we are not yet in a position to answer many of the questions of possibility and propriety that they raise, especially for a realm so prone to uncertainty as war. This is okay to admit. As Werner Herzog sagely put it, "Sometimes a deep question is better than a straight answer."[71] Yet, in all this uncertainty, one key takeaway lesson emerges from this survey of technology and its potential effect on counterinsurgency in the future: In a time of massive change, those that choose to stand still, to ignore the trends and not adjust appropriately, are making a choice through their inaction. They are choosing to lose the wars of tomorrow.

Endnotes

1 The following scene is from P. W. Singer and Emerson T. Brooking, *Likewar: The Weaponization of Social Media*, Boston: Houghton Mifflin Harcourt, 2018.

2 "SMEIR: Social Media Environment and Internet Replication," *SMEIR*, https://www.smeir.net/, accessed March 18, 2019.

3 John Arquilla et al., eds., "Cyberwar Is Coming!" in *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Calif: Rand, 1997, https://www.rand.org/pubs/reprints/RP223.html.

4 The above scene is from Singer and Brooking, *Likewar*.

5 Candace Rondeaux and David Sterman, "Twenty-First Century Proxy Warfare: Confronting Strategic Innovation in a Multipolar World," New America, February 20, 2019, https://www.newamerica.org/international-security/reports/twenty-first-century-proxy-warfare-confronting-strategic-innovation-multipolar-world/.

6 David Kilcullen, "Three Pillars of Counterinsurgency," US Government Counterinsurgency Conference, Washington D.C., 2006, http://www.au.af.mil/au/awc/awcgate/uscoin/3pillars_of_counterinsurgency.pdf.

7 "Format of US Overseas Internal Defense Policy (USOIDP)," CIA, January 1, 1962, https://www.cia.gov/library/readingroom/document/cia-rdp78-06207a000100050008-4.

8 J.C.R. Licklider, "Licklider Describes the 'Intergalatic Computer Network,'" April 25, 1963, http://www.historyofinformation.com/detail.php?entryid=1029.

9 "From Brick to Slick: A history of Mobile Phones," *Wired*, March 2019. https://www.wired.com/2009/03/gallery-cell-phone-history/.

10 P. W. Singer and Emerson T. Brooking, "Terror on Twitter," *Popular Science,* December 11, 2015, https://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media.

11 Donald Rumsfeld, "Transforming the Military," *Foreign Affairs*, June 2002, https://www.foreignaffairs.com/articles/2002-05-01/transforming-military.

12 Arthur K. Cebrowski and John H. Garstka, "Network-Centric Warfare: Its Origin and Future," *Proceedings* 124, no. 1/1,139, January 1998), https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future.

13 Patrick Lin, "Pain Rays and Robot Swarms: The Radical New War Games the DOD Plays," *Atlantic*, April 15, 2013, https://www.theatlantic.com/technology/archive/2013/04/pain-rays-and-robot-swarms-the-radical-new-war-games-the-dod-plays/274965/.

14 P.W. Singer, "Wired for War," HMH, 2009; April Glaser and Rani Molla, "The Number of Robots Sold in the US Will Jump Nearly 300 Percent in Nine Years," *ReCode*, April 3, 2017, https://www.recode.net/2017/4/3/15123006/robots-sold-america-growth-300-percent-jobs-automation.

15 Oriana Pawlyk, "Pentagon Still Questioning How Smart to Make Its Drone Swarms," *Military.Com*, February 7, 2019.

16 Henry Conrad, "Here's What Jobs Robots Will Be Taking over in the near Future," *ZME Scienc*e, September 15, 2015, https://www.zmescience.com/research/robot-jobs-15092015/.

17 Molly Kinder, "Learning to Work With Robots," *Foreign Policy*, July 11, 2018, https://foreignpolicy.com/2018/07/11/learning-to-work-with-robots-automation-ai-labor/.

18 Steve LeVine, "Robots May Have given Trump an Edge in 2016," *Axios*, July 8, 2018, https://www.axios.com/robots-automation-populist-uprising-2016-presidential-election-45400a64-9ee3-4a46-b473-ab822429631b.html.

19 Abdel Bari Atwan, *Islamic State: The Digital Caliphate*, Oakland, California: University of California Press, 2015.

20 Peter Newman, "IoT Report: How Internet of Things Technology Growth Is Reaching Mainstream Companies and Consumers," *Business Insider*, Jan. 28, 2019 https://www.businessinsider.com/internet-of-things-report

21 United Nations, *2018 Revision of World Urbanization Prospects,* 2018, available at https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html

22 Thomas McMullan, "What Does the Panopticon Mean in the Age of Digital Surveillance?" *Guardian*, July 23, 2015. https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham

23 Bradley Boughton, "2017 Cyber Security Threats, Predictions, Funding & Trends," *Glocomms*, February 22, 2017, https://www.phaidoninternational.com/industryinsights/2017-cyber-security-threats-predictions-funding-and-trends-715030103047878.

24 Michelle Drolet, "Botnets: Is Your Network Really Protected?" *CSO*, March 13, 2017, https://www.csoonline.com/article/3179430/botnets-is-your-network-really-protected.html.

25 Chris Meserole, and Alina Polyakova, "Disinformation Wars," *Foreign Policy*, May 25, 2018, https://foreignpolicy.com/2018/05/25/disinformation-wars/.

26 David Canellis, "China Is Forcing Blockchain Devs to Dox Users, Censor Content," *TNW*, January 10, 2019, https://thenextweb.com/hardfork/2019/01/10/china-blockchain-censorship/.

27 Elsa B. Kania, "数字化－网络化－智能化: China's Quest for an AI Revolution in Warfare," *The Strategy Bridge*, June 8, 2017, https://thestrategybridge.org/the-bridge/2017/6/8/-chinas-quest-for-an-ai-revolution-in-warfare.

28 "Artificial Intelligence (AI) Trends," *Mad Scientist Laboratory*, December 14, 2017, https://madsciblog.tradoc.army.mil/11-artificial-intelligence-ai-trends/.

29 Elizabeth Woyke, "General Electric Builds an AI Workforce," *MIT Technology Review*, June 27, 2017, https://www.technologyreview.com/s/607962/general-electric-builds-an-ai-workforce/.

30 "Deere to Advance Machine Learning Capabilities in Acquisition of Blue River Technology," *PR Newswire,* September 6, 2017, https://www.prnewswire.com/news-releases/deere-to-advance-machine-learning-capabilities-in-acquisition-of-blue-river-technology-300514879.html.

31 Jonathan Merritt, "Is AI a Threat to Christianity," *Atlantic*, February 3, 2017, https://www.theatlantic.com/technology/archive/2017/02/artificial-intelligence-christianity/515463/.

32 Amie Tsang and Michael J. de la Merced, "Morning Agenda: Masayoshi Son Warns of the Singularity," *New York Times*, September 20, 2017, https://www.nytimes.com/2017/09/20/business/dealbook/masayoshi-son-softbank-artificial-intelligence.html.

33 Lee Rainie and Janna Anderson, "Code-Dependent: Pros and Cons of the Algorithm Age," Pew Research Center, February 8, 2017, https://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/?utm_content=buffera79ab&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

34 Feng Zhang, "Questions and Answers about CRISPR," *Broad Institute,* https://www.broadinstitute.org/what-broad/areas-focus/project-spotlight/questions-and-answers-about-crispr.

35 Antonio Regalado, "China's CRISPR Twins Might Have Had Their Brains Inadvertently Enhanced," *MIT Technology Review*, February 21, 2019, https://www.technologyreview.com/s/612997/the-crispr-twins-had-their-brains-altered/.

36 Luke Dormehl, "This Scientist Can Control a Swarm of Drones with His Thoughts," *Digital Trends*, July 15, 2016, https://www.digitaltrends.com/cool-tech/drone-swarm/.

37 Philip Perry, "New MIT Device Can Read Your 'Inside Voice', Marking the Dawn of Telepathy Tech," *Blg Think*, April 11, 2018, https://bigthink.com/philip-perry/you-can-use-the-internet-telepathically-using-this-device-developed-at-mit.

38 Rhiannon Williams, "Solar-Powered Drone Is Capable of Flying for up to a Year at a Time," *I News*, May 4, 2018, https://inews.co.uk/news/technology/solar-powered-drone-is-capable-of-flying-for-up-to-a-year-at-a-time/.

39 Martin Evans, "'3D Printed Gun' Discovered by Police," *The Telegraph*, October 25, 2013, https://www.telegraph.co.uk/news/uknews/crime/10403432/3D-printed-gun-discovered-by-police.html.

40 Nick Waters, "ISIS Is Building Bombs to Arm Its Drone Air Force," *War Is Boring*, February 10, 2017, https://medium.com/war-is-boring/isis-is-building-bombs-to-arm-its-drone-air-force-4179ce3befa9.

41 Meserole and Polyakova, "Disinformation Wars."

42 "Why TensorFlow," TensorFlow, accessed March 28, 2019, https://www.tensorflow.org/.

43 Eric Schmitt, "Pentagon Tests Lasers and Nets to Combat a Vexing Foe: ISIS Drones," *New York Times*, September 23, 2017, https://www.nytimes.com/2017/09/23/world/middleeast/isis-drones-pentagon-experiments.html.

44 "Houthi Drones Kill Several at Yemeni Military Parade," *Reuters*, January 10, 2019, https://www.reuters.com/article/us-yemen-security/houthi-drones-kill-several-at-yemeni-military-parade-idUSKCN1P40N9.

45 Becky Ferreira, "The Race to Launch the First Student-Built Rocket into Space Is On," *Vice Motherboard*, February 23, 2018, https://motherboard.vice.com/en_us/article/3k77jb/the-race-to-launch-the-first-student-built-rocket-into-space-is-on.

46 Peter W. Singer, "The 2018 State of the Digitial Union: The Seven Deadly Sins of Cyber Security We Must Face," *War on the Rocks*, January 30, 2018, https://warontherocks.com/2018/01/2018-state-digital-union-seven-deadly-sins-cyber-security-must-face/.

47 Jack Wallen, "Five Nightmarish Attacks That Show the Risks of IoT Security," *ZDNet*, June 1, 2017, https://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/.

48 "Saudi Arabia oil facilities ablaze after drone strikes," *BBC.com*, September 14, 2019. https://www.bbc.com/news/world-middle-east-49699429

49 The Coalition Invasion Force Numbered Roughly 380,000 Vs Roughly 1.3 Million Defenders. Katzman, Kenneth "Iraq: Post-Saddam Governance and Security," *fpc.state.gov/*. Congressional Research Service. Retrieved 23 September 2014.

50 Dennis C. Blair and Jon M. Huntsman Jr., "The IP Commission Report," National Bureau of Asian Research, May 2013, http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

51 Paul Triolo, and Jimmy Goodrich, "From Riding a Wave to Full Steam Ahead," *DigiChina* (blog), February 28, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/riding-wave-full-steam-ahead/.

52 P. W. Singer and Emerson T. Brooking, "Eastern Arsenal," *Popular Science*, accessed March 28, 2019, https://www.popsci.com/blog-network/eastern-arsenal.

53 Cade Metz and Natasha Singer, "Newspaper Shooting Shows Widening Use of Facial Recognition by Authorities," *New York Times*, June 29, 2018, https://www.nytimes.com/2018/06/29/business/newspaper-shooting-facial-recognition.html.

54 Jim Giles, "Cameras Know You by Your Walk," *New Scientist*, September 19, 2012, https://www.newscientist.com/article/mg21528835-600-cameras-know-you-by-your-walk/.

55 "Predictive Analytics for Geopolitical Risk," *PreData*, accessed March 28, 2019, https://www.predata.com/.

56 Marc Bain, "New 'Camouflage' Seeks to Make You Unrecognizable to Facial-Recognition Technology," *Quartz*, January 6, 2017, https://qz.com/878820/new-camouflage-promises-to-make-you-unrecognizable-to-facial-recognition-technology/.

57 Tim Maly, "Anti-Drone Camouflage: What to Wear in Total Surveillance," *WIRED*, January 17, 2013, https://www.wired.com/2013/01/anti-drone-camouflage-apparel/.

58 David Hambling, "Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon," *New Scientist*, August 10, 2017, https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/.

59 Brian Michael Jenkins, "International Terrorism: A New Kind of Warfare," Santa Monica, CA: RAND Corporation, 1974, https://www.rand.org/pubs/papers/P5261.html.

60 United States Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism, Update on Results of Retrospective Review of Russian-Related Election Activity, hearing on Twitter, Inc. January 19, 2019, https://www.judiciary.senate.gov/imo/media/doc/Edgett%20Appendix%20to%20Responses.pdf; Philip Haoward and Bence Kollanyi, "Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum," ComProp Research Note, 2016, https://arxiv.org/pdf/1606.06356.pdf; "Facebook expands scope of Russian influence on Americans for second time," *USA Today*, Nov. 1, 2017. https://www.usatoday.com/story/tech/2017/11/01/facebook-says-146-million-americans-targeted-russia-campaign/821306001/.

61 "Mexico election: Concerns about Election Bots, Trolls and Fakes," BBC, May 30, 2018. https://www.bbc.com/news/blogs-trending-44252995;
Andrew Beaton, "How Russian Trolls Inflamed the NFL's Anthem Controversy," Wall Street Journal, Oct 22, 2018 https://www.wsj.com/articles/how-russian-trolls-inflamed-nfls-anthem-controversy-1540233979?ns=prod/accounts-wsj;
"Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate," American Journal of Public Health, Oct 2018. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6137759/

62 Natasha Lomas, "Lyrebird Is a Voice Mimic for the Fake News Era," *Tech Crunch* (blog), April 25, 2017, https://techcrunch.com/2017/04/25/lyrebird-is-a-voice-mimic-for-the-fake-news-era/.

63 Shunsuke Saito et al. "Photorealistic Facial Texture Inference Using Deep Neural Networks," December 2, 2016, https://arxiv.org/abs/1612.00523.

64 Anh Nguyen et al. "Plug & Play Generative Networks: Conditional Iterative Generation of Images in Latent Space," November 30, 2016, https://arxiv.org/abs/1612.00005.

65 Will Knight, "Meet the Fake Celebrities Dreamed Up by AI," *MIT Technology Review*, October 31, 2017, https://www.technologyreview.com/the-download/609290/meet-the-fake-celebrities-dreamed-up-by-ai/.

66 Carl Vondrick, Hamed Pirsiavash, and Antonio Torralba, "Generating Videos with Scene Dynamics," 29th Conference on Neural Information Processing Systems, Barcelona, Spain, 2016, http://www.cs.columbia.edu/~vondrick/tinyvideo/paper.pdf.

67 Matt Chessen, "The MADCOM Future," Atlantic Council, September 26, 2017, https://www.atlanticcouncil.org/publications/reports/the-madcom-future.

68 "A Voice Deepfake Was Used to Scam A CEO Out Of $243,000," *Forbes*, September 3, 2019. https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#55261b4c2241.

69 Singer and Brooking, *Likewar*.

70 General Stanley McChrystal, "War in the 21st Century," Remarks at ECCSR, UAE, Oct 22, 2017.

71 Marc Spitz, "Werner Herzog Says 'The Internet Has Its Glorious Side,'" *New York Times*, August 18, 2016, https://www.nytimes.com/2016/08/21/movies/werner-herzog-lo-and-behold.html.

CHAPTER 26

"Cyber FID": The Role of Cyber in Foreign Internal Defense

Whitney Kassel and Philip Reiner

Approaches to warfare continue to shift dramatically and rapidly in the digital information era, as they have in other moments of epochal change. In the past, evolutions in warfare have impacted special operations forces (SOF) early, as such forces are frequently on the front lines of US engagement abroad, whether in active conflict, "preparation of the battlefield," or clandestine operations. This has not been the case, however, for the integration of digital-age capabilities, specifically cyberwarfare, into certain aspects of the SOF mission. While already integral to many aspects of modern warfare, cyber tools and tactics have yet to be integrated broadly into the frequently SOF-led "foreign internal defense" (FID)[i] and its manifestations in counterterrorism, counterinsurgency, stability operations, and unconventional warfare. The lack of wide SOF integration is true both in the context of ongoing "hot" conflicts and with longer-term great-power competition. As adversaries expand their asymmetric operations and attack US interests in the cyber domain—often below the threshold of armed conflict—SOF will increasingly be called upon to apply their unique capabilities and comparative advantages to undertake cyber missions, in some cases "by, with, and through" partner forces as part of the FID mission. These challenges will require new operational concepts, skillsets, and resources, as well as careful consideration of risks and second- and third-order effects.

Cyberwarfare[ii] through partners and proxies to achieve strategic effect is not a hypothetical exercise. Russia, China, Iran, the Islamic State (ISIS; Daesh), and others execute these types of missions aggressively, building capacity and using proxies to conduct information operations (IO) and offensive cyberattacks. There are also examples of partnered cyber operations being conducted on behalf of the larger US government at the national and strategic level. In fact, the September 2018 National Cyber Strategy lists "building international partner capacity" as a key objective.[1] However, in order to successfully counter adversary campaigns, many of which occur at the operational and tactical levels, SOF must investigate and pursue the systematic integration of defensive, IO, and/or offensive cyber elements into the FID tool set, enabling partner nations to protect their networks and exploit cyber tools to achieve shared objectives. SOF may achieve this by using existing resources or personnel or relying on contracted support and various partnership models within

i Joint doctrine defines FID as "participation by civilian agencies and military forces of a government or international organization in any of the programs or activities taken by a host nation (HN) government to free and protect its society from subversion, lawlessness, insurgency, violent extremism, terrorism, and other threats to its security." Refer to United States Joint Chiefs of Staff. *Foreign Internal Defense*. Joint Publication 3-22. Washington, D.C. August 17, 2018.

ii For brevity, this chapter deploys the term "cyber" in a broad sense to include operations in other domains that may more readily be understood as "cyber-enabled" operations.

the US government and/or private sector. This is already beginning to take shape in real time, in a variety of geographic domains. The cyber domain pervades all modes of future combat activity, whether preparatory or in delivering effects, and SOF's proven "by, with, and through" model will need to adapt accordingly. Based on extensive interviews with practitioners and policy makers, this chapter provides a broad framework for SOF planners to begin conceptualizing the necessary elements of "cyber FID."[iii]

Current Environment

Scholars, journalists, government officials, and military organizations have reserved great time and attention to the increasing criticality of the cyber domain in modern warfare, a fact underscored by frequent reports of the strategic use of cyber tools by the US government,[2iv] its allies,[3v] and, most important, its adversaries.[4vi] Only in the last case, however, have actors deployed cyber tools and weapons through proxies, whether defensive, offensive, or as part of an influence or information operations campaign. This gap between US and adversarial employment may seem marginal in the current security environment, but over time, the strategic advantage of working through proxies in cyberspace will prove significant or even decisive. As Tom Gjelten predicted in 2013, "We're no longer just hurling mass and energy at our opponents in warfare; now we're using information, and the more you have, the less of the older kind of weapons you need."[5]

The United States is far from lagging in the deployment of cyber capabilities in warfare and the operations that both precede and prevent conflict.The intelligence community, US military, and Department of State (DOS), among others, have enhanced their capabilities in the cyber domain dramatically since the early 2000s. With the formation of a unified combatant command, US Cyber Command (CYBERCOM), in 2009, the Department of Defense (DOD) actively signaled its intent to integrate cyber operations into the nation's defense strategy, including offensive cyber operations against its enemies. These operations, along with those of the National Security Agency (NSA) and others, have already shifted the character of twenty-first-century conflict.

Early examples of US government cyber operations can be traced to what can be considered "national" assets, organizations operating within the beltway—whether NSA, the Central Intelligence Agency (CIA), or, more recently, CYBERCOM—and

iii Interviewees for this chapter included representatives from the CIA, Headquarters Department of the Army G-3/5/7, Joint Task Force Ares, Office of the Under Secretary of Defense for Intelligence, Office of the Under Secretary of Defense for Policy, NSA, Naval Post Graduate School, New America Foundation, Special Operations Command, Special Operations Command-Central, SOCEUR JFHQ-C (MARFORCYBER), SOCPAC JFHQ-C (MARFORCYBER), United States Army Cyber Command, United States Army John F. Kennedy Special Warfare Center and School, CYBERCOM, and the US National Security Council Cyber Directorate. Interviews were also conducted with representatives from private industry who requested anonymity.

iv For example, Stuxnet, the ongoing campaign against ISIS, and instances of "persistent engagement."

v For example, US cooperation with Estonia.

vi For example, Russian deployment of malware against Ukrainian forces and the Syrian opposition, Iranian training of Hezbollah in use of social media and electronic warfare, and Iranian training of Syrian forces.

largely above the fray of day-to-day tactical operations. This has changed somewhat in recent years, particularly after the August 2018 rescission of the Barack Obama–era Presidential Policy Directive 20 (PPD-20).[6] While it remains unclear what policy framework was established in its stead, the Donald Trump administration loosened PPD-20 constraints, giving the commander of CYBERCOM the authority to be more aggressive in the use of force in cyberspace, with less coordination and oversight from civilian authorities in the Pentagon or White House.[7]

In the same vein, both the US military and intelligence community have pushed cyber operations, or at least their effects, "forward" in recent years, conducting influence operations and cyber espionage in support of combat operations in Iraq, Syria, and elsewhere.[8] In 2015, Joint Task Force ARES, an NSA/CYBERCOM joint unit, systematically dismantled the ISIS media network through an offensive cyber campaign known as Operation Glowing Symphony.[9] General Tony Thomas, then United States Special Operations Command (USSOCOM) commander, credited the classified cyber operation as directly supporting the counter-ISIS offensive on the ground.[10] In early 2019, US forces also reportedly executed a cyberattack against Kata'ib Hezbollah, an Iranian-sponsored militia group.[11]

While cyber operations have grown in importance among the tools available to US forces, at least via the national-level entities that support them, those forces have simultaneously become increasingly reliant upon and intertwined with partner-nation forces on the ground. During his administration, President Obama frequently advocated "leading from behind" and working by, with, and through allies to achieve US policy objectives.[12] The Trump administration has furthered this approach, dramatically drawing down conventional troop levels in Afghanistan, Syria, and Iraq, while leaving small groups of SOF in place to conduct counterterrorism strikes and other operations in partnership with host nation forces.[13] USSOCOM's 2019 strategy encapsulates this approach as a core tenet for the Army Special Operations Forces (ARSOF): "ARSOF supports joint force and interagency efforts, primarily through a partnered approach."[14] While these partnerships may, in some cases, involve assistance in the defense of partner-nation telecommunications networks,[15] they have not generally included cyberwarfare.

In contrast, US adversaries regularly leverage partner forces in their cyber operations. For example, the Russians notoriously use proxies to conduct cyber operations, though, in most cases, the partners they leverage are private organizations[vii] working in support of Russian campaigns, as opposed to allied governments.[16] Iran has similarly used cyber proxies to conduct operations, training the Syrian Army and Hezbollah to use online influence tactics and even conduct offensive cyber operations against its adversaries.[17]

vii Unlike conventional warfare, the preponderance of cyberwarfare skills can be found outside the government, an aspect also important in the US context, as we explore in this chapter.

The History of Foreign Internal Defense

While the US military has not yet conducted a large number of cyber operations by, with, and through partner nations, the broader construct of working through host nations and indigenous nonstate actors has been an essential special operations doctrine and missions since their inception. Even before the formation of SOCOM in 1987, SOF's predecessors in the Office of Strategic Services during World War II worked primarily with partner forces behind enemy lines. Today, one of SOF's five core missions is FID: "civilian and military agencies of a government in any of the action programs taken by another government or other designated organization to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to their security." Moreover, FID underlies why SOF was devised in the first place.

The FID mission, specifically the way SOF commonly implements it,[viii] has evolved along with the state of warfare itself, from enabling counterinsurgency and combat operations on the part of the Republic of Vietnam armed forces in the 1960s and 1970s (when FID was not even a doctrinal construct) to accompanying Iraqi Special Operations Forces on capture-kill missions against al-Qaeda in Iraq in the 2000s and ISIS in the 2010s. The SOF version of FID also incorporates related nonkinetic operations, including Military Information Support Operations (MISO) and Civil Affairs Operations (CAO), and is often aligned with assistance to civilian government entities on the part of the US DOS, US Department of Justice, US Agency for International Development, and others.

In all these arenas, FID and its corollary, unconventional warfare (by which SOF support "resistance movements" to prepare for a potential uprising or overthrow of a foreign government), are designed to help the US government work itself out of a job, so that eventually host nations can defend their territories and populations and conduct operations without the direct support or participation of US entities.[18] Historically, FID has also included using surrogate forces to facilitate preparation of the battlefield in advance of anticipated larger-scale conflict—an applicable area of effort when considering the potential cyber element of future FID missions.

As the FID mission has evolved and advanced, the technology SOF uses and instructs partner forces to deploy on the battlefield has transformed dramatically, from mortars to High Mobility Artillery Rocket Systems (HIMARs), Morse code to satellite systems, and radio towers to airborne media platforms. While the technology has changed, the core aspects of the FID mission have not, and likely will not, even as warfare advances from land and sea to multidomain efforts including cyber and space. These core aspects include, and will continue to focus on:

- training and equipping partner forces,
- the use of surrogates to advance partner and US strategic objectives,
- "direct action" or combat operations together with partner forces,
- information operations and civil affairs.[19]

viii SOF are far from the only parties that conduct these operations.

The assemblage of these missions and the details of implementation vary dramatically over time, and by country and region. For example, since the invasion of Afghanistan in 2001, the United States has conducted a broad range of activities that could fall within the construct of FID. These activities vary from training in jurisprudence and human rights to a relentless counterterrorism campaign in which Afghan Special Forces are frequently brought on capture-kill raids against Taliban and al-Qaeda targets. Over the last forty years, operations to support partner forces in El Salvador, Honduras,[20] Senegal, Liberia,[21] Thailand, and the Philippines[22] also fall under the FID rubric, each with their own unique characteristics.

Based on dozens of interviews with serving and retired military and civilian officials, the integration of cyber operations to support FID remains nascent. From an institutional perspective and at an operational level, the closest SOF has come to "cyber FID" is communications assistance provided by 18E technology specialists as part of Operational Detachment Alpha (ODA) Special Forces teams, and similar communications personnel on Marine Corps and Navy special operations teams.[ix] These personnel may assist local forces in setting up secure telecommunications networks, avoiding insecure communications methods (e.g., cellular phones and land lines), and deploying basic cyber hygiene activities to include those protecting online web presences and social media activity. However, considerable and uniquely SOF-specific opportunities exist that may expand cyber activities and operations in support of the FID mission set across every region in which SOCOM operates.

Cyber What?

What is considered "cyber" within the US government varies by department, service, and personal opinion—we will leave those debates to other venues. In the FID context, it is easiest to understand cyber operations in three main categories: defensive operations, information operations, and offensive operations. While somewhat simplistic, these categories allows us to consider the tools, training, and authorities that might be required for the majority of hypothetical cyber operations, as well as the potential risks and second- and third-order effects of engaging in these activities by, with, and through partner forces in cyberspace. It is also important to note the application of these types of cyber assistance will depend largely on the type of "partner force" being considered.

The level of cooperation in which the US government is willing to engage will vary dramatically depending on the partner in question. For example, sharing between the United States and the United Kingdom will far outpace what might be provided to other "Five Eyes" nations. The circles of trust and willingness to share will decrease as the US government considers partners with fewer shared objectives and less

ix Note, from an institutional perspective, "cyber FID" anecdotal cases have gone further, and there are several examples of international cooperation in cyber at national and strategic levels.

ability to control the proliferation of deployed cyber tools and capabilities. Operational urgency may shift the US government's calculus with regard to willingness to share.

Defensive Operations

As noted earlier, operations resembling defensive cyber FID are, and have for some time been, part of ongoing missions within the US government. These include assisting host nations with protecting public and private critical infrastructure from cyberattacks or sabotage—as seen in the United Kingdom, Estonia, and Ukraine—and helping partner forces in Iraq and Afghanistan "harden" their networks against espionage and cyberattacks. However, most of these operations are not currently being conducted under SOCOM auspices. Per our research, the known examples of SOF pursuing these missions, in particular in US Central Command (CENTCOM) and US Africa Command (AFRICOM), are anecdotal but seem poised to expand. These defensive cyber FID missions involve SOF components within the geographic commands supporting the network security of partner forces. Simultaneously, conventional forces, the Department of Defense, and other US government agencies spearhead the broader protection of host-nation infrastructure in support of national-level host-government entities.

The potential to expand and institutionalize defensive cyber FID as part of SOCOM's FID mission toolset is vast and would have significant benefits to US and partner forces globally. The need is also increasingly acute. In many cases, partner forces and their civilian counterparts in allied nations are extremely vulnerable to cyberattack, whether those attacks are aimed at debilitating a government or society, or at gathering information on those forces' plans, operations, and Tactics, Techniques, and Procedures (TTPs). Information on how to exploit vulnerabilities in commonly used hardware and software systems is widely available to adversaries, who can easily employ the information to gain access to allied networks. Defending those networks is far more difficult than accessing them; as in all cyber operations, the attacker needs to succeed only once, while those defending their networks must succeed every day. Powerful destructive tools remain broadly available to adversaries, necessitating key training and assistance to defend against adversaries' tactics.

Potential also exists to take tactical-level, SOF-driven defensive cyber FID beyond ongoing conflicts in places like Ukraine and Iraq and apply it to longer-term great-power competition by giving allied forces tools to protect their networks from adversaries. Adversaries are using supply-chain dominance and the construction of telecommunications infrastructure as strategic footholds. These adversary tactics present an opportunity for the United States in terms of long-term preparation of the environment, intelligence collection, and access to signals intelligence and will help prevent the United States from ceding strategic ground that may prove critical in coming years. In addition, allies in regions like Africa and South America, where China has been building sophisticated and all-but-unavoidable telecommunications

infrastructure,[23] will likely soon find themselves requiring significant assistance to protect their communications from unwanted eyes and ears.

Based on the doctrinal SOF mission set, which includes (but is not limited to) FID, we believe forward-deployed SOF teams are best positioned to implement defensive cyber FID at the tactical level in the immediate term. SOF missions require the placement and access to partner forces. SOF often live and work alongside partner forces, building relationships and gaining understanding of cultural context and language. SOF also train, equip, and cooperate with allies, the exact skillset required to conduct cyber FID. It should be noted that not only SOF can conduct these operations. Cases likely arise in which augmentees from other government organizations or even the private sector will be required to conduct certain missions, particularly extremely technical ones.

A number of models exist on which the defensive cyber FID mission could be based. Overall, it is not difficult to imagine how defensive cyber tools could fit into the capabilities already provided to allies through SOF and FID missions all over the world. SOF already work with partner forces in the fields of intelligence, surveillance, and reconnaissance (ISR); electronic warfare; forensics; radio and satellite communication; and, in some cases, nascent cyber operations. Providing SOF teams, specifically 18E personnel on ODAs, with mobile "cyber tool kits" that can be brought forward easily and given to partner forces, with instructions on how to implement basic cyber hygiene, would add cybersecurity to the effects of those existing tools.

Information Operations

From Russian interference in the 2016 US presidential elections, the 2017 French elections, and the 2019 European Union elections to the use of social media in attacks against the United Kingdom, Syria, and Ukraine, little doubt exists the manipulation of online information to achieve political and strategic effects is one of the most (if not the most) critical domain in which US forces will operate in the twenty-first century.[24] There is also little doubt US adversaries have quickly surpassed our defensive capabilities in the sophistication and widespread use of information operations to undermine US interests and promote their own. As the United States works to close this gap and build up its own capabilities in the IO domain, it will need to both enhance its partners' capabilities and develop ways to work with its allies to achieve desired effects and to dominate the IO landscape.

Of the two IO models mentioned previously—outright training/assistance and cooperation—the latter may be the more urgent one to address. This is because partner forces' knowledge and understanding of the IO environment in their own country or region and their ability to operate in that space make them extremely valuable assets in US-led IO operations. For example, consider the establishment of online identities and networks, which could spread a particular narrative in support of a US objective in a partner nation. True residents of that nation, and native speakers

of its language(s), are far more believable and inherently legitimate than anything even a sophisticated US actor could create.[x]

Thus, it is in the United States' strong interest to increase the IO capabilities of its partner nations, both to support those nations' security objectives and to enhance the base through which US IO campaigns can reach target audiences. There are several examples of this at the national and strategic level. Specifically, during the 2018 US midterm elections, the US partnered with European nations[25] to help prevent Russian interference similar to that seen in the 2016 presidential elections. Similar partnerships with SOF and tactical units could directly support partner operations by preparing the battlefield in regions where government support may be low or tentative. Moreover, these partnerships could convince civilian populations to leave a dangerous area prior to operations or debunk antigovernment messages that could pose a direct threat to partner forces.

There is inherent risk in providing sophisticated IO techniques to forces who may ultimately use them in ways that either do not align with US objectives or pose ethical and/or legal challenges. As we move from defensive to IO and offensive cyber FID, these risks increase exponentially. In the case of IO, adverse effects are most likely to surface if partner forces campaign to discredit critics or undermine the free press or open elections. These are real risks and should be closely considered when implementing this type of cyber FID. However, these risks are no more severe than the potential risks of providing those same allies with the lethal capabilities the US government has long provided. Similarly, the US can and should implement careful monitoring of the IO environment in nations where this type of assistance is provided. The US should also hold partner forces accountable for the use of these tools, potentially through the cessation of this and other assistance, when necessary.

Offensive Operations

While certainly the most controversial and complex of cyber operations, SOF-enabled partner-force offensive cyber operations have the significant potential, and failing to explore this domain presents an extremely high risk. As noted previously, US adversaries have already enabled their proxies to conduct offensive cyberattacks, with devastating effects in Ukraine and elsewhere. Without some level of assistance in this domain, US allies will cede a strategic advantage in their own struggles, putting US strategic objectives at significant risk.

As with defensive and IO cyber missions, some level of cooperation in the offensive domain exists already between the United States and its close allies. Few details are available in the unclassified domain, but operations such as Stuxnet indicate the US government is open to sharing offensive cyber tools with certain allies under certain circumstances. These types of missions likely make use of highly classified tools

x While this chapter specifically addresses FID, in which partner nations are wittingly supported by and operating with US forces, FID missions provide additional—while still under Title X—benefits worthy of significant consideration that go beyond the nature of this chapter's remit.

developed within the US government. Such tools would almost certainly not be shared with other allies because of the high risk of exposure, as well as the uncertainty of how such tools might be used once they have left the control of the United States and select allies.

In the operational and tactical contexts occupied by SOF, particularly through efforts under the FID mission set, this level of sophistication and secrecy generally would not be required, given the technical proficiency and level of threat faced by many SOF allies in places like CENTCOM and AFRICOM. There are a number of widely available and relatively easy-to-use offensive or "hacking" tools, from mimikatz26 to Mirai27 and the tools used in Triton28 or Sandworm29 malware attacks, whose exposure poses no significant risk to the United States. While these tools are unlikely to have dramatic effects against technologically sophisticated actors like Russia and China, they could still prove helpful, if not decisive, in many cases.

These tools are widely available online, but partners with whom SOF conduct FID worldwide may not have the technical expertise to understand and exploit such tools without US assistance (or that of our adversaries, who may step in if we do not). Access to offensive tools could allow partner forces to gather sensitive intelligence by infiltrating adversary networks (intelligence to which the United States would most likely also gain access), shut down or sabotage adversary operations from a safe standoff, avoid direct conflict in which they may lack the upper hand and be defeated, or establish a foothold on enemy networks ("leaving a cache," as one senior expert suggested) for use in future operations.

While the physical access necessary to conduct these types of operations may arise only through partnered operations via the FID mission, national-level efforts undertaken by other departments and agencies are also necessary. Tactical-level operations can supplement these national-level efforts in ways unique to the SOF community. In many environments, this capability could prove decisive, particularly as adversaries increase their use of cyber tactics not only on the national level but also on the battlefield.

Providing offensive cyber tools to allies or even simply teaching them to use the tools available in the public domain carries significant risk. In an already incredibly complex cyber-threat landscape, the distribution of capabilities across public and private industry, as well as regionally, makes effective defense and offensive operations challenging in the best of circumstances. Further complicating the picture by providing capabilities to additional actors, regardless of the origins or availability of the tools, would arguably undermine US interest in some cases, as it attempts to keep up with these developments and stay ahead of the threat landscape. In the long term, however, the same methods the United States has used to control weapons—from night vision goggles to F-16s—over many decades of FID and security assistance can be applied to offensive cyber weapons.

Dating back several decades, US security assistance has played a critical role in the implementation of US foreign policy. However, it has always carried significant risk,

such as powerful weapons and capabilities falling into the wrong hands, being used by allies in unintended ways, or simply proliferating in unpredictable and dangerous ways. The US government has set up a system of controls to try to prevent these outcomes, from "Leahy vetting" to end-use monitoring (EUM). While these controls are far from perfect, they have, in many cases, reduced the risk that must be weighed against the potential benefit of equipping allies with critical tools. This same calculus can and should be applied to cyber tools, with the risk of providing certain capabilities being weighed carefully against the benefits to US allies and the US strategic objectives those alliances and operations serve.

Roles, Responsibilities, Authorities, and Resources

If policy makers choose to pursue cyber FID, then SOCOM and its partners will need to consider carefully how to appropriately resource and authorize broad-scale implementation of cyber and cyber-enabled FID. At this time, the most critical issue limiting the implementation of cyber FID, or any additional cyber mission, is the availability of resources. The US government possesses limited expertise and capability in the cyber domain, skills desperately needed to defend US networks and conduct operations on behalf of the US government. Because of these limitations, SOCOM and the services may not have the resources to conduct cyber FID with their current force structure. Rather, existing personnel will require additional training and equipment to implement many of the operations described above. In cases where existing SOF personnel do not possess or cannot obtain the requisite skillsets easily, outsourcing to forces from the services, reserves, CYBERCOM, or NSA that have been trained specifically to operate "forward" and in denied areas, may prove more efficient than extensive training of SOF. This is taking shape in real time, with partners around the globe. As the "SOF Truths" state:

> *Although SOF are highly skilled and extraordinarily trained, to maximize effectiveness, they often require non-SOF subject-matter experts and capabilities. . . . This truth is also applicable to the Cyber Workforce, which is often dependent on Signal, Intelligence, Electronic Warfare, Fires, and Information Operations capabilities as well as interagency, multinational, and commercial partners.*[30]

Per existing legislation, authorities that could be relied on for both cyber defensive and information operations under Title 10 (DOD security cooperation) and Title 22 (DOS security assistance)[xi] funds include Section 333, 1206/2282, Section 127E,

xi "Title 22 funds are appropriated to the State Department, which often transfers them to DOD, which in turn manages and executes most security assistance programs. Title 22 includes Foreign Military Sales programs. Title 22 is less flexible in some ways, mainly because Congress authorizes and appropriates these funds on a by-country and by-program basis and requires congressional notification and permission to move funds from one effort to another." Refer to Kelly, Terrence K., et al. *Security Cooperation Organizations in the Country Team: Options for Success*. Santa Monica, CA, RAND Corporation Arroyo Center, 2010. https://www.rand.org/pubs/technical_reports/TR734.html

and Section 1202.[31] However, once operations move past those delineated in Title 10 and into Title 50,[32] different conversations will be required. For example, while the authorities to conduct defensive cyber FID operations already exist, the authorities required to implement offensive cyber FID, in particular, are not currently available to most SOF. These authorities will need to be carefully coordinated with CYBERCOM, the intelligence community, and other parts of DOD to ensure legality, strategic alignment, and prevention of mission overlap in cyberspace.

However, if leadership at the White House and DOD determine cyber FID to be a priority, exact details regarding its implementation can and will be untangled. At this early stage, policy makers must not focus on ownership or bureaucratic positioning but on the mission itself and its criticality to defending US interests in the short and long terms.[33]

Conclusion

The current lack of cyber elements in the FID toolset undermines US efforts to maintain the advantage in both great-power competition and confined, regional missions. Lawmakers, privacy advocates, and others raise valid concerns about how the proliferation of cyber tools at the tactical level might impact US interests; however, the sands are shifting toward full digitization of warfare, and such concerns will not slow the trend or change what is necessary to compete on tomorrow's battlefield. Our adversaries have experimented with and deployed cyber tools through proxies and partners in ways that directly undermine US national security, while avoiding kinetic engagement. As the United States seeks not only to compete with these efforts in the short term but also to maintain its influence in strategic regions and "prepare the battlefield" for future conflict—particularly in areas where long-term adversaries are making significant investments—we must use existing boots on the ground to seed capabilities and partnerships. SOCOM is already deploying these forces as part of their FID mission set, working hand in hand with partner forces who need cyber capabilities. The United States must use this presence to expand its cyber capabilities. As one senior DOD official explained, "demand is going to exceed supply." The time in which that becomes a true statement is coming fast—in some cases, it is already upon us.

Bibliography

Brown, Benjamin. "Expanding the Menu: The Case for CYBERSOC." Small Wars Journal, June 2018. https://smallwarsjournal.com/jrnl/art/expanding-menu-case-cybersoc.

Childress, Michael. *The Effectiveness of US Training Efforts in Internal Defense and Development: The Cases of El Salvador and Honduras.* RAND Corporation, National Defense Research Institute. Santa Monica, CA. 1995.

Duggan, Patrick M. "Man, Computer, and Special Warfare." *Small Wars Journal*, January 2016. https://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare.

Duggan, Patrick M. "UW in Cyberspace: The Cyber UW Pilot Team Concept." *Special Warfare* 27, no. 1 (January–March 2014), 69, http://static.dvidshub.net/media/pubs/pdf_14790.pdf.

Duggan, Patrick M., and Oren, Elizabeth. "US Special Operations Forces in Cyberspace." The Cyber Defense Review, Vol. 1, No. 2 (FALL 2016), pp. 73-80 (8 pages). https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1590227/us-special-operations-forces-in-cyberspace.

Gladding, Ryan S., and McQuade, Sean P. *Cyber-Enabled Unconventional Warfare: The Convergence of Cyberspace, Social Mobilization, and Special Warfare.* Thesis, Naval Post Graduate School, Monterey, CA. December 2015. https://calhoun.nps.edu/handle/10945/47951.

Graja, Claire (Rapporteur). *SOF and the Future of Global Competition.* Center for Naval Analysis (CNA). May 2019. https://www.cna.org/CNA_files/PDF/DCP-2019-U-020033-Final.pdf.

Lyngaas, Sean. "NSA's Joyce Outlines How US Can Disrupt and Deter Foreign Hacking." Cyberscoop, February 28, 2019. https://www.cyberscoop.com/rob-joyce-nsa-disrupt-foreign-hacking/.

McCoy, William H. *Senegal and Liberia: Case Studies in US IMET Training and Its Role in Internal Defense and Development.* RAND Corporation, National Defense Research Institute. Santa Monica, CA. 1994.

Munoz, Carlo. "Do Special Operations Forces Need Their Own Elite Cyberwarfare Team?" *Daily Dot*. January 2016. http://www.dailydot.com/opinion/specialoperations-elite-cyberwarfare-team

Nakasone, Paul M. "A Cyber Force for Persistent Operations." *Joint Forces Quarterly*. 1st Quarter 2019. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf

O'Brien, Michael (Master Sergeant). *Foreign Internal Defense in Iraq: ARSOF Core Tasks Enable Iraqi Combating-Terrorism Capability*. Originally published in the January-March 2012 edition of Special Warfare. Accessed via the US Army John F. Kennedy Special Warfare Center and School website, https://www.soc.mil/SWCS/SWmag/archive/SW2501/SW2501ARSOFCoreTasksEnableIraqiCombatingTerrorismCapability.html.

Smeets, Max. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly*, p. 90-113. Fall 2018. https://cisac.fsi.stanford.edu/publication/strategic-promise-offensive-cyber-operations.

Taw, Jennifer Morrison. *Thailand and the Philippines: Case Studies in US IMET Training and Its Role in Internal Defense and Development.* RAND Corporation, National Defense Research Institute. Santa Monica, CA. 1994.

Tebedo, Jason C. *Special Operations and Cyber Warfare*. Naval Postgraduate School (Master's Thesis), December 2016. https://calhoun.nps.edu/handle/10945/51622.

Vavra, Shannon. "US Cyber Command has shifted its definition of success." Cyberscoop, April 24, 2019. https://www.cyberscoop.com/cyber-command-success-tim-haugh/.

United States Department of Defense. *The Department of Defense Cyber Strategy.* Washington, D.C. April 2015.

United States Department of Defense. *Cybersecurity Reference and Resource Guide 2018.* US Department of Defense, Chief Information Officer, Cybersecurity Strategy and International Division. Washington, D.C. May 24, 2018. Cleared for open publication on August 22, 2018.

United States Department of the Army Headquarters. *Cyberspace and Electronic Warfare Operations*. Army Field Manual (FM) 3-12. April 2017.

United States Department of the Army Headquarters. *Foreign Internal Defense*. Army Techniques Publication (ATP) 3-05.2. August 2015.

Endnotes

1 The White House, United States Government. *National Cyber Strategy*. Washington, DC. 2019. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

2 Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Broadway Books, 2014; Pomerleau, Mark. "How Cyber Command can limit the reach of ISIS," The Fifth Domain, September 17, 2019. https://www.fifthdomain.com/dod/cybercom/2019/09/17/how-cyber-command-can-limit-the-reach-of-isis; Lopez, C. Todd. "Persistent Engagement, Partnerships, Top Cybercom's Priorities," Defense.gov, May 14, 2019. https://www.defense.gov/Newsroom/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities.

3 United States Embassy in Estonia, "Joint Statement on the Third US-Estonia Cyber Dialogue," Media Note, US Department of State, Office of the Spokesperson, June 7, 2019. https://ee.usembassy.gov/u-s-estonia-cyber-dialogue.

4 Cerulus, Laurens. "How Ukraine Became a Test Bed for Cyberweaponry," Politico, February 20, 2019. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks; Jones, Sam. "Russia Steps up Syria Cyber Assault." Financial Times, February 2016. https://www.ft.com/content/1e97a43e-d726-11e5-829b-8564e7528e54; https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks; Schaefer, Ben. "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism," *Georgetown Security Studies Review*, March 11, 2018. https://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism; Caravelli, Jack, and Sebastian Maier. "Deciphering Iran's Cyber Activities," Dirasat, No. 18, Rabi 1, 1438, December 2016, King Faisal Center for Research and Islamic Studies, Pg. 25. http://www.kfcris.com/pdf/27b74972d7db3c7547badfbf7f9ddbd158c8e256cd743.pdf.

5 Duggan, Patrick M., "Strategic Development of Special Warfare in Cyberspace," *Joint Forces Quarterly* 79, 4th Quarter, October 1, 2015, https://ndupress.ndu.edu/Media/News/Article/621123/strategic-development-of-special-warfare-in-cyberspace/. Duggan was quoting Tom Gjelten, "First Strike: US Cyber Warriors Seize the Offensive," *World Affairs* (January–February 2013).

6 United States, and Obama, Barack. "US Cyber Operations Policy," Presidential Policy Directive (PPD)-20. White House, October 16, 2012. (Note: while widely available online, PPD-20 was leaked illegally by Edward Snowden as a Top Secret Presidential Policy Directive).

7 Chesney, Robert. "Offensive Cyber Operations and the Interagency Process: What's at Stake with the New Trump Policy," *Lawfare: Cybersecurity and Deterrence*. August 16, 2018. https://www.lawfareblog.com/offensive-cyber-operations-and-interagency-process-whats-stake-new-trump-policy.

8 Vavra, Shannon. "U.S. Cyber-Offensive against Isis Continues, and Eyes Are Now on Afghanistan, General Says," CyberScoop, September 17, 2019. https://www.cyberscoop.com/isis-jtf-ares-cyber-offensive-afghanistan/.

9 Temple-Raston, Dina. "How the US Hacked ISIS," *National Public Radio*, September 26, 2019. https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

10 Lamothe, Dan. "How the Pentagon's Cyber Offensive against ISIS Could Shape the Future for Elite US Forces," *Washington Post*, December 16, 2007. https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-isis-could-shape-the-future-for-elite-u-s-forces/.

11 Lamothe, Dan. "How the Pentagon's Cyber Offensive against ISIS Could Shape the Future for Elite US Forces," *Washington Post*, December 16, 2007. https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-isis-could-shape-the-future-for-elite-u-s-forces/; Starr, Barbara. "US Carried Out Cyber Attack on Iranian-Based Militia," CNN, June 25, 2019. https://www.cnn.com/2019/06/25/politics/us-iranian-proxy-cyber-attack/index.html.

12 Goldberg, Jeffrey. "The Obama Doctrine," *The Atlantic*, April 2016. https://www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/.

13 Terse, Nick. More U.S. Commandos Are Fighting Invisible Wars in the Middle East." *The Intercept*. September 25, 2019. https://theintercept.com/2019/09/25/special-operations-command-military-middle-east/

14 US Army Special Operations Command. *Army Special Operations Forces Strategy*. October 2019. https://www.soc.mil/AssortedPages/ARSOF_Strategy.pdf.

15 Expert interview content, Marine Corps Special Operations Command.

16 Maurer, Tim. "Cyber Proxies and the Conflict in Ukraine." Chapter 9 in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015. https://ccdcoe.org/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf.

17 Brewster, Thomas. "Syrian Electronic Army Hackers Are Targeting Android Phones With Fake WhatsApp Attacks," *Forbes*, December 5, 2018. https://www.forbes.com/sites/thomasbrewster/2018/12/05/syrian-electronic-army-hackers-are-targeting-android-phones-with-fake-whatsapp-attacks/#15c7be266ce4.

18 "Unconventional Warfare Pocket Guide," United States Army Special Operations Command, Deputy Chief of Staff G3, Sensitive Activities Division G3X. April 2016. https://www.yumpu.com/en/document/view/55714545/unconventional-warfare-pocket-guide.

19 United States Joint Chiefs of Staff. Foreign Internal Defense. Joint Publication 3-22. Washington, D.C. August 17, 2018.

20 Childress, Michael. The Effectiveness of US Training Efforts in Internal Defense and Development: The Cases of El Salvador and Honduras. RAND Corporation, National Defense Research Institute. Santa Monica, CA. 1995

21 McCoy, William H. Senegal and Liberia: Case Studies in US IMET Training and Its Role in Internal Defense and Development. RAND Corporation, National Defense Research Institute. Santa Monica, CA. 1994.

22 Taw, Jennifer Morrison. Thailand and the Philippines: Case Studies in US IMET Training and Its Role in Internal Defense and Development. RAND Corporation, National Defense Research Institute. Santa Monica, CA. 1994.

23 Wright, Bianca. "Made in China: Africa's ICT infrastructure backbone." CIO Magazine, March 22, 2020. Accessed at this link on 24 April 20: https://www.cio.com/article/3533435/made-in-china-africas-ict-infrastructure-backbone.html.

24 Mueller, Special Counsel Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. US Department of Justice. Washington, D.C. March 2019; Greenberg, Andy. "The NSA Confirms It: Russia Hacked French Election 'Infrastructure,'" WIRED Magazine, May 9, 2017. https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure; Birnbaum, Michael and Craig Timburg. "EU: Russians Interfered in Our Elections, Too," Washington Post, June 14, 2019. https://www.washingtonpost.com/technology/2019/06/14/eu-russians-interfered-our-elections-too; Rayner, Gordon. "Russia Launches Cyberwar on UK as Macron Offers to Mediate Syria Crisis," Sydney Morning Herald, April 16, 2018. https://www.smh.com.au/world/europe/russia-launches-cyberwar-on-uk-as-macron-offers-to-mediate-syria-crisis-20180416-p4z9t7.html; Helmus, Todd C., et al. Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe. The RAND Corporation: Santa Monica, CA. 2018.

25 Lyngaas, Sean. "Cyber Command's Midterm Election Work Included Trips to Ukraine, Montenegro, and North Macedonia.: Cyberscoop. Accessed at this link on 24 April 20: https://www.cyberscoop.com/cyber-command-midterm-elections-ukraine-montenegro-and-north-macedonia/.

26 Greenberg, Andy. "He Perfected a Password-Hacking Tool—Then the Russians Came Calling," *WIRED Magazine*, November 2017. https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/.

27 Graff, Garrett. "How a Dorm Room *Minecraft* Scam Brought Down the Internet," *WIRED Magazine*, December 2017. https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.

28 Giles, Martin. "Triton Is the World's Most Murderous Malware, and It's Spreading," *MIT Technology Review*, March 2019. https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/.

29 Greenberg, Andy. "Inside the Discovery of Sandworm, the World's Most Dangerous Hackers," Vanity Fair, The Hive, October 29, 2019. https://www.vanityfair.com/news/2019/10/the-discovery-of-sandworm-the-worlds-most-dangerous-hackers; Greenberg, Andy. "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History," WIRED Magazine, October 17, 2019. https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

30 Fogarty, Stephen G., and Jamie O Nasi. "Special Operations Forces Truths: Cyber Truths." *The Cyber Defense Review*, Vol. 1, No. 2 (Fall 2016), pg. 24, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Special_Operations_Forces_Truths_Fogarty_Nasi.pdf?ver=2018-08-01-090211-527.

31 Shiel, Annie. "A CIVIC Quick Reference Guide: US Law & Policy on the Use of Military Force and Lethal Operations – Part II (Partnered Operations)," Center for Civilians in Conflict. August 2018. https://civiliansinconflict.org/blog/quick-reference-us-law-aumf-part-two/. The article provides explanations of each of these relevant DOD and State Department authorities.

32 Wall, Andru E., "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." *Harvard* National Security Journal. 2011. https://www.soc.mil/528th/PDFs/Title10Title50.pdf.

33 Active duty senior DOD official, who requested anonymity in agreeing to be interviewed for the purposes of this project.

CHAPTER 27

Open Minds, Open Societies, and Hybrid Conflict

David Bray and Vint Cerf

Recognizing that predicting the future is fraught with challenges, this chapter strives to highlight the still unfinished work of the internet and focuses on the human impacts of five categories of technical and social work that are needed. Special operations forces (SOF) seeking to win hearts and minds in future conflicts must take a people-centered approach or risk winning the metaphorical, short-term battle only to lose the long-term war.

The Internet, Open Minds, and Open Societies

The internet seems to have become a source of division and frustration in society, not succeeding fully in its goal of bringing different groups together. It *can* bring us together—yet it can also contribute to the devolution of social institutions that once required us to interact and converse in person to achieve social and cultural unity. Never has 50 percent of humanity (i.e., the approximate percentage of people on the planet with access to the internet in 2018) had access to so much new information per day.[1] Yet with that access comes a challenge of our modern age: each of us can find information that supports our preferred beliefs.

We each can and do experience "confirmation bias" (where we "plus up" information that reinforces our existing views and dismiss information that challenges them) and "cognitive easing" (in which, if something is repeated enough, we become comfortable with it and believe it to be true, even if it is not). Both confirmation bias and cognitive easing have much to do with human biology. The time and energy it takes to reexamine every aspect of our beliefs daily is overwhelming, so we don't.

Countering confirmation biases produced by mis- and disinformation delivered by the internet or other publicly available sources presents a difficult challenge. Additional facts may not be sufficient to overcome someone's existing confirmation bias. Indeed, more facts can result in a backlash in which individuals reject facts and reaffirm their existing beliefs.

Thus, SOF operators wanting to counter misinformation online will need to recognize both that everyone has biases and that providing more facts may not overcome misinformation. Alternatively, the ability to listen with curiousity to the views of others over a prolonged period of time will be necessary to build rapport and make shifting beliefs less a short-term battle of facts and more a long-term agreement on how to interpret situations in different contexts. In a crisis or short-fused situation doing so might be impossible. Fortunately, not every day brings crisis, and even in crisis scenarios, the period afterward can provide a time to listen, communicate, and attempt to understand different perspectives. By this means we may become better

informed should further crises happen. We forecast a future need for more SOF operators who engage populations by,

- Listening with curiosity, seeking to understand;
- Avoiding reducing issues to binary positions;
- Being willing to walk a mile in the shoes of others.

The more humans seek to understand others' points of view, the more humans will be aware that our own perspectives and views change and shift constantly as new experiences impact our way of thinking and seeing the world.

Subsequent sections of this chapter examine the different ways internet-based technologies are shaping societies, the battlefield, geopolitics, and SOF activities, and how SOF and external partners can seek to preserve open societies despite the increasing threats of hybrid conflicts that polarize free societies.[2]

How Are Internet-Based Technologies Shaping Open Societies?

Through shared narratives, law enforcement, and technologies, people have shaped social norms and reshaped the distribution of power (i.e., the capability to compel or oblige someone to take a certain course of action). In the twenty-first century, we face a big question: "Quo Vadis?" Where do we want communities and human societies to go, especially given the rate at which new technologies challenge the distribution of power within our societies? There are both huge opportunity for improving our communities with people-centered approaches and significant concern that our digital future may not be as rosy as we would like it to be.

Humans are tool users, and our tools connect to our use of narratives, laws, and technologies to distribute power. Ten thousand years ago, we used fire and stone tools to make the transition from a nomadic lifestyle to agrarian settlements.[3] Tools helped give rise to civilization, including the advances of writing, the development of calendars to aid agriculture, and navigation of the seas.

Even before the start of human civilizations, human nature included selfish instincts that challenged the formation of larger communities beyond immediate family members. While some civilizations generated social order through sheer physical force, compelling obedience, others generated social order through a system of laws that sought to protect communities from the greed, envy, or other hurtful elements of its members. Such societies did not develop laws purely for altruistic reasons. The laws also solidified the power of rulers and included different forms of taxation of the products of their subjects' labor.[4]

For most of human history, people met or knew on the order of 100 different other people.[5] In terms of human history, only recently did we start living in groups that were more than family members. Even more recently could most of us travel to and live in a town that was not where we were born. By comparison, most of

us encounter 80+ different people in a single day who are not immediate family members. When we lived in small agrarian groupings, elders could provide answers to just about every question about how to live and thrive: when you should plant crops and how to plant, harvest, and defend them from pests; and when to know bad weather was approaching. With the internet and other digital technologies, this has changed. A science that better understands human-and-computer interactions involving groups is essential to enable SOF and its partners to better navigate the future. The internet, globalization, and increasing interdependence of the planet has created an environment that is cognitively very different from our ancestors' world.

Laws and legal processes distributed power, and in several cases of early civilizations, solidified the power of community members to compel or oblige others to perform certain actions. These same mechanisms also enabled larger groups of people to coexist more peacefully, at least to the extent that the distribution of power did not motivate any part of the community to revert to sheer physical force to change this distribution.[6]

As communities grew, so did their use and development of more advanced tools. Metallurgy produced bronze and iron tools and weapons, bows and arrows, and later both gunpowder and flintlock firearms. Such technological developments had the effect of expanding civilizations and disrupting the distribution of power within societies.[7] Certain advances, such as the assembly line, required new laws to protect individuals from a consequent asymmetric distribution of power associated with these technologies, such as long work hours in unsafe working conditions. The ethics of societies also shifted, embodied in new laws—such as those against child labor.

Developments such as railroads allowed certain individuals to aggregate power. Other developments, such as radios, enabled communications that challenged the distribution of power. In some cases these technologies helped highlight discrimination against subgroups in societies and provoked the creation of laws protecting civil rights. On the other hand, as in the case of Nazi Germany's use of "People's Radio," radio was sometimes used to foment mobs and create dangerous echo chambers of thought.

How Are Internet-Based Technologies Shaping the Battlefield?

> *"The categories of warfare are blurring and no longer fit into neat, tidy boxes. One can expect to see more tools and tactics of destruction—from the sophisticated to the simple—being employed simultaneously in hybrid and more complex forms of warfare"*[8]
>
> ***—Robert Gates***

Since the mid-1990s, when home dial-up service and early browsers for surfing the World Wide Web (such as Mosaic and Netscape Navigator) accelerated consumer adoption of the internet, networked devices have grown in number, producing an

ever-increasing amount of data. The uptake of these technologies resulted in part from a rapid decrease in their cost and related increase in the global accessibility of the internet.

The internet has come a long way since its origins in the Advanced Research Projects Agency Network (ARPANET).[9] In terms of social outcomes, critical work must be done to reinforce transnational public trust in and security of the internet. Steps that can be taken include empowering entrepreneurs whose efforts can span national boundaries. A concerted effort is needed to build a people-centered internet to support "living learning communities," where knowledge could be found of how to thrive, adapt, and coexist in ways that celebrate a plurality of views and insights and that link rather than separate people.[10] If we recognize our interactions on the internet reflect humanity, then the internet 's future will be tied to how we choose to develop, expand, and enhance its features.

In 2003, one of the coauthors of this chapter (Bray) raised questions in the US intelligence community about whether "organizing by geographical borders would still be the predominant paradigm for societies" by 2030. He asked this question in light of the increasing impact of the internet on our lives. To consider this impact it is worth noting that during the 1990s, folks talked about "going online" as if one left the activities of the real world to enter a digital "cyberspace." As the twenty-first century dawned, it became clear the "real" and "digital" were not two different worlds. Internet activities in both "worlds" overlapped and augmented what people could achieve. Given that the internet itself obscures where a packet of information has come from or is going to geographically, it seems likely that national borders, in an internet world, will become more porous and ambiguous with time.

Having similarly responded to severe acute respiratory syndrome (SARS) in 2003 with the US Centers for Disease Control and Prevention, Bray believes infectious diseases, public health events, and other biorelated activities do not stop at national borders. One cannot forgo the reality that public health events half a world away could ultimately impact all of us. The health of the world has long-lasting, ripple effects on the economic, social, and political stability of communities. This underscores the question of whether organizing by geographical borders will remain the predominant paradigm for societies.

As of 2020, we may be transitioning from the Westfalian concept of nation-states with sovereignty defined by geography to another system. Determining what comes next has become a point of friction within and between societies, and online technlogies have been used to increase polarization and division in target countries. These tactics may have direct political effects or may be used to distract from other ongoing geopolitical conflicts. They may even be used as a precursor to a conventional battlefield engagement. Russian attacks against the Ukraine and Georgia are good examples.[11]

> *"Hybrid conflicts . . . are full spectrum wars with both physical and conceptual dimensions: the former, a struggle against an armed enemy and the latter, a wider struggle for, control and support of the combat zone's indigenous population, the support of the home fronts of the intervening nations, and the support of the international community."*[12]
>
> ***—J. McCuen***

The internet has become a tool to foster division and frustration in society, despite its demonstrated capacity to bring different groups together. Online interactions can contribute to the devolution of social institutions that once required us to interact in person and have conversations as a way to achieve social unity.

For each of us, interactions with our friends, coworkers, media, political institutions, and social networks can be mediated by the internet in such a way that they reinforce our individual worldviews, to the exclusion of other ideas and perspectives. Internet dialogues, often faceless, can produce negative emotions and result in the "shaming" of an outsider. Individuals of all political persuasions are subject to these effects, and the idea of pluralistic societies in which people accept different points of view seems to be eroding.

Consequentally, if civilization is defined by its members not automatically killing a newcomeror a new idea, modern society is at risk of becoming less civilized, less tolerant of a diversity of perspectives, and more tribal in its behavior because of the effects of the internet that seem to be eroding the idea of pluralistic societies. Similar scenarios have happened before. For example, media outlets in the United States from 1895 to 1898 "emphasized sensationalism over facts," according to an account of yellow journalism practices present at that time.[13] Human nature partly accounted for this "bump in the road." We all have biases, including confirmation biases, that manifest when we actively seek information that reinforces what we already think to be true and dismiss information that challenges our beliefs.

We also experience *cognitive ease* where the more something is repeated, the easier it becomes for us to think it must be true, even if it isn't. The journal *Science* published a study in which the researchers classified news, "as true or false using information from six independent fact-checking organizations that exhibited 95 to 98 percent agreement on the classifications. Falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information, and the effects were more pronounced for false political news than for false news about terrorism, natural disasters, science, urban legends, or financial information."[14] The big takeaway: we will be naturally motivated to believe fiction when doing so feels better than believing the truth. People seek the comfort of certainty, and when conflicting facts make them feel uncertain, they will favor fiction if it makes them feel less uncertain. While irrational, cognitive ease and confirmation bias are part of human nature.

For future geopolitical conflicts, perceptions of reality will be shaped by both information and misinformation delivered by the internet. Antagonists will undoubtedly see attitudes and beliefs as a "cognitive domain" distinct from the domains of air, ground, sea, and cyber. Forces may have military superiority in the latter four domains, only to lose legitimacy and support in the cognitive domain through targeted misinformation that erodes support.

How Are Internet-Based, Hybrid Conflicts Shaping the Warfighter, including US and Adversarial Forces?

Hybrid conflicts using the internet extend beyond the cognitive domain; they also include misuse and abuse of the cyber-related infrastructure of the internet. These issues are now important given the sheer number of network devices on the internet. Specifically, in 2015 there were approximately 14 billion network devices for 7.3 billion human beings. That's up from 7 billion network devices two years earlier. Cisco and other firms predicted there could be approximately 50 billion or more network devices globally, relative to about 8 billion people, by 2020. Cisco predicts 500 billion devices will be online by 2030.[15]

The figurative explosion in the number of network devices increases cybersecurity risks and the risks of misinformation on the internet. Warfighters face a future in which infrastructure can be used against them, whether to impede their movement or actions, to alert adversarial forces of offensive and defensive activities, or to use "digital exhaust" from the Internet of Things (IoT) to put combatants at risk.

The IoT also increases cybersecurity risks for the average consumer. Current approaches to cybersecurity, that is, relying on human experts to build and maintain "tougher digital locks" and "higher (fire)walls," will not be sustainable as the IoT continues to expand the potential attack surface. Warfighters cannot assume they can operate without detection. Their adversaries may also use infrastructure sensors and related capabilities to misinform situational awareness to produce bad strategic and tactical decisions.

IoT will make even more visible the flaws present in buggy software and the challenges of guaranteeing the security of any IT system. Human societies can encourage good "internet hygiene" practices and take preventive measures to reduce risk and improve the overall security posture of a system. However, any internet-connected device or system has inherent risks, especially from unscripted, zero-day exploits to which there may be no defense until after an attack has exploited a bug.

Taken together, because of these three concerns, communities might want to consider tackling cybersecurity differently.[16] One approach might include focusing on digital resiliency and a strategy more akin to "internet public health" aimed at both preventive measures and rapid detection, containment, and mitigation of digital threats, i.e., infectious disease control for the internet. Modeled after public health systems, such a method would emphasize teaching internet hygiene to reduce the likelihood of outbreaks. These are actions SOF could consider.

These activities also would emphasize establishing digital-threat-detection procedures focused on signs, symptoms, and behaviors to respond to polymorphic digital threats such as malware that changes signatures. In addition, a public health—like approach to digital resiliency would include mobilizing the equivalent of internet epidemiologists with the training necessary to characterize, contain, and remediate malware and digital threats as quickly as possible, should ones emerge; collaborative actions using trained experts augmented with machine learning may be essential to respond to these risks.

Hybrid Conflict and Special Operations Forces

Internet-based hybrid conflicts are shaping the SOF mission, which must accommodate the social elements of the internet. SOF must also recognize the increasing use of automated programs (bots), algorithms, and artificial intelligence (AI) to shape information flows and activities on the internet. AI-mediated and bot activites over the internet represent a dimension of hybrid conflict that has only begun to present visible signs of disruption to the public, with more disruptions expected for open societies in geopolitics, elections, commercial relations, and public perceptions of technology and other global trends. Consequentally, SOF must incorporate AI and counter-AI activities into future strategies and plans, including recognizing the historical arc of how AI has evolved in parallel with the internet.

In 1957, early AI pioneer Herbert Simon partnered with Allen Newell to develop a general problem solver that separated information about a problem from the strategy required to solve a problem. Since then, the field of AI has experienced two more waves of innovation. Starting in the mid-1960s, the second wave of AI innovation included work on rule-based expert systems represented mainly as "if-then" statements instead of procedural code. The goal of such systems was to perform tasks that expert humans could also do, such as evaluate geological sites or perform medical diagnoses.[17]

In approximately 2015, cumulative advances in the speed, size, and scale of microprocessors and computer memory reached a tipping point that triggered a third wave of AI innovation. It became possible to execute machine learning with sufficient speed and scale to benefit real-world and even real-time applications. Machine learning employs large data sets to train multilayer neural networks statistically to make accurate categorizations of what something is or is not; for example, training a machine to identify accurately images of different objects, places, or entities, or to enable natural language translation, among many other innovative applications.

Importantly, machine learning is, at best, only as accurate as the data provided to it, a textbook example of the computer-science mantra "garbage in, garbage out," where poor-quality data results in poor-quality machine learning. Moreover, machine-learning technology can be "brittle" in the sense that it may fail in unexpected ways with small input variations. Nowadays with the internet, large data sets potentially

exist that could train machine-learning instances; however, human societies must address data privacy, brittle functionality, data quality, and biases.

How Can SOF Respond to and Shape Hybrid Conflict Environments?

To address future internet-based hybrid conflicts, SOF need to renew its focus on the importance of monitoring local and global narratives, given the linkage between narratives, community norms, and the distribution of power. Humans are innate storytellers. This may have to do with consciousness, including our ability to simulate events. Stories allow us to simulate fictitious but plausible realities. By simulating events in our minds, we can "test potential scenarios" without incurring some near-fatal or fatal outcome and, thus, increase our survival chances.

Stories can be told that change behaviors. A simple visceral story of "I did X once and it caused me to puke my guts out" probably would convince several people who have never done X to avoid it.[i] If stories can be told that change behaviors, repeat behaviors over time can become "sticky" habits. Habits inculcate norms. The power of narratives lies in their ability to shape and institutionalize norms and power distribution in our human communities.

There is also increasing evidence, though, that we have developed communication and language to convince others the scenario they faced was similar to what we have also faced (i.e., "myside").[18] Some researchers now call confirmation bias "myside bias," which is adaptive.[19] If the group can collectively be on the same "myside," that may help coordinate responses to threats or opportunities.

Our world is much broader than the immediate environment we see and experience nearby; this has dangerous side effects, such as challenges in reaching consensus or agreeing on the relevant facts for a situation.

Our planet is increasingly interconnected in ways that challenge the notion of organizing into groups based on geographical boundaries. The question is, what takes its place? Affinity groups that divide different groups of humans into "us" vs. "them" labels are one possibility; however, "wars" between different affinity groups might then occur. If affinity groups alone replace how we organize, political discourse would become a winner-take-all game. Without compromise, the fabric of republics and representative democracies might well rip apart. Taken to an extreme, affinity groups are unwilling to tolerate "newcomers" and will become dictatorial autocracies, insisting that to be a member, one must think a certain way. In such a scenario, plurality of thought is not appreciated. Differences in opinion are to be ridiculed or expelled. If this were to occur, such an outcome would paint a troubling future indeed.

SOF operators need to prepare for a future that could include the following:

- More "stormy issues" occuring with increasing tempo in open societies and challenging the interests of different digitally enabled stakeholder groups.

i This is where we get into the serious challenges of misinformation online, namely that the best way for something to go viral is to make it hateful or fearful; positive narratives do not seem to go viral as readily.

- The need to address stability and security from "outside of the box" (or device, as the case might be) and to be proactive in our design thinking.
- The erosion of the nation-state in open societies, if we do not resolve issues across multiple stakeholders.

What Can Be Done to Counter Adversary Narratives and Produce Competitive Advantage?

The United States and other open societies, including several parts of Europe, are becoming collections of "echo chambers," and the internet seems to be devolving to a degree into affinity groups that homogenize ideas or beliefs about how the world works and what we should do for the world ahead. If we become a collection of intolerant affinity groups, we risks becoming autocracies of thought.

We need to remember President Lincoln's quote of "I don't like that man. I must get to know him better."[20]

We believe that to counter adversary narratives and produce a competitive advantage for open societies, our world needs a plurality of ideas and approaches to address the challenging intersection of exponential technologies, issues of globalization and global fragmentation, and questions of the future of both work and life. Members of open societies still have much work to do to help connect those on the planet who want the internet or improved access to it, and to address the digital divide even in places where the internet is available. Many of us also want to ensure a more open internet for everyone and to find new ways to address the challenges of human biases in news and information.

On December 9, 1968, computer science pioneer Douglas Engelbart gave a demonstration that later became known as "the Mother of All Demos," in which he demonstrated a computer with a graphical user interface, a mouse pointer, version control for files, user-ability to jump to other documents by clicking on hyperlinks, and many more features that we associate with how we interface with computers. For 1968, his demo of the future was truly groundbreaking.[21]

When considering the future work of the internet, it is worth remembering that Engelbart also had a vision that human intelligence could be augmented through computer-based tools. This included the idea that technologies could help humans connect, share ideas, and become "living learning communities."[22] Internet access began to accelerate in 1988, and commercial service arrived the following year. Several of Engelbart's ideas, realized in the World Wide Web, contributed to periods of exponential content and activity growth: hyperlinking web pages, sharing knowledge online, and helping humans connect.

Future SOF doctrine must recognize the importance of operating in highly networked contexts composed of humans and machines focused on adapting to and accomplishing certain tasks. These networked contexts will become increasingly important, embodying *krewes* of humans and machines operating together. Instead of assigning a specific person to a role, it may be assigned to a krewe. Krewes may float

across organizations, akin to a freelancing team that brings its own organic devices, software, and algorithms to bear on challenging topics.

Long-term, human organizations may be replaced by networked krewes bidding on work assignments, accomplishing them, and moving on to new assignments; to some degree, contractors and contracted work already parallel this concept. In the future, automated technologies may be able to help the krewe's talent and time management be smarter when it comes to the SOF mission by:

- Highlighting issues for different teams to focus on;
- Suggesting the best pairing of different team members;
- Removing some human biases from decision-making;

Not that software produced by computer scientists is infallible. In fact, we know software will have bugs and biases that human programmers may have included.Thus, future SOF efforts will need to experiment with ways to evaluate the effectiveness of krewes using automated approaches to identify and fix bugs and to pioneer ways to better communicate the tasks of algorithm to all human participants so they can spot existing bugs or biases in code.

What New Tools and Technologies Would Give US SOF Unique Advantages?

Over the last 150 years, humans have built interconnecting technologies allowing for interactaction or broadcast around the world through telegraph, telephone, radio, television, and satellites. Now we have the internet, which lies at the heart of many of the challenges modern society faces, including societal and geopolitical fragmentation, tribalism, misinformation, and disinformation. We need to recognize the lessons of history and of human nature and strive to be brave, bold, and benevolent in finding ways to build bridges rather than walls. This will be largely a people-focused challenge. Technology will take us only so far.

We propose SOF consider six steps to address the human-centric, internet-amplified challenges of misinformation, disinformation, and erosion of trust:

- Step one: Raise questions, ideas, and possible solutions to "what comes next." Most important, discuss what social and political institutions will allow for pluralistic human coexistence and encourage peaceful resolution (and forgiveness) of disputes.
- Step two: Focus on being positive. It is important to focus on positivity even in the face of hate or darkness—getting angry, sad, or giving in to those arguing against coexistence prohibits one's ability to empathize with others and strive to find the common humanity in us all.
- Step three: Reach across groups and ideological divides. If we use the internet only to associate with and get to know people we like and find

supportive of our worldviews, then we will only reinforce the age-old human paradigm of "us vs. them" and will miss the opportunity to find merit in the compassion in or insight of people with which we might not agree in principle.

- Step four: Find ways to benefit multiple groups, not just groups with which we self-identify (lest we accelerate tribalism) or from which we benefit.
- Step five: Work across communal groups and help build a world in which different ideas and people can coexist.
- Step six: Identify which choices we make that disconnect us from others. We need better designed online systems to facilitate better outcomes.

Cumulatively, these six steps could frame the work of many organizations for the decade ahead, recognizing that such challenges cannot be met by technology alone. These steps will vary in degree of difficulty depending on the level of transparency in the architectures, algorithms, and attributes of the interfaces that mediate human interaction.

What Can Initiatives outside US SOF Do to Help Make Open Societies More Resilient against Polarizing Hybrid Conflicts?

A more people-centered, positive online future requires collaboration across sectors and national boundaries and, most likely, the creation of new institutions. Such institutions must work with civil societies, private-sector companies, and public-sector organizations to produce a future with more beneficial choices, options, and freedoms for everyone. Public-sector organizations must support inclusive, open, affordable internet access to the public, given that the internet has become such a connective element in everyday life. Private-sector companies must ensure the services they provide offer both informed choices and value to help individuals and communities. Such public and private services should encourage productive, nondivisive, and nonexploitive uses of the internet. The public must encourage such activities, potentially pioneering community projects or start-ups that promote a more people-centered internet.

Tackling the unfinished work associated with the future of the internet raises many questions: how do we to hold true values as individuals, as communities, and as a world while also adapting to rapid change? The internet and its successors, whatever they may be, will weave together a tapestry of human and computing threads. Just what images will be found in this tapestry will depend on the nature of the threads and the skill and creativity with which the weaving is accomplished.

It seems clear from the considerations in this chapter that we must adopt a realistic appreciation for the way in which computing in all its generality is applied to solving social and economic problems. Our choices of algorithms affect society. We must assure that all members have equal access to the potential benefits these computing tools offer.

After World War II, in part through the Marshall Plan, the United States created global institutions modeled after US ideals—with the specific goal that another world war should be avoided at all costs. This included US military and national security institutions that to this day are unparalleled in their ability to respond to nation-state conflicts and prevent escalation of issues to world war.

The modern world is not the world of 1948. Efforts to adjust such institutions to meet the challenges of terrorism or cyber-related concerns represent Band-Aid and duct-tape solutions at best. Trying to apply laws solely by geography is challenging for the internet era, especially given the challenge of trying to apply laws to technologies that change rapidly and produce social impacts globally. There is clear pressure, however, to reinforce a Westfalian, national sovereignty model. This can be seen especially with the recent actions of the Chinese government to reinforce its "Great Cyber Wall"[23] and the Russians to build RU.NET[24] and test its ability to operate after total disconnection from the rest of the internet. Cumulatively, the era of relative peace may be ending, potentially to be replaced with a different period heretofore undefined.

It is our belief that isolationism is a bad idea. Even if the United States tries to withdraw from the world stage, the rest of the world will continue to become more connected digitally. Threats half a world away will persist and may still be able to reach us in either online or offline ways. As we as authors and associates with the People-Centered Internet have observed, some cyberthreats have already become affordable to small nations and technologically "superempowered" individuals who mean to do harm or sow chaos.

Technology solely for its own sake is also a bad idea. Some players have predicted social media and internet technology as the future forms of human connectivity. Without a people-centered focus, such technologies paradoxically could increase unrest, distrust, disengagement, and the spread of misinformation.

Following the disruptions of 9/11, nations around the world debated what type of future to pursue: One focused on individuals freedom or one that emphasizes centralized planning in the name of regional stability and that risked impedeing individual freedoms? Nowadays, most US institutions and the laws associated with them are poorly primed to respond with the agility needed for the global issues of the coming decades. These institutions need to modernize, not just their technology and capabilities but also their focus and purpose. The debate about the future often gets overshadowed by short-term political debates. Inherantly, short-term thinking does not look at either the last 70 years since the end of World War II and the potential 70 years ahead.

Conclusions

In the aftermath of World War II, the United States and its allies shaped significantly the political and legal frameworks of the modern world; however, nothing guarantees we will shape the remainder of the twenty-first century if we do not recognize that any long-term solutions to the challenges of internet-based hybrid conflicts require understanding of the social and economic dynamics of an increasingly technology-based world.

SOF face such a significant challenge when working to assist other open societies that face hybrid conflicts. The openness of the discussions and plurality of perspectives in such societies puts them at risk of being the target of weaponized disinformation. Domestic and external actors use and will continue to leverage open internet-based commerce, interactions, and discussions to their advantage. In closed societies, data collection about the activities of citizens is a common practice. In open societies, it seems we must institute defenses against inappropriate data collection to protect citizens from harm.

Unless implemented with security in mind, IoT devices used for home, health, or workplace-related interactions also will be avenues for abuse. The conundrum for open societies is to protect citizens from those who exploit internet-enabled devices while avoiding the extremes of censorship and other constraints on utility.

Given these challenges, our recommendation to US SOF is a long-term strategy based on three important pillars. The first seeks to shine a light on and share data with corporations, the public, the media, and our allies associated with what we believe are ongoing, internet-based, hybrid conflicts. This task may prove difficult as such suspicions may be speculative. Such speculation may be informed by methods and means that cannot be divulged fully because of their compromising sources. Even with such challenges, we believe more "sunlight" must be shown to all members of open societies on what we as authors sense are ongoing conflicts. This transparency is needed to exercise the strength of diversity of open societies. In the absence of transparency, the benefits of social, economic, and political discourses will diminish.

The second pillar seeks to better understand human-and-computer interactions, especially at large scales involving teams, organizations, and societies. A better science of understanding these interactions, informed by neurobiology, psychology, and anthropology, is required to forecast social risks and to gauge ways to strengthen the resiliency of the society.

The third pillar of our proposed, long-term strategy is to provide nondystopian narratives of how open societies around the world can use the internet and other technologies to advance positive ends and productive futures for all. Without these narratives, the cognitive battlefield will be ceded to those who sow anger, fear, discord, confusion, and dismay. This is terra incognita–there is no textbook for where we are going, and yet we need to develop narratives that give hope to open societies.

These narratives must offer tangible, visual, and visceral experiences, not merely words. Disney's Experimental Prototype Community of Tomorrow (EPCOT) created a plausible future world. The narratives must enable people to understand the diverse, multistakeholder practices that can cope with a complex, technology-rich world. This may take the form of a Model United Nations class for high schools and colleges. Such experiences would show how governments, technologists, civil society, and the private sector possess shared and unique responsibilities for resolving issues and implementing solutions to problems that arise.

Cumulatively, the 2020s will require SOF and its partners to adapt its doctrines more quickly and flexibly. To cope with the challenges of hybrid conflicts, we must do what we can to address the pernicious effects of misinformation, the fragility of AI-mediated decisions, and the risks posed by the IoT. We should pursue a strategy that aims for Engelbart's vision of "living learning communities." SOF's unique role provides both motive and opportunity to introduce important memes in conflicted areas that reinforce the principles of open societies and defend against authoritarian regimes that seek to undermine and fragment them.

Endnotes

1 "The Internet Is People-Centered for Almost 50 Percent of the World: Join Our Dialog!" People-Centered Internet, December 5, 2018, https://peoplecentered.net/2018/12/05/the-internet-is-people-centered-for-almost-50-of-the-world-join-our-dialog.
2 Glenn, R. "'Thoughts on 'Hybrid' Conflict," *Small Wars Journal,* 2009, https://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf.
3 Aimé, Carla, et al., Microsatellite Data Show Recent Demographic Expansions in Sedentary but Not in Nomadic Human Populations in Africa and Eurasia, European Journal of Human Genetics volume 22, 1201–1207 (2014), https://www.nature.com/articles/ejhg20142.
4 "Abraham Lincoln Imposes First Federal Income Tax," *History Channel*, A&E Television Networks, 2020, https://www.history.com/this-day-in-history/lincoln-imposes-first-federal-income-tax.
5 Tuttle, Russell Howard, "Human Evolution," *Encyclopedia Britannica*, 2020, https://www.britannica.com/science/human-evolution.
6 "Code of Hammurabi," *History Channel*, A&E Television Networks, February 21, 2020, https://www.history.com/topics/ancient-history/hammurabi.
7 Diamond, Jared. *Guns, Germs and Steel: The Fates of Human Societies,* Norton, 1997.
8 Gates, R. "A Balanced Strategy: Reprogramming the Pentagon for a New Age," *Foreign Affairs* 88, no.1 (January/February, 2009), http://www.foreignaffairs.org/20090101faessay88103-p20/robert-m-gates/a-balanced-strategy.html.
9 The ARPANET was a research project sponsored by the US Advanced Research Projects Agency (ARPA), an arm of the Defense Department, to link computers at Pentagon-funded research institutions over phone lines.
10 Waldrop, M. *The Dream Machine: J. C. R. Licklider and the Revolution That Made Computing Personal*. New York: Viking Adult, 2001.
11 https://www.bbc.co.uk/news/world-middle-east-26248275.
12 McCuen, J. "Hybrid Wars," *Military Review* (March-April): 107-113, 2008.
13 US Office of the Historian, "U.S. Diplomacy and Yellow Journalism, 1895–1898," https://history.state.gov/milestones/1866-1898/yellow-journalism, Accessed June 23, 2018.
14 Vosoughi, S., D. Roy, and S. Aral (2018) "The Spread of True and False News Online," *Science* 359, no 6380, 2018, pp. 1146-1151, https://science.sciencemag.org/content/359/6380/1146.full.
15 Cisco. "Internet of Things," https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf, Accessed June 23, 2018.
16 Cerf, V. "What Hath We Wrought?" *IEEE Internet Computing* 21, no. 4, 2017, pp. 103–104.
17 Bray, D. "The Future of Artificial Intelligence and Augmented Intelligence in Public Service." IBM Center for the Business of Government, 2018.
18 Xiaoyan Qiu, et al., "Limited Individual Attention and Online Virality of Low-Quality Information," Nature Human Behavior, June 26, 2017, https://www.nature.com/articles/s41562-017-0132.
19 Kappes, Andreas, et al., "Confirmation Bias in the Utilization of Others' Opinion Strength," Nature Neuroscience, December 16, 2019, https://www.nature.com/articles/s41593-019-0549-2.
20 "Forty-Three Inspiring Motivational Quotes about Teamwork Collaboration," Inc.com, https://www.inc.com/jeff-haden/43-inspiring-motivational-quotes-about-teamwork-collaboration.html.
21 Waldrop, *Dream Machine*, 2001; Jacobsen, A. *The Pentagon's Brain: An Uncensored History of DARPA, America's Top-Secret Military Research Agency*. New York: Back Bay Books, 2015.
22 Waldrop, *Dream Machine*, 2001.
23 Cunningham, Maura Elizabeth. "'The Great Firewall of China' Review: The Chinese Cyber-Padlock," *Wall Street Journal*, March 10, 2019, https://www.wsj.com/articles/the-great-firewall-of-china-review-the-chinese-cyber-padlock-11552245606.
24 Doffman, Zak, "Putin Signs 'Russian Internet Law' to Disconnect Russia from the World Wide Web," *Forbes*, May 1, 2019, https://www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web/#7ee3735b1bf1.

CHAPTER 28

Artificial Intelligence: Risks and Opportunities for SOF

Paul Scharre

Recent rapid advances are changing the art of the possible in artificial intelligence, with significant opportunities for special operations forces (SOF) across the full range of SOF missions. This chapter gives a brief overview of current trends in AI and some examples of potential AI applications to SOF missions.

The AI Revolution

Few technologies are advancing as rapidly and dramatically as artificial intelligence. Since 2012, the field of AI has seen a renaissance in machine learning, driven by advances in data and computer processing power. From 2012 to 2018, the amount of computer processing power, or "compute," applied to cutting-edge machine-learning advances increased 300,000-fold. This exponential rate of growth is faster than "Moore's Law," which has driven advances in computer processing power for the past several decades. Instead of doubling every two years, since 2012, compute in machine learning has been doubling every 3.4 months, an astonishing trajectory of technological development.[1]

There are few other areas related to war in which the underlying technology is evolving at such a rapid pace. Missiles are not 300,000 times faster than they were in 2012. Vehicles are not 300,000 times more fuel-efficient. Armor is certainly not 300,000 times lighter. While many technologies are improving and have significant potential should they come to fruition, AI and machine learning are already being applied to a range of industries. The US military should move aggressively to adopt AI for SOF applications.

What Is AI?

Artificial intelligence is the field of study devoted to making machines intelligent.[2] Intelligence measures a system's ability to determine the best course of action to achieve its goals in a wide range of environments.[3] The field of AI encompasses a range of methods to achieve intelligent behavior in machines.[4]

Broadly speaking, AI systems can be grouped into two general categories. The "first wave" AI systems are "expert systems" that draw on a set of rules of behavior that have been informed by human experts. An example of an expert system is an airplane autopilot, which has rules for behavior in different settings, drawing on the experience of human pilots. "Second wave" AI systems use machine learning, in which behavior is not programmed into the machine but learned from data. There are a variety of machine-learning methods, including supervised, unsupervised, and reinforcement.[5] In supervised learning, the human tells the algorithm what to look for in the data. In unsupervised learning, the human does not tell the algorithm what to look for and the

machine groups data according to patterns. In reinforcement learning, the algorithm learns by interacting with an environment and optimizes its performance to achieve a goal. "Deep learning" is a particularly powerful machine-learning approach that uses "deep" neural networks. Neural networks are connections of artificial "neurons," loosely inspired by biological brains, and deep neural networks are those that have multiple layers.

Underlying all these machine-learning approaches is a common reliance on data and compute. The exponential increases in data and compute over the past decade have enabled machine-learning methods that are effective in training machines across a range of tasks. Machine learning has yielded algorithms with human-level or superhuman performance in object classification, facial recognition, and various games, including Atari games, the Chinese strategy game Go, and real-time computer strategy games such as Dota 2 and StarCraft. Machine learning is being applied to a range of industries, including transportation, finance, and medicine.

General Methods, Task-Specific Machines

Machine-learning methods can be applied to a range of tasks, provided ample data exists and the task is sufficiently bound and has clear metrics for better performance. The applicability of AI methods to a broad range of tasks makes AI a general-purpose enabling technology, much like electricity or the internal combustion engine. Technology writer Kevin Kelly has argued, "AI will enliven inert objects, much as electricity did more than a century ago. Everything that we formerly electrified, we will now cognitize."[6] Moreover, a 2017 study conducted by the McKinsey Global Institute estimated roughly half of the tasks performed currently in the US economy could be automated using existing technology.[7] Many technology analysts have argued that AI is likely to lead to sweeping economic and social changes in the coming decades, akin to another industrial revolution.[8]

Just as past industrial revolutions enabled the creation of machines that were stronger than humans for specific tasks, the new cognitive revolution is enabling the creation of machines that are smarter than humans for specific tasks. However, much like physical machines have been, AI systems will be designed as tools to aid humans in conducting tasks. While the methods underlying AI can be applied to a broad range of problems, once trained, AI systems exhibit "narrow," or task-specific, intelligence. They may be effective at the task for which they are designed but generally have no ability to perform other tasks. For example, an AI translation application can translate between languages (provided it has been trained on those languages) but cannot understand or analyze the text. Other AI systems may be able to engage in some modest reading comprehension, and still others can create relatively realistic computer-generated text given a prompt on a topic. But all these AI systems can perform only one specific task. Useful AI systems often combine a suite of AI tools into a broader application that humans use, just as physical machines developed during the Industrial Revolution have been used for moving mechanical energy.

Forklifts, cars, tractors, trucks, buses, steamrollers, and backhoes are all machines designed to perform specific tasks and powered by the same underlying technology: the internal combustion engine. Many jobs, such as mining, construction, or road paving require using multiple different mechanical machines together. The same concept is true of AI systems, which may combine different methods and tools to build a useful cognitive system.

Current Limitations of AI Systems

One important limitation of today's narrow AI systems is that their performance often drops off dramatically when they are used outside the bounds of their systems' design. AI systems lack the reasoning abilities that allows humans to adapt to novel circumstances, which can make their performance quite "brittle." For example, the first version of AlphaGo, which reached superhuman performance in Go in 2016, reportedly suffered a major drop in performance when the size of the board was changed from the 19x19 grid board on which it was trained.[9] Similarly, multiple independent studies, including by the US government, have shown facial-recognition algorithms decrease significantly in performance when used on faces whose demographics (e.g., race, gender) are not well represented in the algorithm's training data.[10] AI systems that perform well in one setting can fail suddenly and dramatically when subject to slight changes in either the environment or their operating conditions. This has already been a factor in several deaths resulting from Tesla car autopilots, which have driven cars suddenly into parked cars, tractor trailers, or Jersey barriers.[11]

These incidents demonstrate the criticality of conducting robust testing and evaluation in realistic operating environments to better understand the boundaries of AI systems' behavior. However, even with testing, designers and users of AI systems should expect some failures, and plan accordingly, when systems are first placed in real-world operational environments, especially military ones, given their unpredictability. Failures may also occur when systems are first placed in combat environments—even if the systems have been used extensively in training—as combat environments may differ from training scenarios in critical ways, such as environmental conditions, target signatures, or adversary behavior. AI systems often excel at repeatable, precise behavior, but they can perform poorly in novel situations, a significant challenge for military applications.

AI systems are also vulnerable to manipulation, hacking, and spoofing attacks, including novel attack vectors that exploit cognitive vulnerabilities in the systems' thinking processes or learning approaches.[12] Data poisoning entails inserting hidden malicious data into the training data of a machine-learning system, corrupting its learning process and altering its behavior.[13] Adversarial data inputs are tailored spoofing attacks fed to trained algorithms that exploit weaknesses in how they process data in order to trick the algorithm.[14] For example, one team of AI researchers embedded subtle swirls into the shell of a 3D-printed turtle that caused an AI-based image classifier that identifies objects to misidentify the turtle as a rifle.[15] These

important vulnerabilities, which are common across many machine-learning methods, should be taken into account when designing and using AI systems.[16]

Uses of AI Systems

AI systems can be used to perform a range of functions. These include:

- **Classifying** data, including identifying objects, faces, or emotions;
- **Detecting** anomalous behavior inconsistent with historical data patterns, such as fraudulent financial transactions, computer malware, or human behavior;
- **Predicting** future behavior based on past data, such as recommendation algorithms for media content or improved weather predictions; and
- **Optimizing** performance of complex systems, allowing for greater efficiency in operations.

Artificial intelligence can also be used to enable autonomous systems. Autonomy is the freedom a person or machine has to perform a task. AI enables increasingly intelligent machines, which can, in turn, be granted autonomy to perform increasingly complex tasks in a wider range of environments. Autonomy can be embodied in physical systems, enabling advanced robots to perform a wider range of missions in different environments. For example, it can be used in human-occupied vehicles, in applications such as autopilot, intelligent cruise control, or active protection systems for ground vehicles. In addition, autonomy can be applied to nonphysical systems, such as autonomous cybersecurity applications.

The degree of autonomy delegated to intelligent machines is a choice made by human users, who may desire machines to perform some tasks autonomously in some environments, such as automated takeoff and landing for drones or automatic braking in automobiles. For other applications, human users may prefer greater control over the operation of the system. A range of human-machine command-and-control relationships exist. In semiautonomous systems, in which a human is "in the loop," the machine waits for human approval before performing a task. In supervised autonomy, the human is "on the loop," meaning the machine performs tasks on its own, but the human can intervene, if necessary. In fully autonomous systems, the human is "out of the loop" and cannot intervene for a period of time.

In practice, people design machines with a mix of autonomy for different tasks. For example, an automobile has some features that are fully autonomous (such as automatic seat-belt retractors or antilock brakes), some that involve supervised autonomy (such as cruise control), and others that humans direct manually (such as controlling the vehicle's movements or choosing the destination). Using autonomous systems effectively requires not only robust testing and evaluation in realistic operating environments but also educating users on the systems' capabilities and limitations to achieve trust in the machine's performance.

AI, Autonomy, and Special Operations

AI and autonomous systems have many potential applications across the breadth of SOF missions and environments.[17] Some illustrative examples are given below, but these are by no means the full range of potential applications.[18] Special operations forces will have to experiment with and adapt to new potential uses as AI technology continues to mature.

Intelligence and reconnaissance

Robotic and AI systems will present a number of opportunities for SOF to improve reconnaissance, intelligence collection, and analysis. Uninhabited aircraft, or drones, have already been a major boon to reconnaissance and intelligence collection because of their greater endurance and persistence than aircraft with humans onboard. Similarly, more advanced autonomous robotic systems will be able to persist on the battlefield for longer periods of time and operate in different shapes, sizes, and environments than humans can. Increased autonomy will allow robotic systems to penetrate into denied areas and collect intelligence even without a continuous link to remote human controllers. Unattended ground sensors will be able to monitor areas for traffic, building up patterns of life of ground activity. Small robots will be able to navigate into buildings, snake their way into tunnels or buried facilities, monitor activity, and then exfiltrate data. Robotic systems may also be vectors for delivering payloads such as cyber tools, electronic warfare, or kinetic effects.

AI will also help to process and synthesize information, allowing analysts to integrate multiple data sources and identify anomalies more rapidly. AI image classifiers can help process the glut of full-motion video data from uninhabited aircraft, and, more broadly, AI-based classifiers of any sort can help process data in any number of formats, such as audio or electromagnetic signals. One straightforward and easily applicable use for AI is automating many of the steps that humans take today in collecting, processing, analyzing, and disseminating information. Automation is most useful for routine cognitive and physical labor, and simply automating many of the tasks servicemembers perform today in intelligence analysis can help accelerate decision cycles and free up humans for other important tasks. AI tools will not be able to take on the higher-level cognitive functions that humans perform to understand an enemy's intent or to analyze courses of action, but AI tools can be useful adjuncts for human analysts to help them process large amounts of information more quickly and effectively. The net effect of AI and automation for analysts should be to accelerate the targeting cycle, allowing for more rapid and precise synthesis of information.

Force Protection and Mission Support

AI, robotic, and autonomous systems will also have a number of valuable applications to support special operations forces when infiltrating to or on an objective and in exfiltration. Robotic systems can be used for immediate reconnaissance ahead of forces in order to act as the "point person," giving teams extended eyes and ears to

detect potential threats. Similarly, robotic systems can be used to travel alongside, ahead of, and behind small teams, giving them an extended bubble of sensors to detect approaching threats. These robotic systems can consist of a mix of air, ground, sea-surface, or subsurface systems, depending on the mission environment. As robotic systems become increasingly autonomous, the operation of a robotic sensor cloud surrounding SOF teams will become practical without overtaxing the attention of team members, which would not be the case if robotic systems were controlled remotely. Increasingly, autonomous systems will also be able to react automatically to potential threats, cuing additional sensors to identify threats, and to prepare kinetic or nonkinetic defensive measures for use, if needed.

Increasing autonomy will allow robotic systems to surround, give early warning to, and help protect SOF teams when not only moving through open areas but also in Global Positioning Systems (GPS)–denied environments such as inside buildings or underground. Visual-aided navigation allows robots to move through GPS-denied environments and maintain navigational awareness, allowing swarms of air and ground robots to move ahead of SOF teams in buildings or underground to map the environment and to identify potential threats. These robotic systems could not only help protect special operations forces by giving them advance warning of threats but also allow for more rapid mission execution, as they can help map environments quickly and vector forces to find key individuals or locations to accomplish the mission.

Robotic forces can also be valuable adjuncts to SOF teams by carrying additional and resupplying equipment and evacuating casualties. Robotic teammates—using legged, wheeled, or tracked modes of locomotion depending on the terrain and mission requirements—can move alongside SOF teams, carrying additional gear, ammunition, water, or other supplies. Autonomous robotic helicopters can ferry resupply equipment to teams, even under fire or in small landing zones not suitable for larger helicopters. Autonomous helicopters or ground vehicles may be also be used for casualty evacuation to send wounded personnel more rapidly to a higher standard of care. Lastly, wearable robotics (such as exoskeletons) can help SOF personnel carry additional weight—including weapons, armor, or other mission equipment—and/or increase mobility, allowing SOF personnel to move further and farther than would otherwise be possible.

Limitations

Despite their potential ability to assist SOF, robotic systems will continue to have a number of limitations, chiefly in power and endurance.[19] The physical attributes of technologies are not improving as rapidly as the digital attributes. Therefore, future robotic systems will likely possess advanced sensors, autonomy, and decision-making abilities but will remain limited in range, payload, and endurance. On the battlefield, energy needed to power AI systems will be a limited resource, much like ammunition, water, and batteries are today. Robotic systems will likely increase, not decrease,

the SOF energy burden because—even if robotic teammates and exoskeletons can carry additional batteries and robotic systems can resupply teams rapidly—robotic tools require their own power, adding to the energy burden of small SOF teams. Energy burdens will have to be managed carefully, and some robotic systems may not be appropriate for long-duration missions or where regular battery resupply is not feasible. For some special operations missions, however, robotic systems will be a valuable addition and a force multiplier that increases mission effectiveness.

Vignette: Increased Mission Effectiveness

The net effect of these technological additions to the SOF toolkit could be a significant change in the mission effectiveness of special operations forces. Forces that today are often limited by the carrying capacity of individuals could be augmented with robotic systems of various shapes and sizes, which could help expand the situational awareness, lethality, and firepower of SOF teams. The vignette below illustrates how these tools could come together to increase significantly the mission effectiveness of a notional SOF team conducting an operation.

> *The SOF team infiltrates onto a beach that has already been secured by amphibious robotic systems that have autonomously searched the area, identified and flagged any potential mines or obstacles, and confirmed the absence of any personnel on the landing site. As the team arrives on the beach, a network of robotic systems surrounds its position giving the team early warning of any individuals approaching. On the water, low-profile sea-surface robotic vessels, networked with undersea robotic systems, warn of any potential threats approaching from the sea. On land, unattended ground sensors placed along likely avenues of approach warn of any foot or vehicle traffic, while, in the air, small aerial drones give the team a vantage point over the next terrain feature, giving them early eyes on any potential threats.*
>
> *A large-diameter robotic submersible ferries additional equipment to the beach, which the team offloads for overland movement to its objective. The team is equipped with exoskeletons to facilitate more rapid movement, wheeled robotic teammates to carry additional gear and to move with the team, and a swarm of small drones for increased situational awareness and reconnaissance.*
>
> *Robotic teammates and exoskeletons offload the weight burden of SOF personnel, allowing SOF to move rapidly to the objective. As the team moves, small ground and air robotic scouts patrol in front of, behind, and on either side of the team, giving advance warning of potential threats. This allows the team to reroute around individuals discovered*

on the way to the objective, helping the team avoid detection and maintain the element of surprise.

At the objective, robotic systems are used to augment the team in creating a security perimeter around the objective, acting as a force multiplier for the personnel on the ground. Ground and air robotic systems autonomously watch avenues of approach and egress out of the target building and warn SOF personnel of any movement.

The SOF team uses a ground robot to breach the objective, allowing team members to remain protected, and then a swarm of small aerial drones enter the building. The drones navigate and map the structure quickly and autonomously, relaying back a three-dimensional map to the team members who remain outside. Machine-learning–based image classifiers on the drones autonomously locate any individuals inside the building and objects they are carrying (such as weapons) and identify any persons who have been preloaded into a biometric database using facial recognition. This information is also relayed to the team outside, which then has the precise location of any individuals (armed or otherwise) inside the building, their disposition, and real-time video footage of their movements, all without having to enter the structure. The team decides to deploy lethal force against a number of armed individuals in the building and nonlethal measures against individuals whose status cannot be determined. SOF personnel direct the drones to carry out these actions, and the drones do so by using onboard weapons and countermeasures. Once any potential threats have been neutralized, the team moves into the building to secure it and begin site exploitation.

However, actions on the objective have compromised the team's position, and enemy forces begin rallying to counterattack. Overhead drones monitoring the surrounding area identify groups of dismounted personnel and approaching vehicles and alert SOF team members. This information allows the team to direct airstrikes to protect their position while completing actions on the objective. The team also directs overhead drones to search along planned exfiltration routes and identify any personnel or vehicles on the route. By looking at a map showing available routes with overlays of surrounding activity, the team chooses the route with the least risk of attack. Robotic systems deploy smoke screens to mask the team's movements, and large ground robotic teammates deploy ballistic shields to provide mobile cover as the team moves through an open area. Robotic decoys lure enemy

forces in the other direction, creating noise and movement away from the team's egress route.

During exfiltration, aerial drones identify an individual moving to intercept the SOF team. The team changes direction and sends a ground robot scout to intercept the individual. The individual detonates a suicide vest, destroying the robot scout, but leaving the team unharmed. Both air and ground robots secure the helicopter landing zone before the team arrives and provide situational awareness until the team is successfully extracted. If the SOF team had been pinned down in a firefight, robotic helicopters were on standby at a nearby forward arming and refueling point and could have delivered additional ammunition and extracted any casualties.

As this vignette illustrates, AI and robotic systems will not replace military personnel or alleviate the need for humans to direct and conduct military missions, but they can augment human capacity in valuable ways, offloading various tasks and assisting humans in accomplishing the mission.

Adversarial AI Uses

Artificial intelligence is a diffuse technology widely available globally to both state and nonstate actors. While cutting-edge AI research and development will remain limited to a small number of major global corporations, the AI research community is open and AI applications are freely available online for anyone to use and download.[i] Small drones have already proliferated widely and have been used by nonstate actors for attacks around the globe, and additional AI-based systems will likely follow suit.[20] Nonstate groups have already built and deployed homemade robotic systems in the Middle East, including Shia militias in Iraq possessing small armed ground robots and Syrian rebel groups using remote weapons stations.[21] As robotic and AI technology becomes more widely available, nonstate groups will likely continue to repurpose commercially available systems or design their own homemade systems.

In the near-term, the most likely impact of AI developments is that SOF will increasingly face aerial threats, as even actors with relatively modest capabilities will possess the ability to field simple drones for reconnaissance or aerial attack. These flying improvised explosive devices are unlikely to present a decisive threat to US forces, but they could effectively delay or hinder US troop movements or cause casualties. Drones could be particularly effective reconnaissance tools for adversaries, allowing them to pinpoint US units and lay in more sophisticated ambushes using other units or indirect fires. Drones equipped with explosives could

i There is an abundance of free and openly available online resources on AI and machine learning, including arXiv, Github, Google's TensorFlow, Caffe, and other repositories for technical papers, trained models, datasets, and instructional resources

also be effective against high-value soft targets, such as aircraft, similar to the 2012 Taliban attack on Camp Bastion in Afghanistan that damaged eight Marine Corps AV-8B Harrier aircraft. Nonstate groups have already attempted such an attack. In 2018, a Syrian rebel group attacked Russian bases in Syria with 13 small armed drones. Russian forces brought down all 13 drones through a combination of direct fire and electronic warfare.[22] Nevertheless, a similar but successful attack using massed small drones could disrupt operations, cause casualties, or damage high-value assets. One challenge with such a threat is drones could potentially deliver explosives with higher accuracy than mortars or rockets, allowing attackers to deliver more precise fire against key targets.

In the longer-term, autonomous self-driving vehicles pose a potentially significant terrorist threat to ground troops and installations, given ground vehicles have a much higher payload capacity than small drones. Fleets of autonomous vehicles could be laden with explosives or simply used for ramming attacks, as has occurred with human-driven vehicles against civilians in other settings. Autonomy increases the number of vehicles that could potentially be used in such an attack. Without the need for a human driver onboard the vehicle, a small group, or even a single individual, could launch a mass vehicle attack, overwhelming an installation's defenses and causing casualties.

AI developments will apply to not only robotic systems but also nonphysical AI systems, such as AI-based synthetic media (computer-generated text, audio, images, or video).[23] Terrorist groups have adopted and exploited social media for propaganda purposes, and will likely continue this trend using synthetic media. Today, tailor-made "deepfakes," fake videos created using deep learning, can be acquired online for $30.[24] Presently, the quality of most deepfake videos is not particularly good, but it is improving rapidly as computing power continues to increase. Within the next several years, high-quality deepfake videos are likely to be widely available to malicious actors. Meanwhile, high-quality synthetic voice generation is possible today. While deepfake videos can currently be detected using machine learning-based detectors, long-term trends point to the creation and availability of detection-resistant fakes, which will have significant implications for disinformation, propaganda, and other information operations.

Conclusion

AI, autonomy, and robotics technologies are evolving rapidly, presenting both new opportunities and challenges for SOF. The special operations community will need to adapt quickly to this new technology and the risks and opportunities it presents. A continual process of experimentation, rapid prototyping, and threat assessment will be essential to adapting to the AI revolution.

Endnotes

1 OpenAI, "AI and Compute," May 16, 2018, https://openai.com/blog/ai-and-compute/.

2 Nils J. Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements*, Cambridge, U.K.: Cambridge University Press, 2010.

3 Adapted from Shane Legg and Marcus Hutter, "A Collection of Definitions of Intelligence," Preprint, submitted June 25, 2007, https://arxiv.org/pdf/0706.3639.pdf.

4 For a brief nontechnical overview of AI and machine learning, see Paul Scharre and Michael C. Horowitz, "Artificial Intelligence: What Every Policymaker Needs to Know," Center for a New American Security, July 2018, https://www.cnas.org/publications/reports/artificial-intelligence-what-every-policymaker-needs-to-know.

5 On machine learning, see Tom Michael Mitchell, "The Discipline of Machine Learning," Carnegie Mellon University, School of Computer Science, Machine Learning Department (2006), and Ben Buchanan and Taylor Miller, "Machine Learning for Policymakers: What It Is and Why It Matters," Belfer Center, June 2017, https://www.belfercenter.org/sites/default/files/files/publication/MachineLearningforPolicymakers.pdf.

6 Kevin Kelly, "The Three Breakthroughs That Have Finally Unleashed AI on the World," *Wired*, October 27, 2014, https://www.wired.com/2014/10/future-of-artificial-intelligence/.

7 McKinsey Global Institute, "Harnessing Automation for a Future that Works," January 2017, https://www.mckinsey.com/featured-insights/digital-disruption/harnessing-automation-for-a-future-that-works.

8 For example, see Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond," World Economic Forum, January 14, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/; Sean Gallagher, "The fourth Industrial revolution emerges from AI and the internet of things," Arstechnica, June 18, 2019, https://arstechnica.com/information-technology/2019/06/the-revolution-will-be-roboticized-how-ai-is-driving-industry-4-0/; Alan Crameri, "Artificial Intelligence: The fourth industrial revolution," InformationAge, October 3, 2018, https://www.information-age.com/artificial-intelligence-fourth-industrial-revolution-123475170/; Daniel Araya and Creig Lamb, "Surfing the 4th Industrial Revolution: Artificial Intelligence and the liberal arts," Brookings, April 11, 2017, https://www.brookings.edu/blog/brown-center-chalkboard/2017/04/11/surfing-the-4th-industrial-revolution-artificial-intelligence-and-the-liberal-arts/.

9 Bob van den Hoek, "Can AlphaGo Win Lee Sedol on a Larger Size Board? Say, 4x the size," Quora, May 14, 2016, https://www.quora.com/Can-AlphaGo-win-Lee-Sedol-on-a-larger-size-board-Say-4x-the-size.

10 Larry Hardesty, "Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems," MIT News, February 11, 2018, http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212; Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81:1-15, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Cynthia M. Cook et al., "Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, February 2019, http://jjhoward.org/wp-content/uploads/2019/02/demographic-effects-image-acquisition.pdf; Patrick Grother et al., "Face Recognition Vendor Test (FVRT), Part 3: Demographic Effects (NISTIR 8280)," National Institute of Standards and Technology," US Department of Commerce, December 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

11 Jim Puzzanghera, "Driver in Tesla Crash Relied Excessively on Autopilot, but Tesla Shares Some Blame, Federal Panel Finds," Los Angeles Times, September 12, 2017, http://www.latimes.com/business/la-fi-hy-tesla-autopilot-20170912-story.html; "Driver Errors, Overreliance on Automation, Lack of Safeguards, Led to Fatal Tesla Crash," National Transportation Safety Board Office of Public Affairs, press release, September 12, 2017, https://www.ntsb.gov/news/press-releases/Pages/PR20170912.aspx; "Collision between a Car Operating with Automated Vehicle Control Systems and a Tractor-Semitrailer Truck Near Williston, Florida" NTSB/HAR-17/02/ PB2017-102600 (National Transportation Safety Board, May 7, 2016), https://www.ntsb.gov/news/events/Documents/2017-HWY16FH018-BMG-abstract.pdf; James Gilboy, "Officials Find Cause of Tesla Autopilot Crash Into Fire Truck: Report," The Drive, May 17, 2018, http://www.thedrive.com/news/20912/cause-of-tesla-autopilot-crash-into-fire-truck-cause-determined-report; "Tesla Hit Parked Police Car 'while Using Autopilot,'" BBC, May 30, 2018, https://www.bbc.com/news/technology-44300952; Raphael Orlove, "This Test Shows Why Tesla Autopilot Crashes Keep Happening," Jalopnik, June 13, 2018, https://jalopnik.com/this-test-shows-why-tesla-autopilot-crashes-keep-happen-1826810902.

12 Ram Shankar Siva Kumar et al., "Failure Modes in Machine Learning," Microsoft, November 11, 2019, https://docs.microsoft.com/en-us/security/engineering/failure-modes-in-machine-learning.

13 Jagielski, Matthew, et al., "Manipulating machine learning: Poisoning attacks and countermeasures for regression learning," arXiv, April 1, 2018, https://arxiv.org/pdf/1804.00308.pdf; and James Vincent, "Twitter Taught Microsoft's AI Chatbot To Be a Racist Asshole in Less than a Day," Verge, May 24, 2016; and Peter Lee, "Learning from Tay's Introduction," Microsoft, March 25, 2016, https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/.

14 Anh Nguyen A, et al., "Deep Neural Networks Are Easily Fooled: High Confidence Predictions for Unrecognizable Images," Computer Vision and Pattern Recognition (CVPR '15), IEEE, 2015; and Nicolas Papernot et al., "Practical Black-Box Attacks against Machine Learning," Preprint, submitted March 19, 2017, https://arxiv.org/pdf/1602.02697.pdf.

15 Anish Athalye, et al., "Fooling Neural Networks in the Physical World with 3D Adversarial Objects," October 31, 2017, https://www.labsix.org/physical-objects-that-fool-neural-nets/.

16 Amodei et al., "Concrete Problems in AI Safety," Preprint, submitted July 25, 2016, 4, https://arxiv.org/pdf/1606.06565.pdf; Dario Amodei and Jack Clark, "Faulty Reward Functions in the Wild," OpenAI blog, December 21, 2016, https://blog.openai.com/faulty-reward-functions/; Joel Lehman et al., "The Surprising Creativity of Digital Evolution: A Collection of Anecdotes from the Evolutionary Computation and Artificial Life Research Communities," Preprint, submitted March 8, 2018, 6, https://arxiv.org/pdf/1803.03453.pdf.

17 Miles Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," February 2018, https://maliciousaireport.com/.

18 Paul Scharre, "Robotics on the Battlefield, Part II: The Coming Swarm," Center for a New American Security, October 15, 2014, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_TheComingSwarm_Scharre.pdf?mtime=20160906082059.

19 Paul Scharre, et al., "Super Soldiers: Emerging Technologies," Center for a New American Security, October 23, 2018, https://www.cnas.org/publications/reports/emerging-technologies-1.

20 Ulrike Franke, "The Caracas attack won't be the last of its kind," *The Verge*, August 17, 2018, https://www.theverge.com/2018/8/17/17703570/caracas-drone-attack-venezuela-president-nicolas-maduro; Christoph Koettl and Barbara Marcolini, "A Closer Look at the Drone Attack on Maduro in Venezuela," The New York Times, August 10, 2018, https://www.nytimes.com/2018/08/10/world/americas/venezuela-video-analysis.html; and Dmitry Kozlov and Sergei Grits, "Russia says drone attacks on its Syria base have increased," Associated Press, August 16, 2018, https://apnews.com/2b07cc798d614d84a32ff83f6abe2e7e/Russia-says-drone-attacks-on-its-Syria-base-have-increased.

21 Adam Rawnsley and Austin Bodetti, "The Warbot Builders of the Middle East Spill Their Secrets," *Wired*, February 2, 2017, https://www.wired.com/2017/02/warbot-builders-middle-east-spill-secrets/; Robert J. Bunker and Alma Keshavarz, "Terrorist and Insurgent Teleoperated Sniper Rifles and Machine Guns," Foreign Military Studies Office, Ft. Leavenworth, KS, https://info.publicintelligence.net/USArmy-TeleoperatedSniperRifles.pdf; Robert Beckhusen, "Syria and Iraq Are Incubators for Remote-Controlled Guns," War is Boring, August 30, 2016, https://medium.com/war-is-boring/syria-and-iraq-are-incubators-for-remote-controlled-guns-27ce6004ab1f; Jassem al Salami, "An Iraqi Shi'ite Militia Now Has Ground Combat Robots," War is Boring, March 23, 2015, https://medium.com/war-is-boring/an-iraqi-shi-ite-militia-now-has-ground-combat-robots-68ed69121d21.

22 David Reid, "A swarm of armed drones attacked a Russian military base in Syria," CNBC, January 11, 2018, https://www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html.

23 John Borthwick, "Synthetic Media," render, July 29, 2018, https://render.betaworks.com/synthetic-media-d0adcc53800a.

24 Henry Ajder et al., "The State of Deepfakes: Landscape, Threats, and Impact," Deeptrace, September 2019, 5.

CHAPTER 29

Weaponized Information: Influence and Deception in the Age of Social Media

David M. Perlman, CDR Pablo C. Breuer, and Sara-Jayne Terp

> *"All warfare is based on deception. . . . The skillful leader subdues the enemy's troops without any fighting."*
>
> —***Sun Tzu,*** **The Art of War**[1]

Introduction

Since the 2016 US presidential election, much of the world has developed a keen interest in what could collectively be referred to as "information disorder." In the United States, "fake news" was the initial focus, before the term lost meaning through overuse. The news cycle has swept through "Russian election interference," "Cambridge Analytica," "microtargeting," "misinformation," "polarization," "filter bubbles," and countless other terms related to this topic. These trends reveal both a growing awareness that the information ecosystem (consisting of digital networks, traditional media, and human beliefs and communication) is a critical foundation for the politics and economy of a free and democratic society and that this foundation is crumbling. In the past, such efforts to interfere in the internal affairs of other nations would have resulted in war. Instead, today we find ourselves in a time of competition short of armed conflict.

This chapter is for readers dedicated to the defense of a free and democratic society. Our target audience is readers who are grounded in the theory of military strategy and tactics based on traditional notions of the Westphalian nation-state and the diplomatic, military, information, economic (DIME) model of the instruments of national power. Many will also be familiar with military information support operations (MISO) and other perspectives on information and communication as a form of "support"—that is, support for kinetic superiority, which is traditionally the primary focus of military strategy in Western nations. For those with this background, it may be challenging to read that the new technologies of digital communication, and particularly social networks, enable persuasion that poses an existential threat not only to the United States but also to the very idea of a free and democratic society.

How could a few Twitter bots[i] and targeted Facebook advertisements possibly count as an existential threat in a world with nuclear weapons and aircraft carriers? For readers with those questions, we include a vignette at the end of this chapter; but, in brief, *the decisions about when and how to use our mighty kinetic weapons are made by groups of people utilizing technological information systems*, and—given enough

i Fully automated accounts.

data, computational power, and broadcast bandwidth—modeling, and at least partially controling, collective human behaviors and system outputs is surprisingly easy.

Some might object that controlling collective human behavior sounds suspiciously close to science-fiction ideas of "mass mind control" and flies in the face of ideals of free will and personal responsibility, but consider the analogy of a weather report: you can't predict where and when *one* raindrop will fall, but you can certainly predict when it will rain, and that is usually all you need. Elections are routinely decided by less than one percent[2]; for that matter, many businesses live or die by 0.01 percent changes in metrics on their quarterly reports. The philosophy of free will and responsibility is beyond the scope of this article, but we urge readers to set aside any reservations and follow along with our exploration of what can be accomplished by moving a few percent of a carefully selected demographic.

We will discuss fundamental differences about these new information attacks, explain what it means for an information ecosystem to be healthy or unhealthy, and what an "attack" looks like. We will also explore the kinds of consequences that can befall political and economic systems when the information ecosystem is under attack, and we hope it will be clear that such an attack is of paramount concern, not a mere matter of "support" to kinetic military activities. We will further discuss potential countermeasures and offer some overarching recommendations. We focus primarily on democratic, free-market societies, but we will not limit our discussion to "election interference." The nation's strength requires use of all of the instruments of national power. Democracies, in particular, require the citizenry believes in the legitimacy of their leaders' power and understand how the government functions. An information attack that targets elections, and therefore casts doubt on the legitimacy of leaders, is an attack on the foundation of that democracy.

History of Communication Technology and Society

> *"Every revolution has its medium, and every new medium creates its own new form of revolution.... But revolutions come with unexpected costs. Printing liberated humanity, but also triggered centuries of religious and political struggle."*
>
> **—*Bill Kovarik*, Revolutions in Communication[3]**

Throughout history, military thinkers such as Sun Tzu, Niccolò Machiavelli, and Carl von Clausewitz have recognized the importance of misinformation. Deception is as old as warfare. New technology has always enabled misinformation. Technologists have rarely anticipated how their innovations could be abused for malice. The internet has completed a cycle in broadcasting to the masses that began with the printing press invented by Johannes Gutenberg and has fundamentally changed misinformation.

Until approximately 1445 CE, message transmission in the Western world was limited. While papyrus was invented around the second century BCE[4] it was not

universally available until much later. Broadcasting and amplifying messages required that fascimiles be made by hand and transmitted separately. Further complicating the issue of transmitting to a mass populace, literacy was limited and messages could be transmitted only as far as they could be carried physically. Transmission of messages during this time period was limited mostly to nation-states or religious institutions.

Although printing presses existed in China at the end of the first century CE[5] not until the development of the Gutenberg press in approximately 1455 did transmitting messages to a large population become easier in the West. The cost of the press, materials needed for printing, and initial typesetting were expensive and time-consuming and served to limit who could afford to mass produce their message. Literacy was still limited, and messages still had to be hand carried. The Gutenberg press catalyzed an increase in literacy throughout the West, thereby increasing the population of who could receive a "transmitted" message. The change brought about by the Gutenberg press also represents the first time creators of a technology failed to account for how it could be used against them. The Catholic Church had no objection to Gutenberg's first Latin Bible; but fifty years later, the Protestant Reformation thrived by embracing the new technology. The church was forced into a defensive strategy (presaging today's media politics) that combined attempts to censor the new media with their own extensive use of the printing press for propaganda.[6]

In the 1830s, the invention of the telegraph became the next step in the information revolution.[7] The telegraph allowed for near instantaneous transmission of messages over a long distance. The creation of the telegraph network infrastructure was initially expensive, and the transmission and reception of messages required knowledge of Morse code at both the transmitting and receiving stations. While messages could be retransmitted beyond the original source, telegraph remained a point-to-point medium not particularly well-suited for reaching a mass audience simultaneously. Transmitters had to know something about their intended recipient, and both message transmitters and recipients had to be able to reach a telegraph station. The need for infrastructure served as a gatekeeping function for who can transmit and receive messages. A government or company could simply refuse to transmit a message or deliver a transmitted message.

In 1896, the Guglielmo Marconi radio[8] provided two game-changing capabilities: the abilities to broadcast to a populace without needing to know the recipient and to receive messages without the need for specialized knowledge. The capabilities allowed for the concept of a "universal" recipient. While transmission equipment of any real power was expensive, anyone with a radio receiver within range of the transmitter could receive a message. Instantaneous delivery of messages to a large population within a relatively large area became possible. Soon after realizing the power of radio broadcasts, nation-states called for regulation at the 1906 International Radiotelegraph Convention in Berlin,[9] and the US Federal Communications Commission (FCC) was established in 1934.[10] Nation-state regulation and the prohibitive cost of high-power transmission equipment limited who could transmit. The falling cost of equipment allowed the general

populace to receive messages from their own homes and led the radio to become the preferred source of trusted news and information; message reception had become democratized. The faith in the truth of radio transmissions was so ingrained that there was widespread panic in 1938 when an entertainment broadcast, *The War of the Worlds*, was mistaken for real-world news.[11]

In 1927, the invention of the television in the United States[12] became the next innovation in the information revolution. The first commercial television station appeared in 1928, and for the first time, images could be transmitted to a mass audience. In 1936, Adolf Hitler used television transmission of the Olympic Games to convey his views of racial supremacy and to promote his form of government.[13] By the 1950s, television had become the premier way to influence populations, and access to this powerful medium was tightly controlled. As late as the 1990s, one needed a head of state to demand national television stations interrupt regularly scheduled broadcasts to carry a message. In the United STates, television broadcasts were limited to a small handful of networks who all abided by the "Television Code," and by the 1980s, there was a well-established and uniform American national culture.[14]

While the Electronic Numerical Integrator and Computer (ENIAC) was created for the United States Army in 1943[15] and the Advanced Research Projects Agency Network (ARPANET) was created in 1969,[16] computers did not fundamentally change the delivery of misinformation until much later. In the 1980s and 1990s, corporations introduced computers to a large portion of the populace. The internet became publicly available in 1991 and was widespread in US homes by 2001. While the ability to "broadcast" messages arguably started with Usenet groups in 1980, the first widely recognized social media platform was Six Degrees,[17] which did not appear until in 1997, followed by other platforms such as Friendster (2002), Facebook (2004), and Twitter (2006). While every previous advancement in communication technology democratized the *receipt* of information, transmission still remained in the hands of a select few. The internet and social media finally democratized the ability to *transmit* to a wide audience. We now live in a world where Katy Perry, an entertainer, can use Twitter to instantly reach twice as many people as the president of the United States. This democratization has had many benefits, but there are also costs. Audiences can no longer be provided any assurance of who originates a message, so provenance and authenticity of alleged facts and media is always in question. The loss of centralized coordination has led to a breakdown of shared national knowledge and identity in a nation as diverse as the United States.

The democratization of transmission to mass audience is not the only fundamental change that the internet provided to those that seek to conduct influence operations. The ability to measure the effectiveness of messaging is critical to all influence operations. In 1994, the first internet advertisement appeared when AT&T paid HotWired for space at the top of their homepage. The birth of internet advertising gave rise to tracking click-through rates as a measure of the effectiveness of any particular advertisement. On social media, beginning in 2009, Facebook's "like" and Twitter's

"retweet" buttons allowed for similar measurement of messaging effectiveness on social media platforms. This near instantaneous feedback of message effectiveness allows for much more rapid AB testing and message honing than is available via traditional media and misinformation channels.

The rise of the internet and social media has fundamentally changed the delivery of misinformation. By democratizing transmission to a mass audience, social media has removed gatekeepers who might prevent transmission of harmful messages as well as removing any assurance that a message is being transmitted from an authoritative source. Additionally, the advertisement-driven model of the internet has led to the ability to track effectiveness of messaging in near real time and allow for rapid testing, evaluation, and honing of influence messaging. In short, the informational instrument of national power can now be wielded by a small group, or even an individual. Because of this, it is necessary to understand social media as a dual-use technology and to evaluate its potential for strategic latency.

The Structure of Social Media

"Move fast and break things."

—Mark Zuckerberg[18]

The power of fully democratized mass communication makes social media a key topic from a strategic latency perspective. A social networking service[ii] such as Twitter or Facebook consists of:

- A computer system (i.e., servers, custom software) designed for the primary purpose of facilitating human users sharing human-readable information (e.g., words, pictures) with each other.
- A population of users, including individual humans as well as other account-holding entities.
- The collection of human-scale information hosted on the system (e.g., "posts," "tweets," "memes," "hashtags").
- The metadata stored on the servers that defines the graph relationships of the network, such as who is "friends" with whom and who has "liked" which posts.

ii There is some ambiguity in usage of terminology. We use "social media" to refer to the collective sphere of socially oriented digital communication and "social networking service" to refer to a specific platform such as Twitter, Facebook, and WhatsApp. We use "social network" interchangeably as either an abbreviation for "social networking service" or in the social-sciences sense of a theoretical abstraction. The distinction should be clear from context.

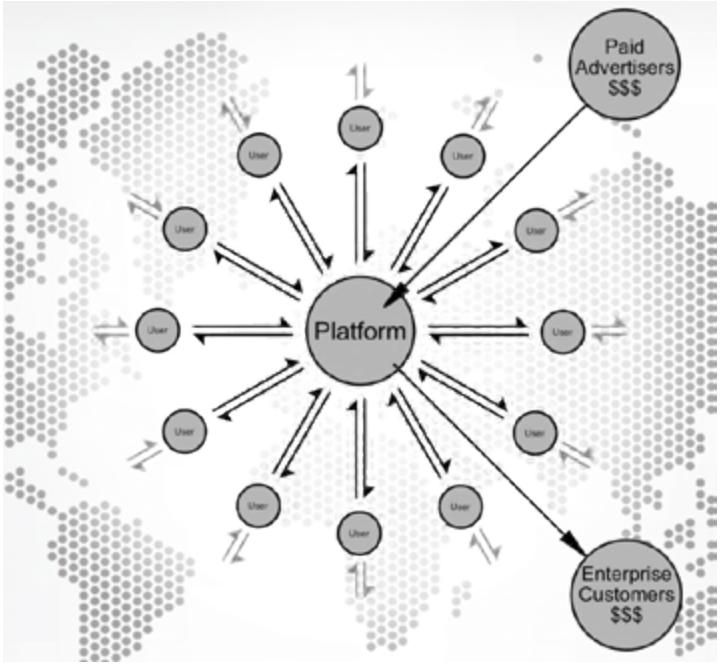


Figure 1. Schematic representation of a generic social networking service embedded in a larger context.

Every social network is also embedded in a larger society, including political, economic, and legal systems and a broader information ecosystem that includes traditional news and other media. This social context creates an additional category of "societal metadata," which also constitutes a particular social networking service:

- The cultural connotations of the particular platform, e.g. Twitter is associated with news while Instagram and SnapChat are associated with millennials.
- The laws that constrain the service, such as fiscal or content regulations.
- The business model of the service, where the money to run it comes from. This is usually advertising for the services we are most interested in, but there are other possibilities as well.
- The various characteristics of the user population. For example, European users are highly concerned about privacy (consider General Data Protection Regulation); in some developing nations, labor for manual content promotion is affordable and readily available ("click farms").

The embedding of a social networking service in a societal context also allows us to define "inputs" and "outputs." The "inputs" are the pathways by which information enters the social networking service. Inputs can be organic, when users observe something in the world around them and post it onto the network; or, information

can be injected directly into the network, primarily in the form of paid advertising or "promoted" content. The "outputs" are the pathways by which the information in the social network (the users and the servers collectively) affect the world outside. Similar to inputs, outputs can be organic, in the form of users' collective behaviors, resulting from what they have seen on the social network; or, information can flow out of the network in bulk, for example, when it is sold to advertisers or other enterprise customers, for purposes of marketing or research.

In Figure 2, the heavy double arrows represent the dense data flow within the social network itself, representing a constant feedback loop of users reading content out of and entering content into the network via mobile apps and desktop websites. Within this cycle, there are two kinds of "filter funnels." While each user makes individual choices about what to post, the collective pattern of information selection from the user population into the platform is represented as a funnel of "social and cognitive filtering." On the other side, a large volume of information is contained in the platform's servers, where algorithms known as "recommendation engines" decide, on an individual basis, what to present to each user's feed. The collective pattern of information selection from the servers to the user population is also represented as a funnel in our diagram. This funnel is often referred to as "the algorithm." The inputs and outputs mentioned above are represented in the four corners of this figure. Finally, a social networking service's computer servers also gather private user data such as geolocation, demographics, browsing behavior, and advertising statistics.[iii]

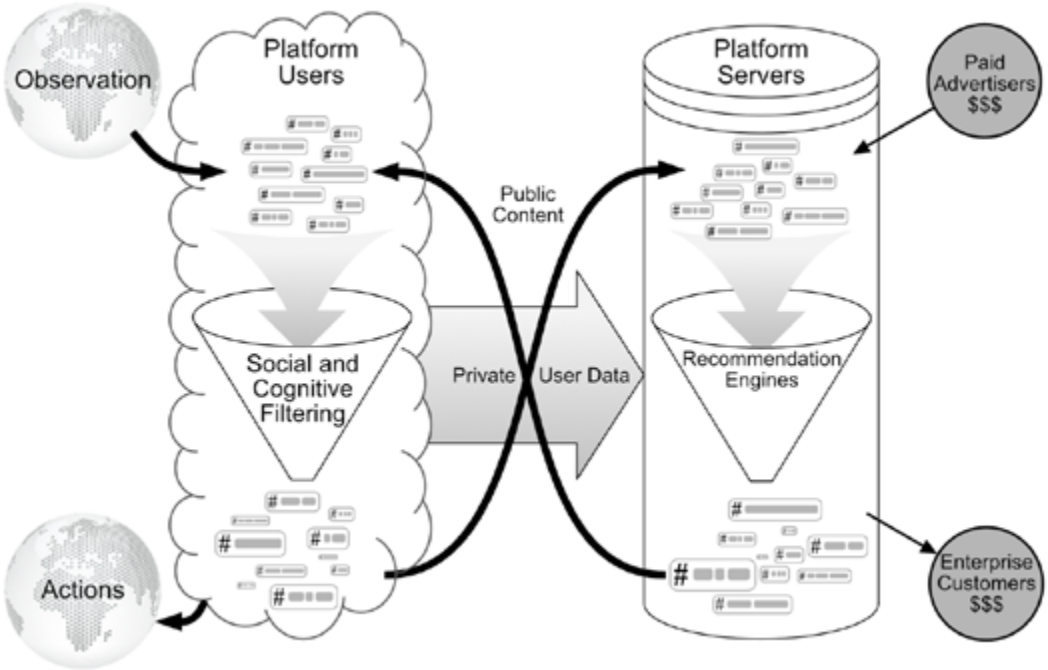


Figure 2. Information flow and filter funnels in a social networking service.

Although this model certainly oversimplifies the complexity of a real social networking service, it contains enough essential elements to allow us to discuss the unique features of weaponized information in the age of social media.

Under normal circumstances, we might assume the content contained in a social network would, for the most part, accurately reflect the human users' distribution of thoughts, beliefs, and experiences. For example, if a meme or hashtag is "trending," this ought to mean that people do, in fact, really like (or, in some cases, hate) it. It resonated naturally with a large number of users, and they "liked," shared, or took other actions to promote it. By design, social networks also allow business or political entities to use paid advertising as a traceable and accountable mechanism of influence. Content boosted through paid advertising can be vetted, and, in cases where abuse is discovered, the responsible parties can be identified immediately. While this equilibrium and transparency is maintained, the platform arguably serves the interests of a free and democratic society.[iv] The democratization of mass communication was an explicit goal of those who created new communication technologies such as the internet, and as long as this equilibrium appeared to hold, the internet and especially social media were celebrated as a humanitarian leap.[19]

Sociotechnical Systems and "Misinfosec"

> *"The lethal combination is when you exploit both people and technology."*
>
> ***—Kevin Mitnick, 2002***[20]

A social networking service as we have described it is an example of a sociotechnical system (STS).[21] In order to design, manage, or understand a sociotechnical system, it is necessary to combine social, cognitive, emotional, and technological perspectives. The Interaction Design Foundation writes, "Exploring a design problem by rising to an STS mindset can reveal further dimensions of a design's use potential and inspire development."[22] This holds equally true for a system's *misuse* potential and inspiring the development of exploits. In the security world, this STS mindset has always been implicit in the concept of "social engineering." A social engineering attack is "the acquisition of information about computer systems by nontechnical means,"[23] specifically by using deception to manipulate human users and/or administrators.

Many people consider social engineering attacks to be the easiest and most common kind of cyberattacks,[24] and they represent an enormous and growing problem.

iv Recently, many people have raised serious questions about this "attention economy." When a platform's profits depend on maximizing engagement, it creates an incentive to tune the algorithms to show more sensational, shocking, divisive, and even sometimes violent content. There are concerns that social networks' relentless drive for engagement may trump good corporate citizenship and even national security. There are also privacy concerns about how social networks use the user data they collect. (Breaux, T. D., *An Introduction to Privacy for Technology Professionals,* International Association of Privacy Professionals, 2020). These are important issues and we certainly do not mean to dismiss them lightly. However, for the purposes of this chapter, we are only interested in exploring how hostile adversaries can misuse social networks.

In a social engineering attack, the *vulnerability* of the STS is some collection of cognitive biases or other human psychological weaknesses; the *exploit* is constructed from known techniques of psychological manipulation and deception; the *attack vector* is an email message, phone call, or other message targeted at an individual; and the *outcome* of a successful attack is generally that the attacker acquires a password or some other form of access to a computer system. But social engineering is only a tiny bit of the full scope of potentially exploitable vulnerabilities in sociotechnical systems. An emerging field of research and practice on sociotechnical security[25] or "misinfosec"[26] considers the massive scale of effects that are possible from attacks on sociotechnical systems when there are hundreds of millions of users and information can be spread to most of them within seconds. For the kind of attack considered by misinfosec, the *vulnerabilities* are the interacting collective of the human cognitive biases and the biases in the recommendation engines' algorithms[27]; the *exploits* might include anything from traditional online ad campaigns to overseas troll farms, click farms, and sock puppets,[v] and even control of traditional media such as television or print; the *attack vectors* are memes, narratives, hashtags, and other forms of information trends that target entire populations[28]; and the *outcome* of a successful attack would consist of changes in behaviors and/or beliefs of those entire populations and the real-world effects of those changes, such as political or economic movements, or even mass murder.[29]

TABLE 1: SECURITY CONCEPTS MAPPED INTO "MISINFOSEC" DOMAIN

	"Pure" Cyber	Social Engineering	Misinfosec	
Risk exposure	Access to sensitive data, admin control of systems, denial of service, data loss, financial transfers		Political and economic effects, election results, market movements, protests, riots, genocide	
Attack surface	Computer networks	Individual humans	Populations of humans (Demographics)	Recommendation algorithms
Vulnerabilities	Code bugs, weak passwords or encryption, buffer overflows	Psychology, cognitive biases and fallacies, irrational emotional responses	Social psychology; social, economic, or racial injustice and unrest; mob instincts, social belonging, and group identity	Algorithmic bias, lack of ad vetting/auditing, susceptibility to SEO/SMO techniques
Exploits	Code/scripts that manipulate vulnerabilities	Social interactions that manipulate and deceive	Conspiracy narratives; sensationalism; clickbait; using nationalism, religion, race to provoke fear, anger, or violence	click farms, botnets, follow-backs, trend hijacking, paid promotion
Persistence	Hidden, dormant code	Established trust relationships	Cult-like groups; penetration of pseudoscience or "alternative facts" into mainstream; demographics devoted to compromised news sources or public figures	Large follower counts, high search rankings

v Manually operated accounts with fake identities.

Marketing or Misinfosec: A Note on Dual-Use

> *"Strategic latency refers to the inherent potential for technologies to bring about significant shifts in the military or economic balance of power."*
>
> ***—Strategic Latency and World Power, 2014[30]***

Persuasion has always been big business, and the rise of the internet and social media has led to unprecedented business and economic development.[31] At least two of the most profitable businesses in the world—Facebook and Google—are, arguably, primarily digital marketing behemoths.[32] All of the techniques we discuss in this chapter were developed for civilian purposes as a result of the tremendous business incentives, and all of them continue to be used primarly for legitimate business, or, in many cases, simple financially motivated fraud and scams. But any technology can be dual use; the key distinction is not the nature of the technology itself, but whether the intent is hostile and the result is a "shift in power."[33] Although it is possible, to a limited extent, to distinguish between ethical "white hat" and illegitimate "black hat" digital marketing activities,[34] we focus only on how these technologies have the potential to "bring about significant shifts in the military or economic balance of power" without concerning ourselves too much about carving out exceptions for "legitimate" marketing or political campaigning. With that in mind, we will first give an overview of techniques that can be considered closely analogous to "exploits" in the domains of human cognitive vulnerability, and recommendation algorithm vulnerability, and then proceed to consider the larger-scale structure of digitally mediated mass persuasion and how new developments have made it far more powerful.

Cognitive Vulnerabilities and Exploits

> *"There's a sucker born every minute."*
>
> ***—Never actually spoken by P.T. Barnum***

Salesmen, politicians, performers, and religious leaders have been refining psychological techniques of persuasion since antiquity.[35] These techniques take advantage of "cognitive biases" and "cognitive fallacies," predictable cognitive patterns that bypass rational thought and drive behavior.[36] A complete study of psychological techniques of persuasion would be an enormous undertaking far beyond our scope, but we will mention a few particularly relevant ones to this chapter:

- The "foot-in-the-door" technique or "yes ladder": starting with an easy point of persuasion and building it up one small step at a time.[37]
- The "door-in-the-face" technique, also known as "framing effects": starting with an outrageous and unacceptable point so that subsequent offers or gambits seem reasonable in comparison.[38]

- A picture is worth a thousand words: using visual media such as memes, GIFs, or fake videos to make content more compelling.[39]
- Kernel of truth: hiding items of disinformation among other items of verifiable information.[40]
- Halo effect or celebrity endorsement: making people believe a message by having a celebrity or respected figure deliver it.[41]
- In-group bias and social conformity: developing real or fake networks of accounts that make target audiences think this is what "people like me" believe.[42]
- Guilt by association and scapegoats: Discrediting individuals or accusations by deflecting onto members of a despised out-group.[43]
- Simple repetition: flooding a target audience with a message so it comes to believe the message without any conscious decision.[44]
- Push polls: using fake polls to make a certain position seem desirable because it is "popular."[45]
- Competing narratives and "false equivalence": promote real or manufactured debate between alternative messages, one or more of which is the "payload."[46]
- "Whataboutism," straw man, and other forms of misdirection: the adversary distracts from unfavorable facts by offering an emotional but unrelated reply.[47]
- Fear and hate mongering: uniting the masses behind a message by associating the message with strong negative emotions about a despised out-group; for example, depicting Jews or immigrants as murderers and rapists.[48]
- 419 scams or conspiracy narratives: using unconvincing materials to filter for particularly gullible individuals.[49]

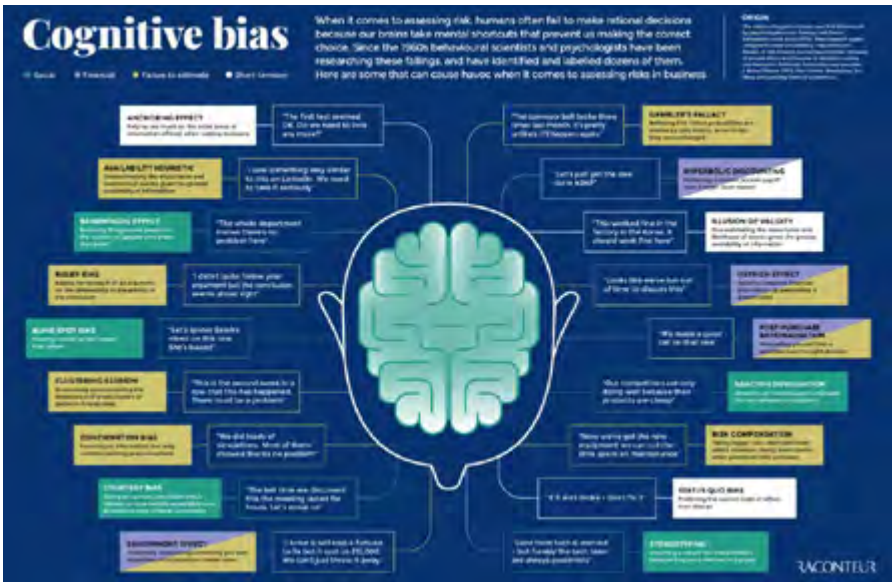


Figure 3: Helpful infographic on Cognitive Bias (courtesy of Raconteur).

Algorithm Exploits

> *"By far, the greatest danger of artificial intelligence is that people conclude too early that they understand it."*
>
> ***—Eliezer Yudkowsky[50]***

Recommendation algorithms (and other machine-learning/artificial-intelligence systems) are now so enormously complex that no one fully understands how they work or what they will do in any particular situation.[51] This uncertainty has created an ongoing "arms race" between the companies who build the algorithms and marketers who are constantly developing new techniques to manipulate them.[52] These techniques are generally referred to as search engine optimization (SEO) and social media optimization (SMO)[53] and consist of passive techniques such as fine-tuning a website's metadata or active techniques such as bots and spam, and everything in between. Some common and highly effective techniques to influence an algorithms' content ranking include:

- Promotion by fake accounts: these include "bots," "sock puppets," and "cyborgs" (partial automation).
- Pay-per-click (PPC) and "phone farms": real humans with real accounts are paid to "like" content.
- Social media spam: posting massive volumes of content directed at unwitting users.
- Keyword/hashtag hijacking or stuffing: adding many common keywords, or one currently trending keyword, to unrelated content.
- Impersonation: using accounts claiming to be someone famous and respected to promote content.
- Blog comment spam: using unmoderated, unsupervised comment forums on blogs, YouTube videos, newspaper articles, Google Maps, Yelp reviews, and other platmforms to promote content.

Insights from Digital Marketing

It is also helpful to understand some general terms and concepts from digital (and traditional) marketing. Any influence campaign, whether carried out by legitimate advertisers or a hostile entity, involves certain steps:

- Message selection and optimization: The message is based on the goals of the campaign, but there are many decisions to be made about the exact content and form, which will depend on the other choices in the campaign. It is particularly important to optimize a message for a target audience.

- Audience selection and targeting: Likewise, all details of the audience will not be dictated by the goals; the exact audience may be refined based on the medium or other choices.
- Medium selection: The planners must choose which form of communication to use: Websites or social media? Or even TV or print? The choices of media fall into two categories, passive and active, and there are specific techniques for each category.[54]
  - Passive or broadcast media would be websites that might or might not appear in searches, or social media posts that might or might not be displayed in a user's feed. This would also include more traditional broadcast or display media such as TV, radio, and billboards.
  - Active media or "direct marketing" would be anything that is intentionally delivered directly to a specific user. This could be search engine sidebar ads, paid targeted social media ads, or even email, phone, or postal mail.
    - Targeting websites for direct display to users in sidebar ads is called "search engine marketing" (SEM)
    - Targeting social media content for direct display as promoted ads is called "social media marketing" (SMM)

A campaign will be most effective if choices are made based on evidence. The primary tool for evidence-based optimization is "AB testing," where two or more versions of a campaign are tested simultaneously and the response metrics compared. With traditional media, this testing process can be slow and difficult; one of the most transformative features of digital media is that the speed of computation and data transmission is now so great that AB testing can be done in a rapid iterative cycle, where dozens or hundreds of different approaches can be tested, measured, altered, and retested, sometimes even without human intervention.

A campaign will also be most effective with detailed and precise audience targeting. Another transformative feature of digital media is the enormous volume and detail of user data, especially on social networks. This allows extremely detailed and precise targeting of specific messages to narrow demographic slices or even individuals, which is called "microtargeting" (and has received a great deal of scrutiny, although generally not within a security context).[55]

Even without resorting to "black hat" techniques, the power of rapid iterative AB testing combined with microtargeting is immense. Advertising "conversion rates"—the percentage of users who take the desired action, per baseline statistic such as email count, page views, or number of times an ad is displayed—have traditionally been low, from a fraction of a percent to a few percent in the best circumstances.[56] But a campaign that uses the best available techniques in clever ways can achieve conversion rates greater than 50 percent.[57] The structure and modeling of user data is key to the most powerful campaigns, so we will consider that next.

Demographic Modeling and "Big Data"

> *"Andrew Hacker has suggested that the use of electromagnetic computers to simulate the political behavior of the real world has led to essentially trivial findings.... [But] its successful employment is a legitimate subject of concern in normative terms, as well as proof that Hacker was in error to dismiss it lightly. The history of science is full of evidence that solutions to old problems often create new problems"*
>
> ***—Joseph Bernd, 1966***[58]

The power to influence is closely connected with the power to measure. Population-scale models of consumer and political preferences have existed as mathematical abstractions in the field of economics for generations. New developments in graph theory and computational social science can model the spread of information through social networks. Additionally, models from voting theory and market economics show how population preferences lead to political and financial "outputs." All these models combined can now be fully fleshed out with the enormous volume and depth of personal user data aggregated by social network platforms. Combining these models with the armamentarium of new and old tactics and techniques for algorithmic and social/cognitive manipulation allows an unprecedented degree of power to test, refine, and implement influence campaigns from the earliest stages all the way to the desired outcomes of political changes. The result of the convergence of these developments is the emergence of influence campaigns with vastly greater complexity, scale, precision, and effectiveness—and dramatically lower cost—than ever before.

This power results from the combination of huge collections of user data and the computing power to apply enormously sophisticated analyses and production algorithms, techniques variously referred to as "data science," "machine learning," or "artificial intelligence." A collection of user or population data is both "wide"—that is, it describes a large number of individuals—and "deep"—that is, it contains many distinct pieces of information about each individual. A deep user database contains a shockingly diverse amount of information about individuals, such as demographics, purchasing habits, travel and movement habits, financial information, political preferences and affiliations, social connections, and even subtle metrics derived from application logs, such as how fast they read, how long their attention tends to stay on one thing, sleep-wake cycles, and even some kinds of health data. Such a database might contain ten thousand or a hundred thousand variables. Much of the art of working effectively with such data sets revolves around distilling this massive collection of numbers (which always contains many missing variables, errors, and redundancies) into something more meaningful on a human scale that can be used for tasks such as prediction and targeting.

The mathematics of data science is beyond the scope of this chapter, but it is important to evoke a general sense of how data scientists think. A large data set

can be thought of as having ten thousand dimensions (or whatever the number of variables). In order to make practical use of the data, the number of dimensions must be reduced to something manageable while still capturing the most important aspects of the overall data set. When discussing machine learning and data science, one customarily draws two-dimensional diagrams as generic representations of the data dimensions, without worrying about the details. For example, a representation of political voting data can be drawn as a cloud of points, where each point is an individual, the colors represent the actual vote or party affiliation, and the two-dimensional space of the diagram is a simplified representation of however many variables in the reduced data set turn out to be relevant.

These diagrams can be used to represent schematically the movements of population-aggregate beliefs and the outputs of market or political movements. In the future, this could be used to generate virtual tactical battlefield displays for planning, monitoring, or analyzing influence operations. We will use such diagrams to describe some theoretical advanced influence operations. But first, we will describe a useful heuristic for thinking about population beliefs and influence operations.

The Overton Window and Mass Influence

Joseph P. Overton described "The Overton Window" as the range of public political discourse tolerated within a given society's media ecosystem.[59] His original presentation of the concept considered any policy issue to be represented by a single dimension. The Overton Window is the "realm of the politically possible": the range of positions that, say, a politician could express and hope for any possibility of success; in the original model this range of positions is represented by a single line segment along the single issue dimension. The idea of a unidimensional political spectrum is useful for simple rhetoric, but we will show here how it can be adapted to much more useful "Overton Blob" on the multidimensional population preference diagram.

The original presentation of the Overton Window merely used it as a device to describe how policies shift incrementally with changing societal norms. The Overton Window drifts slowly over time; lobbying and advocacy can steer that drift to some extent, but Overton's original point was that ideas outside the "realm of the possible" were simply unattainable.[60] Highly motivated lobbyists can achieve significant policy changes, but this can be expensive and may require extraordinary brilliance. For example, between 1980 and 2001, Enron achieved many of its policy goals around deregulation of energy futures trading using traditional methods of lobbying, campaign contributions, and advertising, including the innovative, award-winning "Metal Man" TV ad campaign.[61] Although the desired change was well within the Overton Window of the time, Enron spent countless millions over decades to achieve it.[62] But the enhanced power of the contemporary techniques we discuss in this chapter suggest a bolder approach to the Overton Window.[63]

Consider the challenge facing an entity who wishes to advocate a position far outside currently acceptable discourse. The straightforward, incremental approach is

essentially the "foot in the door": advocate an incremental change and gradually work toward the desired shift in population preferences. But consider instead a "door-in-the-face" approach. The entity would begin by establishing an extreme, even ludicrous, narrative. Once the extreme narrative has been injected into the public discourse, everything less extreme immediately becomes fair game; thus, the Overton Window has been expanded more rapidly than possible with an incremental approach.

To make this process work, two things are required: a detailed understanding of the preference landscape, to facilitate targeting of the fringe cluster in a way that supports the desired policy goals; and a reliable method for injecting extreme content into the public discourse, items well outside what would have been acceptable previously. Big data and demographic modeling have taken care of the first requirement. The second requirement is easier than ever before, thanks to the advanced influence techniques we have discussed. Worse, social media and the internet thrive on extreme spectacle; most people receive their news from Facebook, which provides ample opportunity for radical shifts in opinion through algorithmic and cognitive manipulation.

To illustrate how this might work, we present a tongue-in-cheek hypothetical scenario that builds on the real-world story of the "cinnamon challenge."

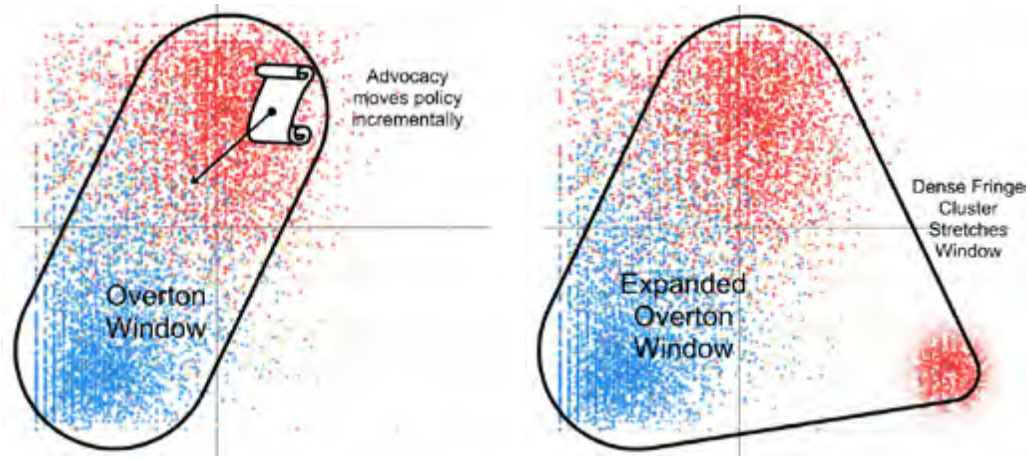


Figure 4: Moving the Overton Window.

The cinnamon challenge first appeared in 2001, but suddenly went viral in 2012, with 70,000 mentions a day on Twitter at its peak, and more than 1.5 million videos online—the most popular of which had 56 million views as of 2020.[64] There's no reason to believe there was any hidden agenda other then the usual hype around sensational cultural phenomena, but what would it look like if it had been a part of an influence campaign of the type we just described? Consider an oregano manufacturer who wants to increase sales dramatically. An extreme approach would be an ad campaign promoting the consumption of heaping spoonfuls of oregano, but it would be challenging to directly convince

people of such a ridiculous idea. However, eating a spoonful of *cinnamon* is not only ridiculous but also agonizingly painful and even potentially fatal, which makes it ideal fodder for a media ecosystem driven by sensation. Our imaginary oregano supplier could easily manufacture a cinnamon challenge trend, starting with staged videos, then promoting them using familiar techniques such as botnets and perhaps a celebrity tie-in.

Persistence in Digital Influence: Conspiracies and Cults

Briefly popular, the cinnamon challenge faded away almost as fast as it appeared. An adversary who desires large-scale, ongoing influence would want to establish a persistent campaign. The most obvious ways to do this would be to buy news stations, film studios, and the loyalties of talk show hosts, and, in fact, both Russia and China currently have extensive stakes in various American media.[65] More subtle approaches to persistence also exist. In the cinnamon challenge story, the Overton Window expands not because *everyone* participates but because enough individuals engaged in the same activity to bring it to the level of public discourse. This phenomenon can be represented diagrammatically as a small, dense cluster well outside the main population. In reality, the cinnamon challenge population was only bored teenagers who quickly moved on to the next fad. But for purposes of persistence, one might imagine a "cult of cinnamon" that could cause the cluster to remain cohesive. In order to accomplish this, an adversary would have to inspire and unite a significant number of individuals by constructing narratives of identity and otherness.

The 419 scam/conspiracy narrative technique is particularly well suited to this purpose. Large-scale promotion of implausible conspiracy theories is a potentially powerful way to allow particularly credulous individuals to self-select into an ideological identity group, united by an "us-against-the-world" mentality and other cultlike patterns. The group identity and demographics would have to be constructed in such a way that the adversary is able to reactivate the cluster for ongoing influence activities by feeding them information directly; for example, an aspect of the group identity might be loyalty to media sources under the adversary's influence. An adversary who knew how to "hack ten million useful idiots"[66] and establish such a persistent, controllable population cluster—a "Weaponized Useful Idiot Demographic"[67]—for purposes of political and social influence would be powerful indeed.

Detecting and Defending against Disinformation Campaigns

There are many published "solutions" to disinformation attacks and social media protection.[68] While they are all useful, it is foolish to think any one of them will solve the disinformation problem single-handedly. Proposed solutions often address small pieces of an attack, are intractable, or do not scale. Disinformation campaigns are whole-system attacks, and to solve them, one must examine whole-system solutions. We need a "thousand bullet," not a "silver bullet," solution.

Models and Frameworks

We provide an overview of models and frameworks that we have developed (or repurposed) to allow defenders to better understand the nature of an incident, and to map out the space of potential solutions. We can look at the solution space in several different ways. One is as a human space, in which we are engaged in narrative warfare. Human communication is generally at the level of stories, or narration: we tell each other stories about the world, as sentences, image sequences, or memes. Each person bases their sense of self ("identity"), their belonging to different groups ("in-groups"), and exclusion of others ("out-groups") on narratives. Narratives are typically personal, emotionally charged, deeply entrenched, and difficult to shift directly. In this space, it becomes important to track and disrupt narratives and their components (e.g., memes, stories, sentiments) not by countering them directly with "facts" but with "information aikido." It is easier to redirect an angry mob to a different house than it is to disband the mob. Narrative warfare is a growing field,[69] and its techniques are a useful component in countering disinformation. Using natural language-processing techniques, like topic modeling and gisting, to track narratives from disinformation actors and highlighting narratives to potential target audiences have also proved useful.

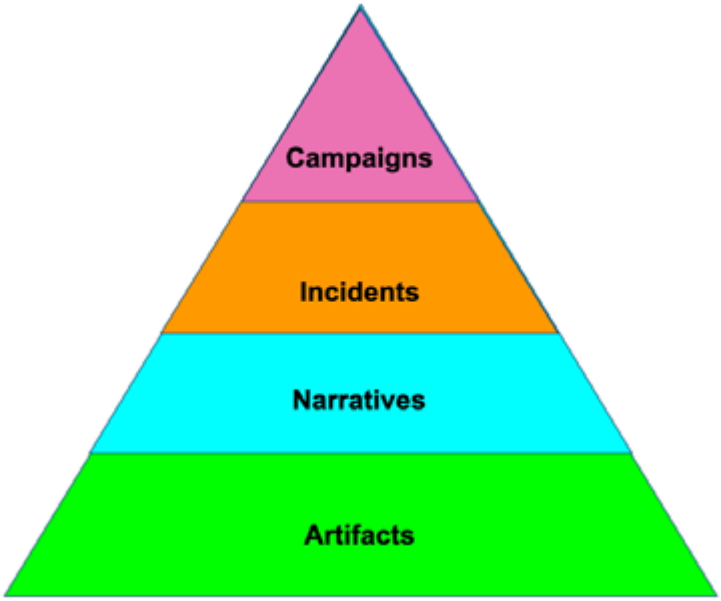


Figure 5: Misinformation Pyramid

The misinformation pyramid is another view of this space. In it, we have the different views of creators of misinformation ("attackers") and the people trying to counter them ("defenders").[vi] Attackers create incidents (e.g., MacronGate), which

vi The third group involved, the targets of the misinformation ("populations"), are not part of this diagram.

often form part of long-term campaigns (e.g., destabilize French politics). Narratives are the stories on which we base our beliefs. To transmit these stories, we need artifacts: for example, the user accounts, tweets, images, and connections between them, visible in each attack. While the attacker sees the whole of the pyramid from the top down, the defender usually sees it from the bottom up, working back from artifacts to understand incidents and campaigns (unless they are lucky enough to have good insider information or intelligence). The pyramid layers are about not just information but also action. Most contemporary misinformation work is at the artifact or narrative level; analysis of operations tends to be at incident or campaign levels.

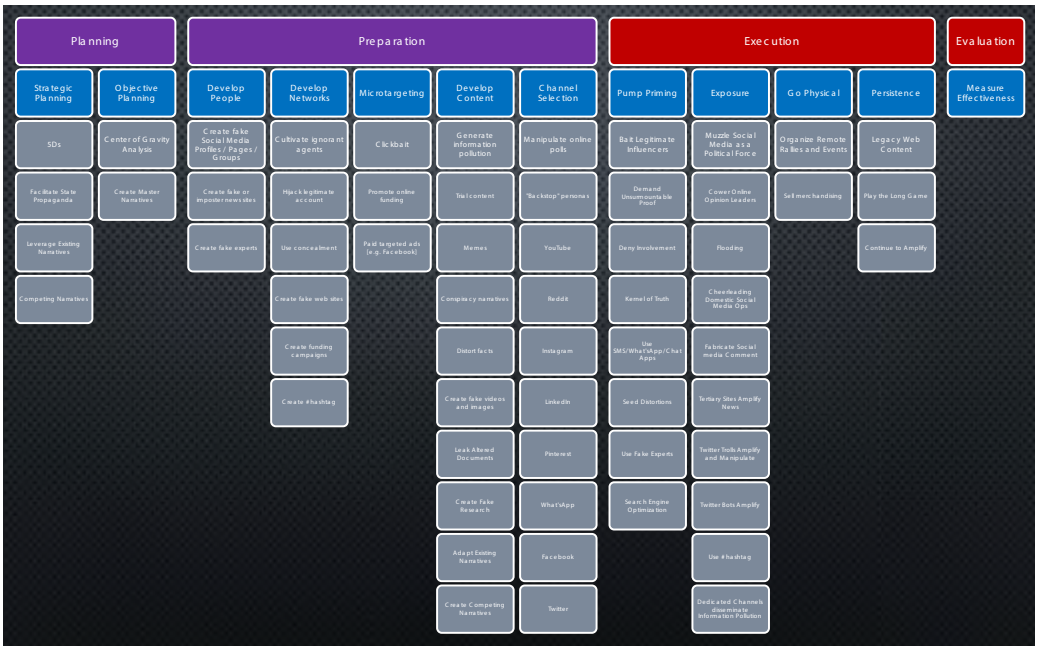


Figure 6: Adversarial Misinformation and Influence Tactics and Techniques (AMITT) Framework

A useful view of a disinformation incident is as a collection of the objects seen within it, including the techniques, tactics, and procedures (TTPs) that the attacker used. We created the Adversarial Misinformation and Influence Tactics and Techniques (AMITT) framework model to describe common disinformation TTPs and the misinformation kill chain of which they are a part. We distilled AMITT from examining the US Department of Defense's *Joint Planning* process (JP 5-0)[70] and Information Operations publication JP 3-13[71]; MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)[72]; and other models of mass influence, including advertising models. The model is designed to be a logical extension of ATT&CK and was populated by down-selecting from 68 real-world incidents to the 22 with the most varied TTPs.

The top line of AMITT lists the stages necessary for conducting an attack: planning, preparation, execution, and evaluation. Within planning, strategic planning forms a commander's intent, specifically, the overall objective of the misinformation campaign. The second line lists the steps of the misinformation kill chain. Below each link of the kill chain are TTPs that support completion of that link. Not shown are the tasks performed at each of these steps, and counters to each of the steps and techniques.

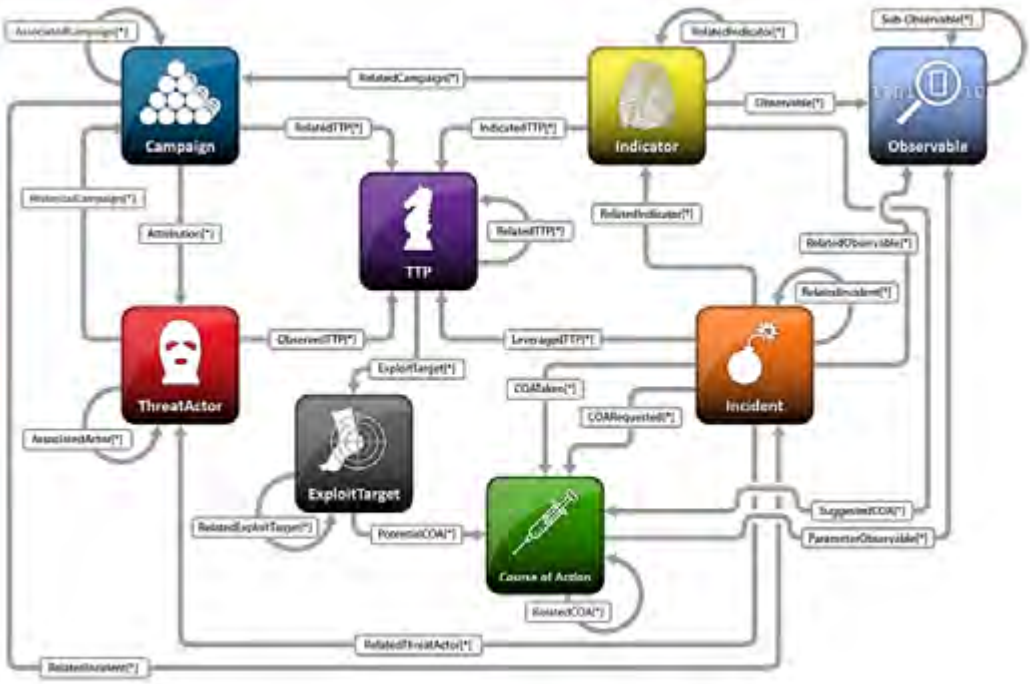


Figure 7: STIX Object connections.[73]

Disinformation incidents are rarely isolated events. The AMITT TTPs are part of richer description languages drawn from information security, including STIX (Structured Threat Information eXpression), that allow analysts to share and compare information about shared threat actors, narratives, TTPs, artifacts, potential countermeasures, and other objects in each incident and campaign.

Countermeasures

Now that we've presented several models to facilitate thinking about attack planning and the defensive kill chain, we will address countermeasures and tools. Adversary tactics move quickly in this arena, so it is impossible to present a comprehensive and authoritative list of tools and countertactics, but the basic spaces and categories are more consistent. Any of the offensive techniques we have already discussed can be adapted for defensive or counter-offensive use. In addition, the current counter landscape includes:

- **Detecting artificial amplification.** Many disinformation campaigns rely on signal amplification, either through "useful idiots" or by raising message visibility using nonhuman traffic (bots and botnets). Databases of known bad online and state-sponsored actors, with data from pages and social media feeds from these actors, have proven useful places to look for emerging narratives and links to new actors and artifacts. Increased efforts in disinformation detection, mitigating advertising click fraud, and other platform integrity concerns has driven adversaries to adapt and focus more on protecting their assets, which makes tracking bots and botnets more difficult. But there is still value in simple bot/botnet detection techniques including analysis of similarities across accounts linked by topic, hashtags, retweets, and references, and time-series analysis to check for sleep-wake patterns and activity correlations, especially with adversaries new to this space.
- **Fact verification.** Fact verification can be done manually or in an automated fashion. Manual verification does not scale to the internet. Automated verification via natural language programming (NLP) scales better but is insufficient to deal with the vast amount of information on the internet. Additionally, automated fact verification cannot handle satire or editorials.
- **Social-graph analysis.** There have been attempts to detect misinformation via social-graph analysis, but a suitable model has not yet been suggested. Most social-graph analysis is geared to examining human networks, as opposed to social networks. In human networks, people make friends and connections at a much higher rate than they lose them. This model is well explained by scale-free networks. In misinformation, however, the governing characteristic is link destruction, which often results in bifurcating a population. No current social model explains this phenomenon.

These counters are insufficient to work on an internet scale, and these defenses will show results only after misinformation is consumed. Once consumed, counternarratives must overcome their own cognitive friction, bias, and cognitive dissonance. Finally, these counters address only a small portion of the kill-chain and have historically not been synchronized. The AMITT work on counters covers the whole misinformation kill chain.

Conclusion

Misinformation is as old as warfare, but the internet and social media platforms have allowed for revolutionary changes in its delivery. While it was relatively simple to attribute the source of mass influence campaigns in the past, the democratization of reaching mass audiences has added to the challenge of attribution. The ability of a nation-state to govern its own internal affairs free from external influence is a condition of peace under the Westphalian model. Adversaries such as Russia and China have leveraged the complexity of the internet and the social media battlefield

to fray the edges of international norms, as laid out by the traditional Wesphalian definition of a nation-state, but their recent actions to affect internal affairs of other countries have not resulted in war. This fact yields two conclusions: 1) we are in a perpetual state of competition short of armed conflict (war); and 2) we are now entrenched in a post-Westphalian world. These conclusions necessitate states either reestablish old international norms or define new ones.

Appendix

Department of Defense Duffer Cloud: A Disinformation Vignette

When the DOD awarded Duffer Corporation the contract for unified general-purpose cloud services, many hailed the move as a long-overdue modernization that would improve efficiency, interoperability, security, and economies of scale. Disappointed competitors inevitably grumbled, but Senator Forethought, head of the Armed Services Committee (ASC), General Backsight, head of US Central Command, and Senator Swinton, the senior senator from Duffer's home state, all supported the decision. The trio held regular press conferences to express the importance of the contract to the US military and to express their total confidence in Duffer. On the other hand, Senator Boer preferred to tweet about "this unholy alliance of the Deep State and globalist corporate elites," but she had always been somewhat fantastical and conspiracy minded, and few officials took her seriously. In any case, some officials were already questioning her unusual friendliness with the foreign nation Incidentambia. Conversely, analysts saw clear signs of concern among US adversaries, including Incidentambia. Many of the adversaries were known to take cyberwarfare, digital communication, and other emerging leveling technologies seriously and were sensitive to trends in US military modernization, all of which were also widely considered a sign that we were on the right track.

One day, an unusual video is posted in several fringe social platforms and goes viral when Senator Boer mentions it favorably on Twitter. Blurry and taken from an awkward angle, but clearly audible, the video appears to show the Duffer Corp. CEO and the director of the NSA joking about Duffer's cloud services participating in mass surveillance of US and foreign customers. Within 24 hours, Duffer holds an emergency press conference to announce the video is fake and backs up their claim with clear and incontrovertible forensic analysis. Most pundits acknowledge the proof and praise Duffer's rapid response and transparency, but the additional news coverage only serves to spread the story to a wider audience. In any case, most people ignore the careful attempt at rational persuasion and merely double down on their beliefs.

Almost as soon as the press conference ends, Duffer's public-relations team becomes aware that another video—this one in French—has appeared overseas, showing the head of Duffer's European headquarters having a similar conversation with European Union intelligence officials. Officials quickly debunk the video, but another one appears on a similar theme. Then, stoking the confusion, yet another

video appears to show a meeting of Duffer executives with a notorious strongman dictator in an oppressive state. Duffer debunks each video almost as soon as it appears, but the tedious technical details fail to reach a wide audience, while botnets and clickbait sites continue to boost the wild tales. Although the fakery seems obvious and the narrative self-contradictory, the pundits' eagerness to promote their own explanation merely keep the "Deep State Duffer" story in the news.

Eventually, the mainstream news cycle largely moves on. Senator Boer continues to preach deep-state conspiracy stories to her own Twitter choir, and variations on the theme bubble and stir on the fringes. Public-relations teams have done what damage control they could, and social media sentiment analysis suggests the Duffer Cloud is being rehabilitated. Within a year, DOD and Duffer begin the long and slow upgrade process. Service members and staffers complain about inconvenience and technical difficulties. Much of the grumbling takes place on Facebook and various other online forums, but complaining is an ancient and harmless military tradition, and this raises no red flags.

Without warning, a protest convenes in front of the US embassy in the friendly, but somewhat unruly, nation of Waschout. The protestors shout demands and slogans based on a dubious but viscerally compelling mutation of the Deep State Duffer story in which a terrifying international cabal engages in exploitation and human trafficking at the expense of the locals. Embassy security disperses the protest, but the protesters reconvene in front of the local Duffer Corp. office. They remain there, as the local police appear hesitant to take aggressive action.

Unknown to anyone in the United States, human-staffed "phone farms"—funded via cryptocurrency from untraceable sources—have been building up WhatsApp groups dedicated to conspiracy theories and diligently testing variations on the Deep State Duffer theme. The protests receive little coverage in the United States at first. Senator Swinton and some Duffer executives hold a small town hall near headquarters to reassure the employees their coworkers in Waschout are safe and the US is unwavering in support of the employees. As the town hall is ending, a confrontation breaks out: a man shouts something incoherent about human sex trafficking. Unwisely, a Duffer executive moves closer to see what the ruckus is all about; when the man catches sight of him, he pulls out a gun and declares his moral duty to make a citizen's arrest for these crimes. Panic breaks out; people scream and run away as Senator Swinton's security moves to confront the interloper. He is clearly a few cards short of a "well-regulated" deck; his poor trigger discipline leads to an accidental discharge, and security has no choice but to take him down. No one else is hurt, and mainstream news reports are sober and factual.

But over the next few days, anonymous posters on fringe forums make a connection between the Waschout protests and some newer, more exciting rumors, and soon Deep State Duffer 2.0 is trending, darker and more compelling than before. As the story goes, Duffer and Swinton are part of a ring of human trafficking and

international exploitation backed by the NSA and a sinister globalist cabal; the man at the town hall was a hero for uncovering the truth, and the cabal killed him for it.

Social networks are having a field day, and the top search results for Duffer and Swinton are clickbait sites full of ludicrous, extravagant, and salacious stories, boosted by social media bots. Legitimate mainstream news networks initially resist giving in to the temptation of these sensational stories. But then, sensing opportunity in the midst of chaos, Duffer's main competitor Drift announces a lawsuit claiming the bidding process for the DOD contract was rigged. Coincidentally, Senator Boer has been receiving extensive campaign contributions from a complex network of entities with ties to Drift, and she shows strong support for the lawsuit by questioning the procurement process—as well as making frequent oblique references to the widespread ludicrous rumors. Mainstream reporters and pundits, aware that their audiences are largely unfamiliar with the new round of rumors, carefully attempt to explain the context without giving it weight. But once the Deep State Duffer train has made the jump from internet-fringe to mainstream media, there is no going back. Soon the airwaves are filled with talk shows hosting "experts" on "both sides" of the "controversy," and average citizens are discussing the most outlandish conspiracy theories about Duffer Corp. as if they have elements of truth.

Meanwhile, many reasonable people discuss the merits of the Drift lawsuit. In the midst of a debate about delays and inefficiencies, a shocking document appears on the internet. No one is quite sure where it came from, but the Complaint Catalog is an extensive list of candid complaints from service members, running the gamut from ordinary inefficiency to rude and unfriendly customer service, all the way up to inexcusable levels of incompetence and even hints of misappropriation and fraud. Investigation easily reveals that most of the complaints were accurately scraped from service members' public social media posts. Some of them were gathered, by unknown means, from ostensibly semiprivate forums like LinkedIn and NextDoor; these, too, are mostly traced to their original sources and verified. Some of them cannot be traced to a specific online source, but reporters track down a number of the individuals involved, who are mostly pleased with the attention and happy to confirm that, yes, they vaguely remember that maybe something like that happened at some point.

The repeated appearance in the news of further items leads almost everyone to accept the Complaint Catalog as authentic. Eventually, a few of the more dedicated investigative journalists and analysts point out that the 5 percent of unverified complaints happen to include a significantly higher proportion of severe allegations, but this is a subtle and boring warning that gets little traction. The narrative of a "mostly verified" Complaint Catalog that "contains allegations of fraud" takes root in the fertile ground prepared by the widespread coverage of Deep State Duffer stories. The gambit (for the truth is, the Complaint Catalog is an artifact of deception) is so successful that it becomes a point of pride for those who like to think of themselves as "skeptical intellectuals," who believe they can make a nuanced distinction between the Deep State Duffer conspiracy—which is obviously a bunch of nonsense that only

“those other people” believe—and the Complaint Catalog, which has gone through a transparent and accountable process of verification. Ironically, those who question the authenticity of the Complaint Catalog are now ridiculed as conspiracy nuts.

A handful of forward-thinking security specialists have figured out by now that this whole process is most likely an attack campaign planned and executed by Incidentambia; they warn future similar attacks are likely. But without terms of art, frameworks, and an established community, they find the problem difficult to explain to those outside their own small community. Starting a conversation by describing a handful of artifacts is easy enough, and figuring out stories that the artifacts bind together is not too hard, but climbing up a sort of “pyramid of pain” to explain how and why a collection of stories constitutes the elements of an intentional, goal-directed campaign is a challenge. Without any sense of process and progression, explaining how an adversary might be able to plan and execute such a thing, let alone how to fight or prevent it, is even harder. To make matters worse, conversations frequently break down into arguments about word definitions. For the most part, defense, business, and political leaders remain unaware of even the possibility of a through line tying together all the events around the Duffer Cloud contract and pointing back to Incidentambia.

Back at Duffer Corp. headquarters, the mood is grim. A few financial analysts have published speculative projections that, despite the large cash value of the DOD Cloud contract, the company may be a loser in the end if its stock goes down much more. Contractors find the DOD personnel they work with increasingly hostile and sensitive to the smallest problems. The initial strong support from Senators Forethought and Swinton has dwindled. Senator Swinton has been steering clear of the topic altogether since the town-hall scare. General Backsight no longer feels free to comment publicly now that the topic has been politicized. Forethought is still supportive, but more reserved in public, and increasingly burdened with sharp questions about the Complaint Catalog from officials on Capitol Hill. Competitors other than Drift have been emboldened to file their own legal challenges, each one celebrated and publicized by a jeering Boer, and Duffer’s legal team is increasingly concerned about the prospect of an actual court hearing. Unbeknownst to all of them, the agents of Incidentambia, lurking in the shadows, are preparing the next attack in this campaign, more brutal than anything so far.

It is just over a year before Senator Forethought is up for election when accusations of an affair with a staffer hit the news. The accusations are supported by the carefully choreographed release of a series of photos, videos, chat transcripts, and screenshots. Each time one artifact is identified as a forgery, another one appears just in time to draw attention from the debunking. Another former staffer, attractive and photogenic, appears on TV with damning, and fundamentally unfalsifiable, accusations. The narrative of impropriety spreads like wildfire, boosted by bots and other mechanisms, while the public remains mostly unaware that all the evidence was forged. In theory, it is no secret that the former staffer is now a political

operative for an opposing party, but Forethought's own party strategists warn that attacking the "victim" will most likely backfire. Senator Forethought is left floundering with no effective response to the setup.

Throughout the planning and execution of the propaganda and protests in Waschout, the Incidentambia team used methods from market research to evaluate and refine their procedure for inspiring anti-US protests abroad. Now, while the US news media are consumed with the manufactured Forethought scandal, they trigger protests at three other US embassies and one military base abroad, in selected cities where Duffer also has offices. Once again, embassy and base security effectively disperse the protestors, but a little bit more force is used this time, and, by the time the mobs reassemble at the Duffer offices, the protestors are angrier and the local police even less sympathetic to the rich US corporation taking advantage of their fellow countrymen.

Into this heated environment comes the biggest bombshell so far, as social media accounts appearing to belong to General Backsight send out a tirade of confessional and accusatory messages about the misdeeds of Duffer Corp. and the US military: mass surveillance at home and abroad and shocking stories of civilian casualties covered up in, as it happens, the very nations where the protestors are already near the boiling point. The impostor accounts are taken down within minutes, but networks of bots and click farms spread the content rapidly across multiple platforms. The protests turn into riots, and the Duffer offices are ransacked. US officials evacuate the embassies because the rioters are rumored to be heading back their way. Back in the United States, the message spreads fast, thanks to automated amplification by bots, as well as a few unfortunate retweets by Senator Boer. As soon as the news reaches his office, General Backsight makes his first public appearance in months to disavow the messages and plead for peace, but a short, out-of-context clip of his tearful message is shared extensively by fringe conspiracy communities and taken as proof positive that his message is coerced, fanning the flames higher.

Work on the Duffer Cloud has now entirely ceased. Weeks go by, with the stock tumbling. A video leaks, showing the CEO cursing a DOD representative; to everyone's surprise, this turns out to be an entirely authentic self-motivated leak by a real, uncompromised employee. In fact a large contingent of employees now oppose their own company's involvement with the US government. While they have not fallen for the outlandish conspiracy theories, as an expression of their rationalism and moderation, they have given equal weight to the arguments on "both sides" and concluded with a position somewhere in the middle. Unfortunately, since a hostile adversary entirely manufactured one of the sides, the "middle" is neither accurate nor moderate.

After the shock of the first incident, the lawyers and board advisers dictated two things: Duffer Corp. needs to be more secretive about their large contracts in the future; and the company ought to accept the lucrative offer of another huge contract from Incidentambia. Thanks to a well-established and wide-ranging infrastructure of information control, which includes firewalls and strict censorship

of all communications, as well as advanced techniques of psychological engineering of cultural and social norms, their responsibility for these events remained a secret, and they were able to continue to do business in the United States with one hand while exercising "sharp power" with the other. As a result of these multiple layers of secrecy, few are aware of the irony when Duffer Corp. yields to the pressure from its employees, lawyers, accountants, risk managers, and board of directors—as well as the total collapse of topcover from Backsight, Forethought, and Swinton—and pulls out of the cloud deal entirely.

Drift Corp. swoops in to fill the vacuum, and within a year, it has taken over the contract, this time with as little publicity as possible. However, over the following two years, a similar campaign plays out, and eventually they, too, drop the contract like a hot potato. By the time any significant progress is made on the actual system upgrade, so many years have passed that the word "cloud" itself sounds quaint and old-fashioned. Politicians rail for real military modernization, the kind that is only possible with the cutting-edge technologies flowing out of Incidentambia. The adversary has achieved a multiprong victory: US military operational capacity has been substantially impacted by years of information-technology disruption; the US economic base has suffered because the tech sector lost a substantial portion of its ability to compete with Incidentambia in the critical cloud services sector; and Incidentambia's cloud services sector developed deep relationships with multiple US companies—and benefited from quite a bit of technology transfer along the way.

> *After these lessons had been dinned into my soul millions and millions of times, so that I could never forget them, a strange thing came to pass—there was a kaleidoscopic change—I had another dream.*
>
> ***—Major General Sir Ernest Swinton,* The Defense of Duffer's Drift**[74]

General Backsight awoke from a feverish nightmare with an urgent sense that the emerging DOD Cloud project was in danger. As he contemplated this, he recalled other images, from real life—diagrams, tables, pyramids, and flowcharts—from a recent briefing he had largely ignored, some vendor with a clever name talking about security and social media. He recalled another recent meeting, a consultant from that vendor exhorting him to create his own Twitter account, and LinkedIn, and Facebook, and so on, which he had also ignored; he was never much one for self-promotion. He also recalled, of course, extensive news coverage of "election interference" that seemed to come down to a certain adversary buying ads on Facebook, but no one had tried to convince him that the ads actually changed enough votes to matter, so he had largely ignored that hullabaloo as well; anyway, politics wasn't his business. He recalled a briefing with slides titled "Disinformation 101," but it seemed like a mere review of the psyops he had learned about decades ago. Another memory came to him, the movie *Inception*, which he had enjoyed greatly but considered a guilty pleasure, with its silly notion of real people fighting dream battles with

real consequences. Dream battles on a dream battlefield. The sixth dimension of battle, maybe. He heard Rod Serling saying, "A dimension not of sight and sound, but of mind," and, suddenly, he understood how all the pieces fit together as a new dimension of battle, or maybe "security" was a better word, with its own kinds of tactics, countermeasures, and so on.

Later that day, he met with his old friend Senator Forethought who had seen many of the same briefings (and also liked *Inception* and *The Twilight Zone*). He explained his new understanding of these briefings, how they were talking about a new dimension of security, a field so new that the teams giving these briefings didn't even use the same words as each other: "disinformation," "misinfosec," "cognitive security." He shared his intuitive grasp of how the newest communication technologies created a highly mobile ocean of ideas, beliefs, and identities—real, stolen, and synthetic—and that the movement of waves in this ocean represented the changing priorities and motivations of millions of individuals all at once. Anyone with sufficient cleverness and modest resources could learn to make waves in this ocean and, thus, exercise enormous power. With this shared understanding, they developed the outline of a plan to protect the Cloud project, which ultimately led to these preparations:

- Pursuing a wide range of approaches to developing better relationships between defense and the technology sector, including quietly but widely seeding the idea that, at the very least, tech companies should not work with adversarial foreign nations instead of the United States.
- Taking advantage of improved relations to develop regulations and policy guidelines to limit the most potentially harmful forms of mass amplification on social networks, especially amplification that takes place entirely behind encryption, by limiting the size and forwarding rate of groups on individual messaging platforms, for example.
- Promoting a culture in all levels of the defense community to exercise widespread and vocal transparency about national security–relevant evidence-based policies, emphasizing in particular that the duty to stay out of partisan politics does not trump the necessity for evidence-based national security policies and practices. In other words, if a politician says the earth is flat, you have a duty to contradict him if the topic at hand is satellite navigation.
- Investing more in publicizing official documents of national security strategy and priority, so the general public (and elected officials) are less confused about who exactly our allies and adversaries are, and developing social norms in the defense community around remaining loyal to that distinction.
- Reiterating the traditional assertion that high-quality education is a primary national security priority, including education on media literacy and critical thinking, and particularly awareness of cognitive fallacies, such as "false equivalence," and how they feed into journalism.

- Taking deepfake-identification technology out of the lab and running it in real time; this didn't work very well at first but was funded in hopes it would become more effective over time.
- Mandatory monitoring of social network identities—on every possible platform, of everyone above a certain level of authority—to prevent impersonation.
- With consent, monitoring defense personnel's individual social media profiles for mass collection by suspicious entities.
- Tasking SIGINT with a "listening station" to monitor mentions of defense-relevant topics on social networks, with ongoing research to identify signals of coordinated campaigns.
- Studying past campaigns to understand the psychological and operational aspects of composing and propagating narratives and counternarratives to achieve (or prevent) predictable demographic movements and behaviors.

General Backsight and Senator Forethought were enthusiastic about their novel defensive plans, so they were somewhat disappointed when the first wave of Duffer Deep State Deepfakes hit, and they were pretty bad. They were alerted to the first video almost immediately, and took it down from several platforms, but, nevertheless, it spread widely. However, when the deepfake train finally ended, the damage was limited. After the first few videos, communication between the listening station and the platforms started to run smoothly, and the last few videos were taken down quickly enough to restrict their spread. Senator Boer amplified the narrative and received a significant amount of criticism in return, from both sides of the aisle. Sensationalism won out in the mainstream news, and the rumors were nearly ubiquitous, but after the initial news cycle, they seemed to fade a bit more quickly than previously and there was more of a backlash against those who embraced the hoax. One could see the video campaign as a failure of the defense, but careful analysis suggested that the countermeasures had at least succeeded in imposing greater costs on the various actors involved.

Things got considerably worse when the riots hit Waschout. By now, General Backsight had no specific recollection of his dream, but he was certain that these developments were bad, with multiple casualties and damage to both the embassy and Duffer Corp. offices. Eventually, investigators determined the agents of Incidentambia had been quite concerned when they learned of the new limitations on group size, and so allocated ten times the funding to this operation. They hired an army of locals as phone-farm operators, and with such large numbers, a few of them turned out to have a real knack for the operation and joined the Incidentambia agents in planning the strategy. As a result, the campaign benefited from a fine-tuned understanding of local culture and customs, which the US defensive team lacked. In the end, this round may have gone poorly, but it provided a valuable lesson.

Over the next few years, the various scenarios played out, and as Backsight reviewed the outcomes, he felt confident that this was a stand-up fight and not the one-sided

nightmare he recalled dimly. Backsight was now a highly respected expert in misinfosec. He was praised when the IC found evidence that his preventive countermeasures had caused Incidentambia to abandoned plans to wreak havoc by impersonating senior US military social media accounts. General Backsight was convinced that the outcome would have been devastating, although he could never quite say why he was so sure. As Duffer Corp. neared completion of the main installation, Backsight and the narrowly reelected Senator Forethought found themselves having a late-night chat about the strange story of Backsight's warning dream.

"War is never easy," said Backsight, "and that's exactly what this is. I remember I used to think, who cares about some tweets and some Facebook ads? That stuff is for kids! But with all I've seen, I know that entire nations can fall on this battlefield."

"Yes, it's been a rough ride, and frightening at times," said Forethought. "Do you think it will ever be over? Will we win?"

Backsight thought a moment. "I don't think this is the kind of conflict that ends," and although Forethought looked crestfallen, Backsight was merely thoughtful. "It's like asking, will the police ever win? Will we ever defeat crime? Might as well ask, will we ever defeat bad weather!" He laughed. "No, this is a security matter, not a traditional war. There's no 'adversary' to defeat… or, rather, anyone who wants to can play the role of adversary. Anyone can afford to get in on this game, that's what technology has brought us to," he said, staring into space as he took another sip of his drink. "I honestly don't know what to think. The analogy of defeating crime, that's apt. There's an old saying, police work is only easy in a police state. Or," he sat back, "'The Price of Freedom is Eternal Vigilance'. Back when I had that dream, we weren't vigilant at all. We weren't prepared. I think that what I saw in my dream was a potential future where we didn't even put up a fight because we didn't even know how to find the battlefield. But I think you must agree, we're solidly in the game now."

Forethought nodded, listening intently. "I feared we would be sitting ducks, but we are putting up a real fight. And maybe we aren't on our way to winning once and for all, but neither are we on our way to losing. I think we can stay a half-step ahead of the bad guys for a while yet. And if that's what my career gives to my country, then I can sincerely say I'm proud. I did my best."

With that, they raised their glasses and finished their drinks. Not too much later, General Backsight retired and moved back to his hometown of Dreamdorp, where he took up fishing as a hobby, and his children and grandchildren soon became quite sick of hearing the same social engineering joke every time they saw him.

Authors' note: In 2019, when we wrote about both the imaginary Senator Boer spreading baseless conspiracy theories and the attack on the US embassy in the imaginary nation of Waschout, we were concerned that we might have gone too far for anyone to find the scenarios believable, but, in the wake of the attack on the US Capitol on January 6, 2021, we became concerned that we might not have gone far enough and hope our readers find our scenarios to still be relevant.

Endnotes

1 Tzu S. The Art of War. Library of Alexandria; 1961. 204 p. http://classics.mit.edu/Tzu/artwar.html.

2 "List of Close Election Results." Wikipedia. [cited 2020 Jun 22]. https://en.wikipedia.org/wiki/List_of_close_election_results; MIT Election Data and Science Lab. Election Data Archive. [cited 2020 Jun 22]. https://electionlab.mit.edu/data.

3 Kovaric, B. *Revolutions in Communication: Media History from Gutenberg to the Digital Age*. 2nd ed. Bloomsbury Academic, 2019.

4 "The History of Paper." Paper Sizes. [cited 2020 Jun 22]. https://www.papersizes.org/paper-history-overview.htm.

5 "Printing Press." History.com. 2018 [cited 2020 Jun 22]. https://www.history.com/topics/inventions/printing-press.

6 Francois W. "Vernacular Bible Reading in Late Medieval and Early Modern Europe: The 'Catholic' Position Revisited." Cathol Hist Rev. 2018;104(1):23–56. https://muse.jhu.edu/article/691024.

7 "Morse Code & the Telegraph." History.com. 2009 [cited 2020 Jun 22]. https://www.history.com/topics/inventions/telegraph.

8 Smith-Rose RL. "Guglielmo Marconi: Italian Physicist." *Encyclopedia Britannica*. [cited 2020 Jun 22]. https://www.britannica.com/biography/Guglielmo-Marconi.

9 International Radiotelegraph Convention (1906). Govt. print. off. in Washington, 1912, Internet Archive, December 18, 2011. https://openlibrary.org/books/OL7216568M/International_radio_telegraph_convention_of_Berlin_1906.

10 International Radiotelegraph Convention (1906), Internet Archive, 2011.

11 Klein, Christopher, "How 'The War of the Worlds' Radio Broadcast Created a National Panic," History.com, October 30, 2013, https://www.history.com/news/inside-the-war-of-the-worlds-broadcast.

12 Eschner, K. "The Farmboy Who Invented Television." Smithsonian Magazine. [cited 2020 Jun 22]. https://www.smithsonianmag.com/smart-news/farmboy-who-invented-television-while-plowing-180964607/.

13 Hoff, P. "German Television (1935–1944) as Subject and Medium of National Socialist Propaganda." Hist J Film Radio Telev. 1990 Jan 1 [cited 2020 Jun 22];10(2):227–40. https://doi.org/10.1080/01439689000260181; "Berlin 1936 Olympic Games: History, Poster, and Facts." *Encyclopedia Britannica* [cited 2020 Jun 22]. https://www.britannica.com/event/Berlin-1936-Olympic-Games; "What Happened When Hitler Hosted the Olympics 80 Years Ago" Time. [cited 2020 Jun 22]. https://time.com/4432857/hitler-hosted-olympics-1936/.

14 Hirsch, P. M. "Television as a National Medium: Its Cultural and Political Role in American Society." In: *Handbook of Urban Life*. 1978. p. 389–427; Neuman, W. R. "Television and American Culture: The Mass Medium and the Pluralist Audience." *Public Opin Q*. 1982 [cited 2020 Jun 22];46(4):471–87. https://www.jstor.org/stable/2748768; Price ME, Price DP of LBNCS of LME. *Television, the Public Sphere, and National Identity*. Clarendon Press; 1995. 324; Publisher A removed at request of original. 9.2 "The Relationship Between Television and Culture." In: *Understanding Media and Culture*. University of Minnesota Libraries Publishing edition, 2016. This edition adapted from a work originally produced in 2010 by a publisher who has requested that it not receive attribution.; 2016 [cited 2020 Jun 22]. https://open.lib.umn.edu/mediaandculture/chapter/9-2-the-relationship-between-television-and-culture/; Code of Practices for Television Broadcasters. In: Wikipedia. 2020 [cited 2020 Jun 22]. https://en.wikipedia.org/w/index.php?title=Code_of_Practices_for_Television_Broadcasters&oldid=961558806.

15 ENIAC - CHM Revolution. [cited 2020 Jun 22]. https://www.computerhistory.org/revolution/birth-of-the-computer/4/78.

16 "ARPANET: Definition & History." *Encyclopedia Britannica*. [cited 2020 Jun 22]. https://www.britannica.com/topic/ARPANET.

17 Then and Now: A History of Social Networking Sites. [cited 2020 Jun 22]. https://www.cbsnews.com/pictures/then-and-now-a-history-of-social-networking-sites/.

18 Henry, Zoë, "Mark Zuckerberg's 10 Best Quotes Ever," *Inc.*, October 14, 2014, https://www.inc.com/zoe-henry/mark-zuckerberg-move-fast-and-break-things.html.

19 Haidt J, Rose-Stockwell T. "The Dark Psychology of Social Networks." *Atlantic*. 2019;(December). https://www.theatlantic.com/magazine/archive/2019/12/social-media-democracy/600763/; Harbath K. Hard "Questions: Social Media and Democracy." Facebook Press Release. 2018. https://about.fb.com/news/2018/01/hard-questions-democracy/; Lever R. Social media and democracy: optimism fades as fears rise. Phys.org. 2017. https://phys.org/news/2017-10-social-media-democracy-optimism.html.

20 "How to Hack People." BBC News World Edition. 2002 [cited 2020 Jun 22]. http://news.bbc.co.uk/2/hi/technology/2320121.stm.

21 Whitworth B, Ahmad A. *The Social Design of Technical Systems: Building Technologies for Communities.* 2nd ed. Interaction Design Foundation; 2013. https://www.interaction-design.org/literature/book/the-social-design-of-technical-systems-building-technologies-for-communities-2nd-edition/about-this-book; Wikipedia Community. Sociotechnical system. Wikipedia. [cited 2020 Jun 22]. https://en.wikipedia.org/wiki/Sociotechnical_system.

22 Interaction Design Foundation. "Socio-Technical Systems." Interaction Design Foundation. [cited 2020 Jun 22]. https://www.interaction-design.org/literature/topics/socio-technical-systems.

23 Beckers K, Krautsevich L, Yautsiukhin A. "Analysis of Social Engineering Threats with Attack Graphs." In: Garcia-Alfaro J, et al., eds. *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*. Springer; 2015. https://link.springer.com/chapter/10.1007%2F978-3-319-17016-9_14.

24 Breda F, Barbosa H, Morais T. "Social Engineering and Cyber Security." In: *International Technology, Education and Development Conference*. 2017. p. 4204–4211. https://www.researchgate.net/publication/315351300_SOCIAL_ENGINEERING_AND_CYBER_SECURITY.

25 Goerzen M, Watkins EA, Lim G. "Entanglements and Exploits: Sociotechnical Security as an Analytic Framework." In: 9th USENIX Workshop on Free and Open Communications on the Internet (FOCI '19). Santa Clara, CA: USENIX association; 2019. https://www.usenix.org/conference/foci19/presentation/goerzen; Sheridan K. A Socio-Technical Approach to Cybersecurity's Problems. Dark Reading. 2020. https://www.darkreading.com/perimeter/a-socio-technical-approach-to-cybersecuritys-problems/d/d-id/1335043.

26 Walker CR, Terp S-J, Breuer PC, Courtney L Crooks. "Misinfosec: Applying Information Security Paradigms to Misinformation Campaigns." WWW 19 Companion Proc 2019 World Wide Web Conf. 2005;1026–1032. https://dl.acm.org/doi/10.1145/3308560.3316742; Rosenblatt S. Meet 'misinfosec': Fighting fake news like it's malware. The Parallax. 2019. https://the-parallax.com/2019/04/17/misinfosec-fighting-fake-news-malware/.

27 Peterson N. "How America's Adversaries Are Using Hybrid Warfare to Capitalize on Civil Unrest." *Coffee or Die*. 2020 [cited 2020 Jun 22]. https://coffeeordie.com/hybrid-war-america.

28 Nimmo B. "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It." *StopFake.org*. 2015 [cited 2020 Jun 22]. https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/.

29 Mozur P. "A Genocide Incited on Facebook, with Posts from Myanmar's Military." New York Times. 2018; A1. https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html; Matishak M, Desiderio A. "Senate Intel report Confirms Russia Aimed to Help Trump in 2016." Politico. 2020. https://www.politico.com/news/2020/04/21/senate-intel-report-confirms-russia-aimed-to-help-trump-in-2016-198171.

30 Davis ZS, Lehman R, Nacht M, eds. *Strategic Latency and World Power: How Technology Is Changing Our Concepts of Security*. Livermore, CA: Lawrence Livermore National Laboratory Center for Global Security Research; 2014 [cited 2020 Jun 23]. https://cgsr.llnl.gov/content/assets/docs/STATEGIC_LATENCY_Book-WEB.pdf.

31 Solis B, Breakenridge DK. *Putting the Public Back in Public Relations: How Social Media Is Reinventing the Aging Business of PR*. FT Press; 2009. https://books.google.com/books?hl=en&lr=&id=xLXinA8LbTMC.

32 Ingram M. "How Google and Facebook Have Taken Over the Digital Ad Industry." *Fortune*. 2017 Jan 4 [cited 2020 Jun 24]; https://fortune.com/2017/01/04/google-facebook-ad-industry.

33 Davis, Lehman, and Nacht, *Strategic Latency and World Power*, 2014.

34 Lincoln JE. "What Is Black Hat Social Media & Does It Affect SEO?" *Search Engine Land*. [cited 2019 Nov 20]. https://searchengineland.com/blackhat-social-media-affect-seo-199516; Carter B. White Hat vs Black Hat Social Media Optimization. Search Engine People. 2008 [cited 2020 Jun 22]. https://www.searchenginepeople.com/blog/white-hat-vs-black-hat-social-media-optimization.html; Rampton J. "Social Media Is the New Blackhat." Forbes. [cited 2019 Nov 20]. https://www.forbes.com/sites/johnrampton/2014/07/21/social-media-is-the-new-blackhat.

35 Cialdini RB. *Influence: Science and Practice*. Allyn and Bacon; 2001. 274 p.

36 Schneider J. "Cognitive Biases Definition Plus 6 Powerful Marketing Examples." *ABTasty*. 2018 [cited 2020 Jun 22]. https://www.abtasty.com/blog/powerful-cognitive-biases/; Wikipedia community. List of psychological effects. Wikipedia. [cited 2020 Jun 22]. https://en.wikipedia.org/wiki/List_of_psychological_effects; Wikipedia community. List of fallacies. Wikipedia. [cited 2020 Jun 22]. https://en.wikipedia.org/wiki/List_of_fallacies; Wikipedia community. List of cognitive biases. Wikipedia. [cited 2020 Jun 22]. https://en.wikipedia.org/wiki/List_of_cognitive_biases; Raconteur. "Cognitive Bias." Risk Culture. 2018. https://www.raconteur.net/infographics/cognitive-bias.

37 Patel, Neil. "Foot-in-the-Door Technique: How to Get People to Seamlessly Take Action." *Forbes*, Oct 13, 2014, https://www.forbes.com/sites/neilpatel/2014/10/13/foot-in-the-door-technique-how-to-get-people-to-take-seamlessly-take-action/#5704bc547d9e.

38 Wikipedia community. Door-in-the-face technique. Wikipedia. [cited 2020 Jun 22]. https://en.wikipedia.org/wiki/Door-in-the-face_technique.

39 Glascock C. "A Picture Is Worth a Thousand Words." *Propaganda for Change*. [cited 2020 Jun 22]. http://persuasion-and-influence.blogspot.com/2015/01/a-picture-is-worth-thousand-words.html.

40 Wardle C. "Information Disorder: 'The Techniques We Saw in 2016 Have Evolved.'" *Essential Guide to Understanding Information Disorder*. 2019 [cited 2020 Jun 22]. https://firstdraftnews.org/latest/information-disorder-the-techniques-we-saw-in-2016-have-evolved/.

41 Birkett A. "The Halo Effect: How it Affects Marketing and UX." CXL. 2016 [cited 2020 Jun 22]. https://cxl.com/blog/halo-effect/.

42 Schneider, "Cognitive Biases Definition Plus 6 Powerful Marketing Examples," 2018.

43 Leonard JG. "Propaganda Techniques to Recognize." Communication Methods Course Syllabus. [cited 2020 Jun 22]. https://www.uvm.edu/~jleonard/AGRI183/propoaganda.html; Wikipedia Community. Scapegoating. Wikipedia. [cited 2020 Jun 22]. https://en.wikipedia.org/wiki/Scapegoating.

44 Paul C, Matthews M. "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It." RAND Corporation; 2016 [cited 2020 Jun 22]. https://www.rand.org/pubs/perspectives/PE198.html.

45 The Problem of So-Called "Push Polls": When advocacy Calls Are Made under the Guise of Research. 2007 [cited 2020 Jun 22]. https://www.aapor.org/Standards-Ethics/Resources/AAPOR-Statements-on-Push-Polls.aspx.

46 Fallows J. "The Press Is Embracing False Equivalence—Again." *Atlantic*. 2019 [cited 2020 Jun 22]. https://www.theatlantic.com/ideas/archive/2019/09/patient-zero-of-the-next-false-equivalence-epidemic/598573/; Sarkis S. "This Is Not Equal to That: How False Equivalence Clouds Our Judgment." Forbes. 2019 [cited 2020 Jun 22]. https://www.forbes.com/sites/stephaniesarkis/2019/05/19/this-is-not-equal-to-that-how-false-equivalence-clouds-our-judgment/#79a4ad0b5c0f; False Equivalence. Wikipedia. [cited 2020 Jun 22]. https://en.wikipedia.org/wiki/False_equivalence; Levinger M. Master Narratives of Disinformation Campaigns. J Int Aff. 2018 [cited 2020 Jun 22];71(1.5):125–34. https://www.jstor.org/stable/26508126.

47 Lucas E. "Whataboutism." *Economist*. 2008 Jan 31 [cited 2020 Jun 22]; https://www.economist.com/europe/2008/01/31/whataboutism; da san Martino G, et al. "Prta: A System to Support the Analysis of Propaganda Techniques in the News." ArXiv200505854 Cs. 2020 May 12 [cited 2020 Jun 22]; http://arxiv.org/abs/2005.05854; Propaganda dictionary: Whataboutism – Propastop. Propastop. 2018 [cited 2020 Jun 24]. https://www.propastop.org/eng/2018/01/26/propaganda-dictionary-whataboutism/; Sheth S. "Facts Don't Matter": How Trump Uses One of Putin's Favorite Propaganda Tools. Business Insider. 2017 [cited 2020 Jun 24]. https://www.businessinsider.com/trump-whataboutism-putin-russia-propaganda-2017-8; Headley J. "Challenging the EU's Claim to Moral Authority: Russian Talk of 'Double Standards.'" Asia Eur J. 2015 Sep 1 [cited 2020 Jun 24];13(3):297–307. https://doi.org/10.1007/s10308-015-0417-y; Treurniet R. The Soviet Origins of Russian Information Warfare: Manifestations of Reflexive Control in Ukraine. [Amsterdam]: University of Leiden; 2016 [cited 2018 Jun 24]. https://openaccess.leidenuniv.nl/bitstream/handle/1887/83864/Treurniet_CSM_2017.pdf; Torres-Spelliscy C. Trump's "Whataboutism on Campaign Finance." Brennan Center for Justice. 2019 [cited 2020 Jun 24]. https://www.brennancenter.org/our-work/analysis-opinion/trumps-whataboutism-campaign-finance.

48 Kirillova K. Fear and Hatred: How Propaganda Persuades with Emotion. *StopFake.org*. 2018 [cited 2020 Jun 22]. https://www.stopfake.org/en/fear-and-hatred-how-propaganda-persuades-with-emotion/.

49 Marmura SME. "Likely and Unlikely Stories: Conspiracy Theories in an Age of Propaganda." Int J Commun. 2014 Sep 1 [cited 2020 Jun 22];8(0):2377–95. https://ijoc.org/index.php/ijoc/article/view/2358;
Kane L. "There's a Reason Nigerian Scammers are So Obvious in Their Emails." Business Insider. 2014 [cited 2019 Nov 20]. https://www.businessinsider.com/why-nigerian-scam-emails-are-obvious-2014-5.

50 Yudkowsky E. "Artificial Intelligence as a Positive and Negative Factor in Global Risk." In: Bostrom N, Cirkovic MM, eds. *Global Catastrophic Risks*. 2008 [cited 2020 Jun 24]. p. 308–45. https://intelligence.org/files/AIPosNegFactor.pdf.

51 Patel N. "The Ultimate Google Algorithm Cheat Sheet." 2015 [cited 2020 Jun 24]. https://neilpatel.com/blog/the-ultimate-google-algorithm-cheat-sheet/.

52 O'Connor P. "An Introduction to Black Hat SEO." *Hubspot*. 2018 [cited 2020 Jun 24]. https://blog.hubspot.com/marketing/black-hat-seo;
Ethical & non-ethical techniques of doing SEO [Infographic]. GO-GULF. 2020 [cited 2020 Jun 24]. https://www.go-gulf.ae/ethical-non-ethical-techniques-of-doing-seo-infographic/.

53 Solis B, Breakenridge DK. *Putting the Public Back in Public Relations: How Social Media Is Reinventing the Aging Business of PR*. FT Press; 2009. https://books.google.com/books?hl=en&lr=&id=xLXinA8LbTMC;
"Difference between SEO, SEM, SMO and What You Really Need." DMG. 2017 [cited 2020 Jun 24]. https://digitalmarkgroup.com/difference-seo-sem-smo-really-need;
Schneider A. "Which Marketing Strategy Is Best for You? SEO, SEM, SMM, or SMO?" WiseStamp. 2020 [cited 2020 Jun 24]. https://www.wisestamp.com/blog/which-marketing-strategy-is-best-for-you-seo-sem-smm-and-smo/.

54 "Difference Between SEO, SEM, SMO and What You Really Need," DMG, 2017; Schneider, "Which Marketing Strategy Is Best for You?" 2020.

55 "Digital Microtargeting: Political Party Innovation Primer 1." Stockholm: International Institute for Democracy and Electoral Assistance (International IDEA); 2018 [cited 2020 Jun 25]. https://www.idea.int/publications/catalogue/digital-microtargeting;
Wilson DG. "The Ethics of Automated Behavioral Microtargeting." AI Matters. 2017 Oct 10 [cited 2020 Jun 25];3(3):56–64. https://dl.acm.org/doi/10.1145/3137574.3139451;
Resnick B. "Cambridge Analytica's 'Psychographic Microtargeting": What's Bullshit and What's Legit." Vox. 2018 [cited 2020 Jun 25]. https://www.vox.com/science-and-health/2018/3/23/17152564/cambridge-analytica-psychographic-microtargeting-what;
Kafka P. "Facebook's Political Ad Problem, Explained by an Expert." Vox. 2019 [cited 2020 Jun 25]. https://www.vox.com/recode/2019/12/10/20996869/facebook-political-ads-targeting-alex-stamos-interview-open-sourced;
Gibney E. The Scant Science behind Cambridge Analytica's Controversial Marketing Techniques." Nature. 2018 Mar 29 [cited 2020 Jun 25]; https://www.nature.com/articles/d41586-018-03880-4;
Faizullabhoy I, Korolova A. "Facebook's Advertising Platform: New Attack Vectors and the Need for Interventions." arXiv. 2018.

56 Bond C. "Conversion Rate Benchmarks: Find out How YOUR Conversion Rate Compares." *Wordstream*. 2020 [cited 2020 Jun 25]. https://www.wordstream.com/blog/ws/2019/08/19/conversion-rate-benchmarks;
"Priceonomics: The Advertising Conversion Rates for Every Major Tech Platform." Forbes. 2018 [cited 2020 Jun 25]. https://www.forbes.com/sites/priceonomics/2018/03/09/the-advertising-conversion-rates-for-every-major-tech-platform/.

57 Kemp S. "How Really American's Approach Can Really Work for You." *Actionsprout*. 2019 [cited 2019 Nov 20]. http://actionsprout.help/en/articles/405942-how-really-american-s-approach-can-really-work-for-you.

58 Claunch JM, Bernd J, eds. *Mathematical Applications in Political Science*. Vol. 2. Dallas: Southern Methodist University Press; 1966.

59 Russell NJ. "An Introduction to the Overton Window of Political Possibilities." Mackinack Center for Public Policy. 2006 [cited 2020 Jun 24]. http://www.mackinac.org/7504.

60 Astor M. "How the Politically Unthinkable Can Become Mainstream." *New York Times*. 2019 Feb 26 [cited 2020 Jun 24]; https://www.nytimes.com/2019/02/26/us/politics/overton-window-democrats.html.

61 Enron. "Metal Man". Los Angeles: Conquest; [cited 2020 Jun 24]. https://www.adforum.com/creative-work/ad/player/6683/metal-man/enron.

62 Benke G. *Risk and Ruin: Enron and the Culture of American Capitalism*. University of Pennsylvania Press; 2018. 272 p.; Ismail MA. "A Most Favored Corporation: Enron Prevailed in Federal, State Lobbying Efforts 49 Times." Center for Public Integrity. 2003 [cited 2020 Jun 24]. https://publicintegrity.org/politics/a-most-favored-corporation-enron-prevailed-in-federal-state-lobbying-efforts-49-times/; Ismail MA. "Enron's Deregulation Fight." Center for Public Integrity. 2003 [cited 2020 Jun 24]. https://publicintegrity.org/politics/enrons-deregulation-fight/.

63 Bolotsky J. Use Your Radical Fringe to Shift the Overton Window. *Beautiful Trouble*. 2012 [cited 2020 Jun 24]. https://beautifultrouble.org/principle/use-your-radical-fringe-to-shift-the-overton-window/; Herriges D. "Moving the Overton Window." Strong Towns. 2015 [cited 2020 Jun 24]. https://www.strongtowns.org/journal/2015/7/30/moving-the-overton-window; Lee A. "Moving the Overton Window." Big Think. 2011 [cited 2020 Jun 24]. https://bigthink.com/daylight-atheism/moving-the-overton-window; Marsh L. "The Flaws of the Overton Window Theory." New Republic. 2016 Oct 27 [cited 2020 Jun 24]; https://newrepublic.com/article/138003/flaws-overton-window-theory; Stoft S. Ripped Apart: How Democrats Can Fight Polarization and Win. Steven Stoft; 2020. 315 p.; Maza C. "How Trump Makes Extreme Things Look Normal." Vox. 2017 [cited 2020 Jun 24]. https://www.vox.com/2017/12/21/16806676/strikethrough-how-trump-overton-window-extreme-normal; Tweedledee5. The Overton Window's Right-Shift and Dilemma of the Self-Defeating Compromise: How to Solve This? Daily Kos. 2013 [cited 2020 Jun 24]. https://www.dailykos.com/story/2013/5/23/1211270/-The-Overton-Window-s-right-shift-and-dilemma-of-the-self-defeating-compromise-how-to-solve-this.

64 Kroll D. "Five Reasons Not to Take the Cinnamon Challenge." *Forbes*. 2013 [cited 2020 Jun 24]. https://www.forbes.com/sites/davidkroll/2013/04/23/5-reasons-not-to-take-the-cinnamon-challenge/#35bd463c6405; The Cinnamon Challenge... by GloZell and her Big Behind Earrings. 2012 [cited 2020 Jun 24]. https://www.youtube.com/watch?v=Cyk7utV_D2I

65 Bell E. Russian Voices in Western Media Leave Regulators with New Type of Headache." *Guardian*. 2018 Mar 18 [cited 2020 Jun 24]; https://www.theguardian.com/media/media-blog/2018/mar/18/russia-uk-us-media-rt-free-speech; Helmus TC, et al. Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe. Santa Monica, CA; 2018. https://www.rand.org/pubs/research_reports/RR2237.html; Kenney C, Bergmann M, Lamond J. "Understanding and Combating Russian and Chinese Influence Operations." Center for American Progress; 2019 Feb [cited 2020 Jun 24] p. 11. https://www.americanprogress.org/issues/security/reports/2019/02/28/466669/understanding-combating-russian-chinese-influence-operations/; Doescher T. "How China Is Taking Control of Hollywood." Heritage Foundation. 2018 [cited 2020 Jun 24]. https://www.heritage.org/asia/heritage-explains/how-china-taking-control-hollywood; Tartaglione N. "Hollywood & China: U.S. Gov't Agency Agrees to Review Foreign Investment Panel." Deadline. 2016 [cited 2020 Jun 24]. https://deadline.com/2016/10/china-hollywood-congress-wanda-foreign-ownership-gao-1201830426/; Tromblay DE. "No More Fun and Games: How China's Acquisition of U.S. Media Entities Threatens America's National Security," Small Wars Journal, 2017 [cited 2020 Jun 24]. https://smallwarsjournal.com/jrnl/art/no-more-fun-and-games-how-china%E2%80%99s-acquisition-of-us-media-entities-threatens-america%E2%80%99s-nati; Drucker J. "Kremlin Cash behind Billionaire's Twitter and Facebook Investments." New York Times. 2017 Nov 5 [cited 2020 Jun 24], https://www.nytimes.com/2017/11/05/world/yuri-milner-facebook-twitter-russia.html.

66 Breuer PC, Perlman DM. Hacking Ten Million Useful Idiots: Online Propaganda as a Socio-Technical Security Project. Las Vegas, NV; 2019. (Black Hat Briefings). https://www.blackhat.com/us-19/briefings/schedule/#hacking-ten-million-useful-idiots-online-propaganda-as-a-socio-technical-security-project-15456;
Richter M. "The Kremlin's Platform for 'Useful Idiots' in the West: An Overview of RT's Editorial Strategy and Evidence of Impact." European Values: Promoting Freedom; 2017 [cited 2020 Jun 25]. https://www.europeanvalues.net/rt/;
Richter ML. RT: A Low-Grade Platform for Useful Idiots. Atlantic Council. 2017 [cited 2020 Jun 25]. https://www.atlanticcouncil.org/blogs/ukrainealert/rt-a-low-grade-platform-for-useful-idiots/;
Showalter M. "To Propagandize the West, Lenin Recruited a Corps of "Useful Idiots." Investor's Business Daily. 2013 [cited 2020 Jun 25]. https://www.investors.com/politics/commentary/lenin-used-useful-idiots-to-spread-propaganda-to-the-west/.

67 Perlman DM. "Applied Computational Social Choice Theory as a Framework for New Cyber Threats." *Cyber Def Rev*. 2019 Dec 9 [cited 2020 Jun 22] ;(December). https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2035048/applied-computational-social-choice-theory-as-a-framework-for-new-cyber-threats/.

68 "Protect Your Brand: How to Battle Disinformation Campaigns." *Recorded Future*. 2019 [cited 2020 Jun 23]. https://www.recordedfuture.com/battle-disinformation-campaigns/; "The Price of Influence: Disinformation in the Private Sector." Recorded Future. 2019 [cited 2020 Jun 23]. https://www.recordedfuture.com/disinformation-service-campaigns/; "Rethinking Brand Protection in the Social Media Protection Era." ZeroFOX. 2018 [cited 2020 Jun 25]. https://www.zerofox.com/blog/rethinking-brand-protection/; Foster JC, Wolfe S, Gustafson C. Social Media Protection for Dummies, ZeroFOX Special Edition. Hoboken, NJ: John Wiley & Sons; 2018 [cited 2020 Jun 25]. 53 p. https://get.zerofox.com/rs/143-DHV-007/images/Social-Media-Protection-For-Dummies-ZeroFOX-Special-Edition.pdf; Zhou X, Zafarani R. "Fake News: A Survey of Research, Detection Methods, and Opportunities." arXiv.org. 2018; cs.CL. arXiv.org; Zhou X, et al. "Fake News Early Detection: A Theory-Driven Model." arXiv.org. 2019; cs.CL. arXiv.org; Mama R, Shi S. "Towards Deepfake Detection That Actually Works." Dessa. 2019 [cited 2020 Jun 25]. https://www.dessa.com/post/deepfake-detection-that-actually-works.

69 Mann DrAK, Cobaugh PL. *Introduction to Narrative Warfare: A Primer and Study Guide*. CreateSpace; 2018.

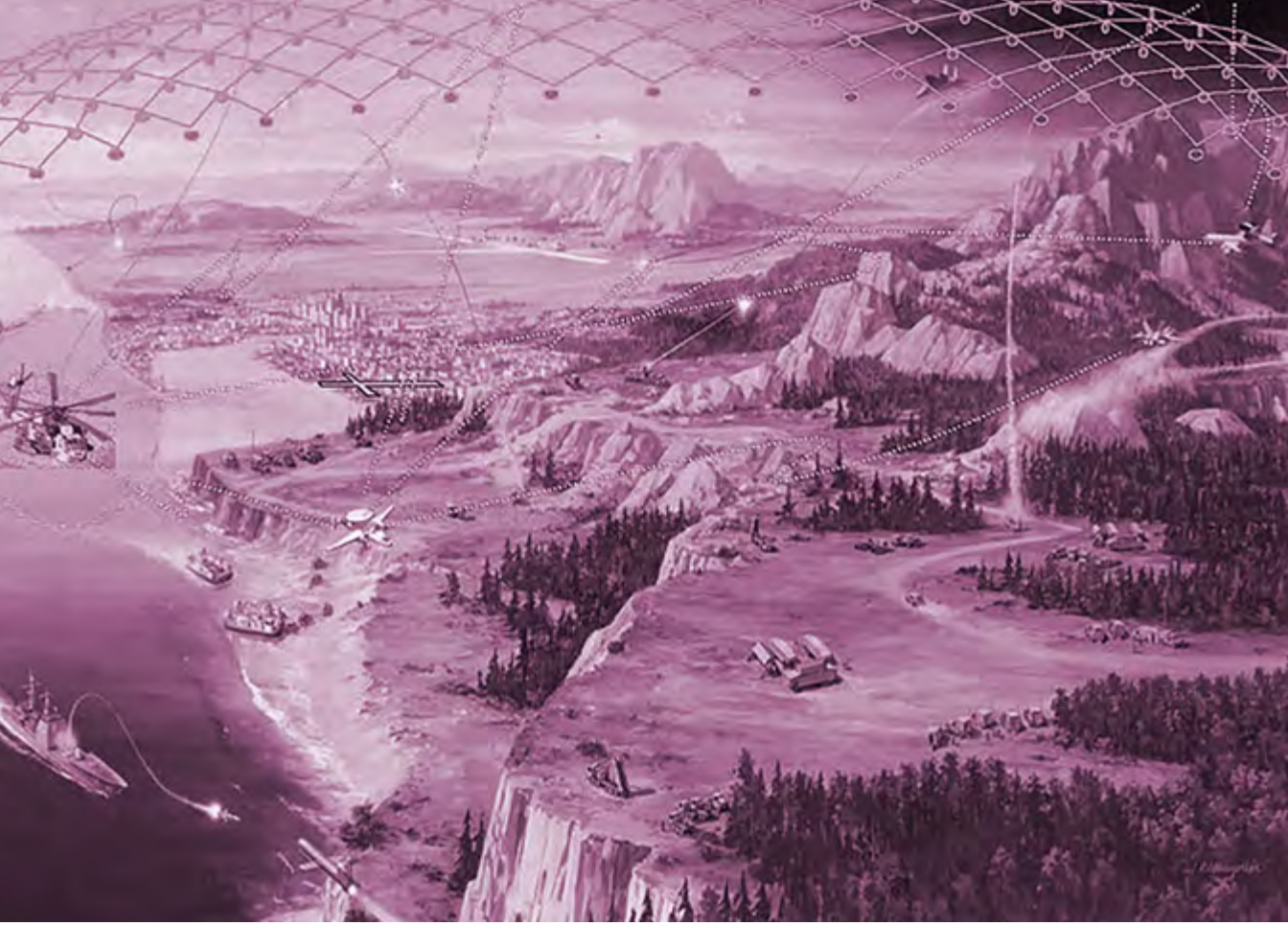
70 Scott KD. JP 5-0, Joint Planning. Joint Chiefs of Staff; 2017 Jun [cited 2018 Jun 24] p. 360. (Joint Planning). Report No.: 5–0. https://www.jcs.mil/Doctrine/DOCNET/JP-5-0-Joint-Planning/.

71 Scaparrotti CM. JP 3-13, Information Operations. Joint Chiefs of Staff; 2012 Nov [cited 2020 Jun 24] p. 87. (Joint Publications). Report No.: 3–13. https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/.

72 MITRE ATT&CK®. [cited 2020 Jun 25]. https://attack.mitre.org/.

73 About STIX | STIX Project Documentation. [cited 2020 Jun 25]. https://stixproject.github.io/about/.

74 Swinton ED. The Defense of Duffer's Drift. United States Infantry Association; 1904 [cited 2020 Jun 25]. 74 p. https://www.google.com/books/edition/The_Defence_of_Duffer_s_Drift/dKhJAAAAIAAJ.



SECTION 6

OPERATIONAL CONSIDERATIONS FOR MULTIDOMAIN WARFARE

CHAPTER 30

Irregular as the New Normal: How Technology Will Change the Prevalence and Character of Irregular Warfare

Richard A. K. Lum and LTC Edwin Churchill

As the world moves through a period of multiple, simultaneous transitions, a number of technology-related trends and emerging issues are increasing the likelihood that irregular warfare will not only be more prevalent in the future but also take on new and challenging forms. Confronting these evolving and proliferating challenges will be the job of special operations forces (SOF), who today need to focus more—not less—attention on the ways in which irregular warfare will evolve and play key roles in the many conflicts to come.

Introduction

The present is a period of transition. Geopolitically, we have witnessed the end of an era of US primacy and anticipate the crystallization of a new one. Not unrelated, we are also observing the rapid emergence and evolution of multiple technologies, each of which would pose tremendous disruption on their own; taken together and in coevolution they portend a massive shift in economy and society. As we contemplate this transition, many in the military realm are solidifying a frame of reference that uses "state versus state," "great-power conflict," or "conventional battle" as one of the primary frames. When using this frame, "irregular warfare" is necessarily sidelined as a future challenge and a key competency as we change our perspectives and our military posture to counter large conventional military threats. We believe this is a mistake. History has shown that irregular warfare is historically the most common form of armed conflict among humans. Even a cursory review of recent trends would suggest irregular warfare will become more revalent in the future.

This chapter adopts the Department of Defense definition of irregular warfare as, "a violent struggle among state and nonstate actors for legitimacy and influence over the relevant populations. Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will."[1] Using this US definition, we will explore briefly some of the reasons why we anticipate more irregular threats in the future and how technology may impact the possibilities for irregular warfare in the future.

Foresight: Anticipating Change

This chapter takes a "futures studies" approach to considering how and why the futures of irregular warfare may look considerably different than its present configuration. An often misunderstood academic field, futures studies concentrates

on understanding and anticipating change in society and using that insight (foresight) to help people reframe their expectations and preferences for the future. Here we will briefly introduce a few key futures concepts that inform this chapter.

Building Blocks for Foresight

Foresight is not prediction but perhaps best thought of as insight into how and why the future could be different from the present. Within the field of futures, researchers use many approaches and methodologies to study change, generate forecasts, and develop foresight. Two of the most important building blocks are *trends* and *emerging issues*. Of the two, trends will be the most familiar to readers. They are descriptions of history. Trends describe past changes that we have measured. Examples of trends include the shrinking middle-class population and rising health-care expenditures.

While trends are extremely important building blocks for foresight, they are far from the only things to consider. All trends bend or break at some point. One of the reasons they do so is what we call emerging issues. In contrast to trends, which are historical, emerging issues are things that may mature to importance in the future, such as emerging technologies, future policy issues, and new ideas or concepts. Useful emerging issues are things that, while fringe or experimental today, might have a meaningful impact on the future if they survive, mature, and enter the mainstream. Historical examples of what were once emerging issues and have become critical parts of everyday life include environmentalism, cellular phones, in vitro fertilization, and social media. Each of these were once considered fringe thinking or just plain futuristic.

Mapping Possible Futures of High Change

While everyone asks questions about the future, they are often asking different questions. Some folks take a *telescopic* view of the future, trying to see a specific thing more clearly at a farther distance. In contrast, a *panoramic* view of the future takes in a broad sweep of the emerging landscape. Those taking a panoramic view are concerned with getting a sense of the general contours of the landscape and the directions that can be taken. It is less about zooming in on the details of a specific tree and more about understanding that the forest ends and canyons take over.

This chapter takes a panoramic approach to exploring the emerging landscape. In doing so, we focus our efforts on exploring the more divergent, logical future possibilities. Divergent, disruptive scenarios allow us to explore a broader sweep of a specific emerging landscape, as represented conceptually in figure 1, below. Of our foresight building blocks, emerging issues are particularly valuable for taking us out into the bands of high change. Thus, emerging issues are the focus of our exploration and discussion.

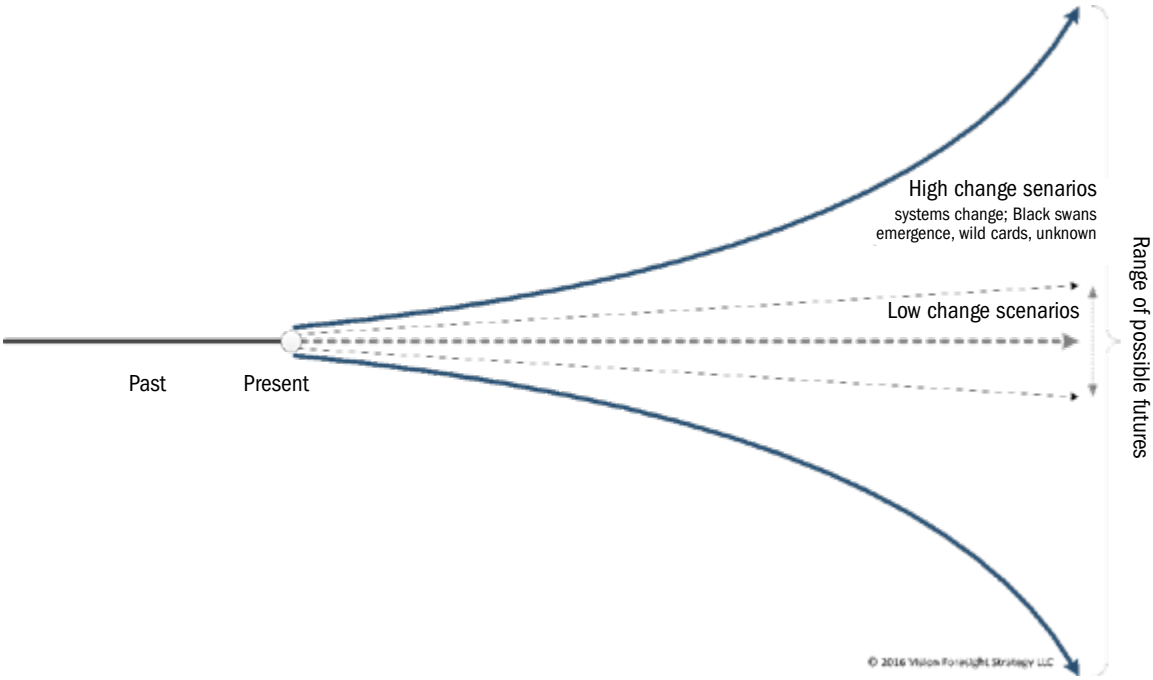


Figure 1: Focusing on mapping high-change scenarios.[2]

Trends: Technological Change Driving the Growth of Irregular Warfare

A number of ongoing global changes suggest irregular warfare will become more important in the future. Some of these trends, such as climate change, promise to impact most categories of human conflict. Others, such as the growth in societal surveillance systems, will play significant roles in shaping particular irregular threats and operations. Technological trends in particular are shaping the future character and likelihood of irregular warfare.

At the global level there are a number of changes underway that may impact the general propensity for and the character of future conflict. These shifts affect the broader contexts for conflict and also relate to the kinds of irregular threats and operations with which we are already familiar. Climate change will increasingly put pressure on littoral communities, water and food systems, and human health. Urbanization continues to progress rapidly, with attendant stress on governance systems, housing, and human health and increased opportunities for criminality. Trends in growing numbers of migrant and refugee flows point to increased stress on recipient states and risks for activities such as human trafficking and recruitment for violent movements (see figure 2). Finally, the growth in global illicit trade suggests greater weakening of governance in some regions and growing world markets to supply irregular threats such as insurgents and terrorists.

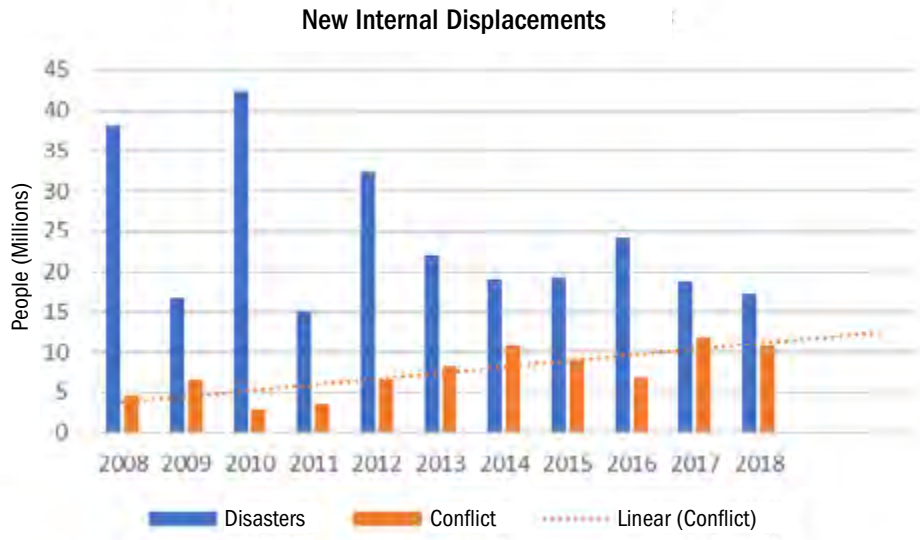


Figure 2. New displacements associated with conflict, violence, and disasters (2008–2018).[3]

A Changing Landscape

Geopolitically, the global landscape has shifted in important ways. Today, we confront aggressive peer and near-peer competitors intent on reshaping norms and reality on the ground. Russian hybrid-warfare operations and Chinese gray-zone strategies are innovations in the modern pursuit of state interests, challenges we have only recently begun to address. In an environment of technologically sophisticated, nuclear-armed, and aggressive competitors, traditional diplomacy will be increasingly challenging, while direct military confrontation will continue to be undesirable. In this context, clandestine and covert approaches will continue to grow more attractive to policy makers.

In terms of our built environment, technology has always played a major role in altering the shape and character of the places in which we live. As we push deeper into the digital era, technology is dramatically reshaping a deceptively familiar landscape. Society is rapidly digitizing itself, shifting more and more functions to the digital environment of computers and the internet. The Internet of Things (IoT) is the trend of embedding computing power and internet connectivity into every conceivable human-made object around us. From watches to phones to household appliances and cars, the built environment around us is rapidly becoming densely interconnected and inherently *aware* of our presence and our actions. Across these sprawling, digital ecosystems move a growing number of soft machines, programs that carry out automation, learn on their own, and even evolve in competition with one another.

In this digital era, therefore, a layer of digital life—some of which is directed by humans and a growing amount that is not—mediate our daily experiences. Increasingly, a vast array of digital systems layered through our built environment

shape what we see and hear, perceive and think, and are able (and incentivized) to do. Thus, the built environment around us looks like the world we remember and yet is aware, calculating, and responsive in a way we traditionally only ascribed to the natural world. Further, it can be subtly and invisibly *manipulated* by others in ways unique to the current era. Our cities and homes are becoming digital jungles at once familiar and uniquely alien.

Across this changed landscape data has become the new electricity, the lifeblood of virtually all activities. Data flows across all digital connections, and understanding how to generate, acquire, and process this data is key to thriving in this evolving landscape (see figure 3). While social and economic disparities of the present understandably loom large in the public mind, moving forward, those who do not understand and are not able to use data will be left behind rapidly.

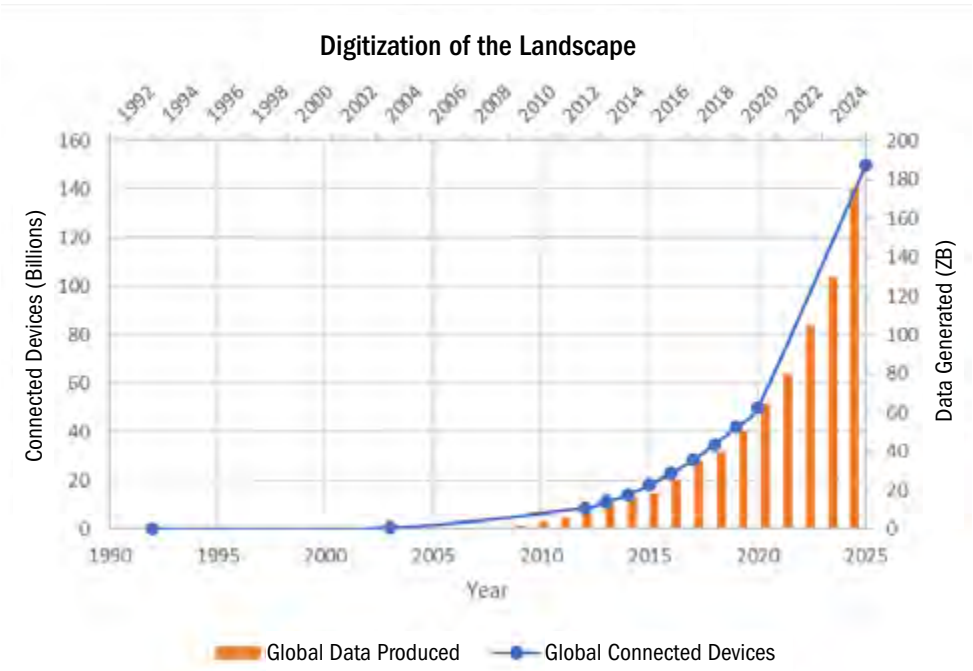


Figure 3. Digitization of the landscape.[4]

Diffusion of Capabilities

One of the most pronounced impacts of technology on conflict has been the diffusion of (previously) statelike capabilities to the smallest actors. While technology has often had a leveling effect in history, the nature of the tools available today to a growing number of actors, coupled with the changing nature of the conflict environment, offers small groups and individuals the opportunity to acquire the power to produce genuinely strategic effects. From a foresight perspective, we want to examine these technologies early for both their positive and negative potential. Technologies are not inherently good or bad; they become so in their application.

To avoid assuming that all emerging technologies are threats to us, we have to anticipate their emergence and shape their development.

The pervasive digitization of society makes cyber tools particularly attractive to actors looking to conduct a broad range of operations, from intelligence gathering to theft and direct disruption. Somewhat related, the importance of social media in daily life across the world offers actors of all types unprecedented opportunities for information gathering, profiling, narrative influence, outright disinformation, and global recruitment. Continuing advances in areas such as computing and robotics lead to trends like the decreasing cost and increasing sophistication of unmanned systems. Digital fabrication offers hobbyists and professionals alike the ability to custom manufacture everything from spare parts to entire homes. Through commercial services, do-it-yourself systems, and crowdsourcing (see figure 4), the average person can access impressive levels of intelligence, surveillance, and reconnaissance (ISR). And through crowdfunding, individuals and groups can—literally—acquire millions of dollars of volunteered investment to fund anything imaginable, from children's books to terrorist innovations.

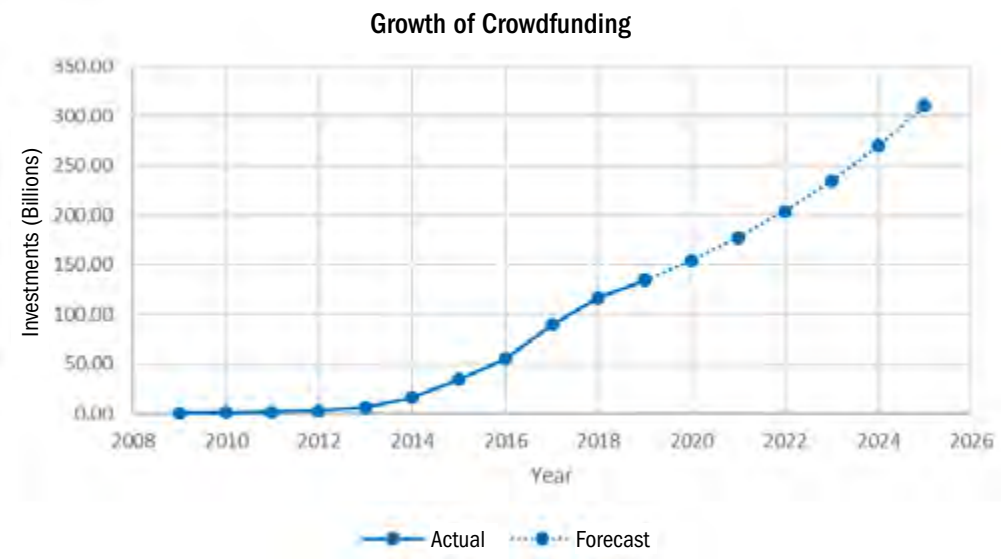


Figure 4. Growth of Crowdfunding.[5]

Across the long course of human history, only an incredibly small percentage of people played a role in innovating tools and techniques within warfare. This number grew slightly during the Enlightenment and then accelerated during the Industrial Revolution. Today, because of our changed technological landscape and because of readily available, adaptable, and largely digital tools, virtually anyone can acquire the means and knowhow to attack or undermine an opponent or provide support to those who do so. Thus, potentially everyone of us is an innovator in ways that matter to human conflict and human security.

Emerging Issues: Anticipating the Truly Disruptive Potential of Technology

In the wide landscape of possible futures, there are many potential emerging issues that could play key roles in shaping the character of irregular warfare. The following are a select few, each of which is driven strongly by technology and, should they mature to become part of a new normal in the future, will have deep implications for irregular warfare and for the challenges (and opportunities) facing SOF.

Mechanized Warlords

Given the current pace of development in robotics and machine intelligence, and given how quickly automation is expanding across all functions in society, the possibility exists for one person being able to assemble and command a veritable army of machines. Anticipating that the cost for computing power continues to fall, and that related technologies such as digital fabrication continue to advance rapidly, we expect to see instances of small groups—even individuals—able to assemble considerable machine forces. One-person armies composed of networks of air, ground, and sea systems; layers of machine intelligences that specify, collect, and analyze data; and customized programs that help plan, offer counsel, and provide management assistance will comprise these armies. Add the ability for machines to create machines, en masse, and one can anticipate terribly complicated and prolonged conflicts.

Armchair Campaigns

Today, in the span of just a few hours to a few days, a person can go online to register a new company, crowdsource start-up funding, outsource product design, contract for marketing and communications, set up automation to engage with prospective customers and provide customer service, locate and secure offshore manufacturing, and handle shipping and payments. In the preinternet era, this would have taken weeks to months. In a similar vein, and drawing upon many of the same types of online platforms, it is easy to see how future actors, availing themselves of even greater degrees of automation, machine intelligence, and a worldwide IoT will be able to design, organize, launch, and manage a variety of irregular operations quickly and anonymously. Such campaigns would not be the one-off attacks traditionally planned by lone-wolf extremists; these would represent sophisticated and prolonged efforts to undermine governments (and companies), assist insurgents, and destabilize communities.

Objects of Hostile Intent

The IoT is rapidly becoming a pervasive reality across much of the world. As more and more of the built environment is connected to these networks, and as future objects and built structures are designed *for* these systems, the time will soon come when we must see the built environment—the buildings and everyday objects around us—as interactive and as alive as the natural environment. It will no longer

serve to assume that the structures we move through and the objects we move past are either inert or dumb. They will comprise entire ecosystems that will detect, assess, and respond to us. Some of this behavior will be intentional and controlled by adversaries and some of it will be the unexpected and unpredictable *emergent behavior* of complex systems of systems. Thus, warfighters will have to understand and account for the natural terrain, the human terrain, and the machine terrain as well as how they overlap and interact. In a world managed via artificial intelligence (AI) and with abundant biometric data a given, no one will be able to move invisibly or unopposed through a built environment.

Biosynthetic Ecosystems

Synthetic biology is a rapidly developing field that promises to enable us to modify living things radically at the genetic level, and even to engineer entirely novel life-forms. Already, scientists can modify the structure of plants to act as sensors for specific conditions, while other researchers and even amateur experimenters have been working on creating chimera species of animals. With continued advances in these areas, and coupling the capability to engineer biology with other future developments in areas like soft and hybrid robotics, we anticipate the ability of future actors to design and deploy entire ecosystems composed of engineered life-forms and hybrid machine systems. Thus, capable actors could create entire forests or underwater spaces as living ISR and defensive ecosystems, evolving and perpetuating themselves with little to no human maintenance. Since scientists can also now cross the germ line with genetic changes, such biosynthetic ecosystems could easily take on a life of their own, for good and ill.

Immortal Leadership

Today, companies offer to deploy machine learning on an individual's social media postings, personal stories, and memories (recounted) to develop an intelligent avatar that can continue to post messages and interact with other people after the individual dies.[6] In the future, companies will be able to draw on the massive amounts of data generated by individuals over a lifetime in an intensely digital society to create interactive—and even adaptive—simulacra that can communicate with the world forever. The simulacra of revered leaders and devout martyrs alike can continue to actively inspire, denounce, and pronounce long after they have passed away. Thus, individuals will be able to continue to provide guidance and their wisdom can even evolve along with a changing world. Therefore, we anticipate digital avatars created through machine learning will be able to impersonate individuals across social media in perpetuity.

Other Notable Emerging Issues

The previous five paragraphs examine only some examples of an ever-growing list of potential emerging issues being driven by rapid advances in multiple lines of

technological development. When we contemplate the futures of irregular warfare, we need to consider critically the many ways in which technology is going to upend assumptions about society and conflict. The following are other notable examples of additional emerging issues:

- **Smart Feral Cities:** urban areas ungoverned by a state but suffused with smart city technologies and connectivity, providing nonstate actors with dramatic new possibilities for governance, control, and combat.
- **Conflict-in-a-Box:** modularized technologies such as digital fabrication, robotics, distributed energy production, synthetic biology, and AI will enable endlessly customizable packages of conflict tools and resources.
- **Nation-Sourcing:** the twenty-first century levy en masse, a disruptive combination of digital fabrication and universal coding skills; this represents the possibility of every household able to become a factory or cyber node instantly.
- **Involuntary Militia:** as civilian populations and infrastructure are increasingly targeted, personal digital entourages for self-defense will necessarily engage in defense and counterinformation operations. This will further blur the lines between civilian and combatant, creating engaged civil combatants.
- **AI Irregular and Mercenary Forces:** as machines continue their rapid (and directed) evolution, they will be deployed increasingly in semiautonomous and autonomous defensive and offensive roles across human conflict.
- **Chimeric Pandemic:** the possibility of chimera creatures developed by irresponsible actors using advanced and easy-to-use genetic engineering tools escaping into the world, posing both direct physical threats as well as threats to existing habitats and ecosystems.

SOF Leadership: Looking Forward, Not Backward

Senior leaders reach their positions because of their skills, perspectives, and unique ways of getting things done. It is, therefore, inherently difficult to ask them to question—and potentially abandon—some of the assumptions and understandings that have served them well previously. Yet, given the trends and emerging issues we have discussed, that is exactly what leaders need to do. To do anything else would be to ignore or, at worse, deny the challenges (and opportunities) we see emerging in the world around us.

The future (multiple) operating environments into which we will send operators will reward teams selected and prepared for those environments. The SOF operators we will need in 2030 will not be those we deployed in 2005. As much as the counterterrorism teams deployed in 2005 were arguably the best trained and

equipped on the planet, how could those same teams with their same equipment and support platforms perform against adversaries fielding biosynthetic ecosystems surrounding hostile-built environments and who are continually inspired by their most revered (and now virtual) immortal leaders?

As we contemplate the challenges of the 2020s and beyond, we must question key assumptions about the special operations forces. In ten years, what should a US Army Ranger look like? What will make an effective SEAL? When we think about operations in the future, like stacking at the door, we have to start asking, what is the "stack" and what is the "door" of the future? In fact, in getting to the X and getting off the X, we have to ask, "what exactly might the X be?" In the future environments we now contemplate, we seem likely to need more than just brute force to achieve our objectives and keep our operators safe.

As we begin questioning our assumptions, we also must revisit the SOF Truths. Some of these core tenets might need to be redefined for the coming era. And then again, perhaps not. People remain more important than hardware, and yet the emphasis might now be on recruiting and developing the right people. We have insisted that we cannot mass produce SOF, and yet we see humans teaching machines that then teach humans. Where might such developments go for SOF in the years ahead? This reflection is neither simple nor easy, and yet it is critically important as the world changes rapidly.

Endnotes

1 United States Department of Defense. *Irregular Warfare: Countering Irregular Threats Joint Operating Concept,* 2.0, May 17, 2010.

2 Vision Foresight Strategy LLC., 2016

3 Internal Displacement Monitoring Centre. 2019. "GRID 2019, Global Report on Internal Displacement." May 10, 2019. http://www.internal-displacement.org/sites/default/files/publications/documents/2019-IDMC-GRID.pdf.

4 World Economic Forum. 2016. "This is What the Internet Looked Like When It Was First Invented." https://www.weforum.org/agenda/2016/04/this-is-what-the-internet-looked-like-when-it-was-first-invented; NCTA. "Internet of Things." https://www.ncta.com/positions/internet-of-things; Patrizio, Andy. 2018. "IDC: Expect 175 zettabytes of data worldwide by 2025." Networkworld. https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html; Reinsel, David, John Gantz, and John Rydning. 2018. "The Digitization of the World from Edge to Core." IDC. https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

5 The startups.com platform. "The History of Crowdfunding." https://www.fundable.com/crowdfunding101/history-of-crowdfunding; Massolution. 2015. "2015CF: The Crowdfunding Industry Report." http://www.smv.gob.pe/Biblioteca/temp/catalogacion/C8789.pdf; Barnett, Chance. 2015. "Trends Show Crowdfunding to Surpass VC in 2016." Forbes. https://www.forbes.com/sites/chancebarnett/2015/06/09/trends-show-crowdfunding-to-surpass-vc-in-2016/#171732da4547; CFX Alternative Trading. No longer available. https://cfxtrading.com/research/10-equity-crowdfunding-statistics-that-should-have-your-attention-infographic.

6 *MIT Technology Review*. 2018. "Digital immortality: How your life's data means a version of you could live forever." https://www.technologyreview.com/2018/10/18/139457/digital-version-after-death/.

CHAPTER 31

Intelligence for Special Operations Forces

John Tullius

Until fairly recently, US HUMINT collectors have maintained a decisive technological advantage over foreign services, augmenting virtually every facet of conducting clandestine operations. However, the global diffusion of technologies—social media, biometrics, closed-circuit television (CCTV), artificial intelligence (AI) and machine learning (ML), and others—has significantly complicated efforts to develop credible cover stories, travel in alias abroad, and meet clandestinely with assets and communicate with them remotely. To redress these issues, and accelerate the adoption of operationally relevant capabilities, virtually every intelligence community (IC) and Department of Defense (DOD) component has established "innovation" centers in Silicon Valley and other technology corridors. While this is a necessary step, these centers have largely failed to fulfill the promise of delivering capabilities to operators rapidly for a variety of reasons. This chapter delves into these issues, providing some thoughts on how to mitigate them.

HUMINT's Critical Role, Sensitivities, and Tradecraft Considerations

While many government agencies conduct human intelligence (HUMINT) overtly, this chapter focuses on the IC and DOD's clandestine efforts to develop and recruit human sources, or "assets," based on the inherent sensitivity of these operations and potential compromise via technological means. Additionally, this form of HUMINT is essential because it is the only "Int" that can provide insight into an adversary's plans and intentions.[1] For example, media reports on the alleged Kremlin insider who provided information on Vladimir Putin's intentions to meddle with the US elections, and his motivations for doing so, illustrate the utility, and extreme risks, of running such sources.[2]

This type of granular insight on a foreign leader's intentions is almost certainly something that none of the other collection platforms—signals, geospatial, and open-source intelligence—can provide. Most often, information derived from these disciplines can provide early indicators and warnings, or address critical information gaps, but they almost always lack the precision and context that HUMINT affords. For example, imagery of an adversary's tanks massing along a border are merely a picture that could have many interpretations; e.g., is it just a training exercise or an imminent attack across the border? Similarly, signals intelligence (SIGINT) reports often tend to be fragmented and ambiguous, rarely containing the thoughts and intentions of foreign leaders given the heightened security practices employed by most adversaries. And while open sources can provide a high percentage of the low-hanging fruit, enhance situational awareness, and provide leads for other collectors, adversaries are not going to openly highlight their plans and intentions on the most sensitive issues.

Consequently, information derived from clandestine sources remains essential to addressing the most critical intelligence gaps, but since espionage is a treasonous act punishable by death or lengthy prison terms, it also entails some of the greatest risks to both the case officer and the source. Operational compromises inevitably will have tragic results, while also hindering efforts to develop and recruit new sources. HUMINT collectors, therefore, are neuralgic about preserving "sources and methods," taking every measure to protect sources' identities.[3]

HUMINT collectors are trained to use sound tradecraft (or TTPs) to protect their sources, which refers to the methods used to operate securely. This includes every facet of operations, from establishing cover identities (masking a case officer's true work affiliation with a more benign assignment like "State" or some other entity), traveling in alias (using fake names and corresponding travel documents), and meeting clandestinely and communicating securely with assets, as well as transferring sensitive information.[4] Every detail of the operational plan is carefully scrutinized to determine risks of compromise by a foreign government service, including the surveillance detection routes (SDRs) and safe houses to conduct meetings, types of covert communications devices utilized, and means for passing information.

Technology Diffusion and Its Potential Impact on HUMINT Operations

Until fairly recently, US HUMINT collectors have employed a range of technological gadgets to enable virtually every facet of their operations, providing significant advantages over other foreign services. However, a number of our near peer adversaries, and even much less technologically astute countries, are utilizing a variety of capabilities, most often readily available commercially, that are hindering efforts to conduct clandestine operations. Ironically, many of these technologies have been deployed since the 9/11 attacks, with US backing, to enhance border security and public monitoring.

The cumulative impact of this technological diffusion has created significant challenges for clandestine operators, and a number of authors have rightly flagged the potential impact on virtually every facet of conducting an operational activity, starting with the ability to create effective cover stories for case officers.[5] The availability of online information, facial-recognition software, and rapidly advancing computing capabilities have made establishing credible cover stories extremely difficult. As Edward Lucas rightly notes, "a cover identity that would have been almost bullet proof 20 years ago can now be unraveled in a few minutes."[6] Similarly, former CIA directors John Brennen and Mike Pompeo have commented publicly on the challenges of trying to match agency officers' digital history with their cover stories.[7]

Even if a credible cover is established, the diffusion of biometrics globally complicates HUMINT collectors' efforts to travel in alias and reenter countries using different identities. International travelers, even to developing regions, are most often greeted by visa officials armed with a range of identifying biometric capabilities, such as digital fingerprinting, retinal scans, and facial recognition. These countries also

have much greater computer-programming capabilities than they did even five years ago, enabling them to store and analyze such data to discern potential threats and traveler anomalies. As Kate Brannen notes, "gone are the days of entering a country with a false passport and wearing a wig."[8] Thus, once this data is collected, a HUMINT operator may experience difficulties reentering a given country in true name or under a different alias, even when equipped with legitimate-looking travel documents.[9]

Once HUMINT collectors are in country, their movements can be tracked readily with the ubiquitous CCTV monitors found in virtually every international city, hampering efforts to go "black" (evading foreign surveillance) and safely conduct clandestine meetings with sources. As an operator begins an SDR, their movements—as well as the sources'—presumably can be fairly easily tracked by foreign services. This omnipresent camera monitoring also complicates efforts to meet at designated safe houses, conduct brush passes on the street, and pass information at "dead drops." All of this is further compounded by capabilities that enable services to track cell-phone patterns and use sophisticated software programs to determine movement patterns and correlate that with other cell phones of interest.[10] It is also a safe bet that many countries have, or soon will acquire, sophisticated drones to augment their surveillance capabilities.

Looking ahead, rapidly advancing 5G and AI/ML capabilities undoubtedly will unleash new capabilities that will exacerbate these operational challenges.[11] China, for example, is working on sophisticated crowd-control algorithms that will complicate HUMINT operators' ability to move freely.[12] As Lucas notes, "the same algorithmic techniques that digital security experts use to spot malware on networks and computers can easily be tweaked to highlight other unusual behavior—sometimes much more effectively than human analysts could do."[13]

Finally, to minimize the risks of face-to-face meetings with assets, HUMINT operators often rely on covert communication (CovCom) devices to communicate securely and pass information. The security of these systems is paramount because any breaches undoubtedly will compromise the source, and potentially other sources using the same system. But what if we are up against a technically savvy service that can potentially hack these systems? Increasingly, that may be the reality in many countries, as foreign services quickly adopt new capabilities to identify and decrypt CovCom systems.

Some Concrete Examples

These potential impacts are not just theoretical concerns; a growing body of evidence indicates such technological advances are already complicating significantly efforts to conduct sensitive operations, not just for the United States but for other countries as well. Most likely, the publicly available examples captured in this chapter comprise only a subset of additional cases that remain unacknowledged.

Most troubling, a number of recent press reports suggest US operators have a significant CovCom problem, which may already be complicating efforts to interact

clandestinely with remote assets. For example, press reports allege, sometime around 2010, the Russians effectively hacked communications systems in use by the FBI's counterintelligence surveillance teams operating domestically.[14] Similarly, other press reports allege, from about 2009 to 2013, the Chinese government cracked CIA's internet-based CovCom system, resulting in the imprisonment and execution of many sources.[15]

Other technical advances are also impacting US operations. For example, following the CIA's alleged 2003 rendition of Hassan Mustafa Osama Nasr off the streets in Milan, Italian authorities reportedly used a version of Analyst Notebook to correlate cell-phone metadata to identify, and convict in absentia, nearly two dozen CIA officers.[16] In 2018, a criminal group reportedly used drones to disrupt an FBI operation,[17] an event FBI deputy assistant director Scott Brunner seems to allude to in his 2018 Statement for the Record to the Senate.[18]

There are also a number of reports of other countries' operations getting compromised through technological means. In 2009, following the Mossad's alleged assassination of Hamas leader Mahmoud al-Mabhouh in Dubai, UAE authorities apparently used a variety of means, including cell-phone tracking and CCTV coverage, to identify the suspected Israeli operators.[19] Similarly, British investigators reportedly used CCTV to identify Russian agents suspected of poisoning Sergai Skripal and his daughter with a Novichok agent in 2018.[20] In Syria, insurgent groups have repeatedly attacked Russian troops with armed drones, reportedly incorporating swarm tactics to increase potential lethality.[21]

Ongoing Efforts to "High Tech" Our Way out of the Problem

The growing realization that we are losing our technological edge has led to a proliferation of IC and DOD "innovation centers," the flavor du jour for engaging with high-tech industries to accelerate technology adoption and develop operationally relevant capabilities more rapidly. The purpose is not to provide a list of these entities, although a quick internet search reveals that most IC and DOD commands have established innovation outposts in Silicon Valley and other technology hubs. Most of these organizations have been established as nonprofits aligned with their respective DOD or IC patron, and they incorporate a variety of operational models. Some of them operate using a venture capital model to identify promising companies and provide seed funding for operationally relevant work, whereas others actively seek mature capabilities that can be immediately procured.

These innovation centers offer, potentially, myriad advantages to expedite the discovery and transfer of operationally relevant technologies.[22] Foremost, as nonprofits, they have more flexibility than government to engage with industry because they are not encumbered by federal rules that hinder effective engagements and quick contracting actions. For example, they have the ability to hire experts and let contracts expeditiously, while also enhancing opportunities to get promising technologies to market, and in the hands of operators, much more quickly.

This approach also allows DOD-affiliated nonprofits to hire business-savvy managers, who have a better understanding of IT companies, their challenges as start-ups, and their more immediate needs to meet margins. Suffice to say, most federal procurement offices, more accustomed to dealing with the much smaller subset of larger, well-established contractors, likely have only a vague notion of how to work constructively with start-ups.

Since most of these smaller IT companies lack experience working with the federal government, the nonprofits can play an essential role helping companies better understand federal contracting practices and setting expectations. Most important, given their connections to government entities, their experience with federal procurement processes, and understanding of the market, these nonprofits can play a vital mentoring role to help companies traverse the "Valley of Death." They can also play a critical role helping companies identify dual-use applications for their products, providing opportunities for other revenue streams and provide greater incentives for working with the government.

But Are They Delivering?

While these innovation centers have great potential, anecdotal evidence based on discussions with experts working in this domain suggests that, at best, they are having mixed results. To be fair, most have been established within the last five years or so, and so they may need additional time to germinate. However, a number of common factors seem to be limiting the impact of the innovation centers: insufficient requirements, sporadic feedback to companies during product development, and suboptimal user inputs throughout the product lifecycle.

Additionally, even when these centers identify useful applications, they often need to find potential end users within their communities. Another, potentially bigger, pitfall: once a user group is identified, the actual contracting may need to be handled through established acquisition offices that may not be nimble enough to manage the transfer rapidly. Some of this stems from institutional biases toward big projects and finding "enterprise-wide" solutions or big-ticket projects that will become programs of record. Or, contracting offices may be encumbered with time-consuming, ossified contracting rules that preclude quick procurements.

Fixing the Problem: New Business Models for the IC and DOD

The foregoing suggests innovation centers are a necessary but not sufficient solution and that we need to adopt a more agile approach that fosters more flexible acquisition practices. While most IC and DOD seniors echo these sentiments, and voice support for closer integration with industry, scant attention seems to be paid to finding solutions for optimizing the innovation centers' effectiveness. Below, I offer a few thoughts on this.

Foremost, DOD and IC entities need to ensure the "backend" processes are equipped to match the innovation centers and their industry partners' need for speed

and agility because many companies, especially smaller start-ups, will not have the patience to wait endlessly for project approvals. Potential gatekeepers that can significantly impede progress include technology-transfer offices, contracting officers, comptrollers, and legal departments. In my experience, many of these staff officers are long-tenured and often lack the basic understanding of new DOD and IC business models, requiring a crash learning course for them, or a changing of the guard.

We also need to jettison the inclination to seek enterprise-wide solutions or big program-of-record initiatives, as these usually are too slow and cumbersome. As a personal example, I managed open-source collection efforts for Europe and the Middle East from 2011 to 2016 during the height of the Arab Spring, the migration of foreign fighters to the region, and the emergence of ISIS. All these issues had a large social media component, requiring automated exploitation and analytic tools. However, as of 2016, these capabilities had not materialized for overseas use, resulting in our officers having to review, compile, and analyze relevant content manually.

These delays stemmed from myriad management and cultural issues, including having former National Reconnaissance Office managers overseeing these development efforts, who were accustomed to developing expensive satellites that took years to deliver, with zero risk tolerance. This approach, however, was anathema to the rapid adoption of the capabilities my unit required. Ultimately, we required a "fail fast" mentality that let us explore many tools, accepting that if only one out of 20 was deemed viable, this would be a success. Although we identified potential applications in the host country, we were not allowed to procure and test them, even in a "sandbox" that was not connected to our servers. Moreover, even though my staff identified software engineers who could automate some of our work, we were prohibited from developing tools in the field.

On a related note, we also need to recognize efforts to find one-size-fits-all solutions are self-defeating because we should never expect to use the same gadgets across all of our operational environments. The alleged Chinese hacking of the CIA's CovCom system illustrates this point. The breach reportedly occurred when operators used a system designed for much more permissive environments in a country that was much more technologically savvy.[23] This example indicates strongly the need to tailor our approach carefully to the prevailing threat level, with more flexible options to meet the operational requirement. In some places, a 60 percent solution that can be traded out quickly for other systems may suffice, whereas in others, we will need more robust capabilities.

Perhaps most important, the successful development of new capabilities requires extensive operator inputs throughout the entire development cycle, starting with clear requirements and regular feedback during the development and testing phases to enhance product viability. If companies take a year to develop a new capability without sufficient user inputs, the odds grow longer for a successful outcome. Conversely, having an operator iterate throughout the process can provide invaluable insights on whether the product is too heavy, not user friendly, lights them up too much at night,

or whatever the case may be. As a corollary, we need to enable field units to identify, test, and develop tools, rather than relying solely on headquarters-designed solutions that may miss the mark.

What about Going Low-Tech: Back to the Future?

The ongoing rush to better integrate with industry seems to presume the IC and DOD will be able to regain our decisive technological edge; however, even with significant improvements, we might not ever widen that gap substantially with our adversaries. China, for example, is reaping years of state planning and investment in IT companies: as of 2013, only two Chinese firms ranked in the top 20 globally, but within five years, the number had increased to 9.[24] Similarly, other countries have fostered competitive IT companies that are vying for market share. Additionally, even for countries that lack a strong IT base, the commercial availability and relatively cheap cost of many of these capabilities virtually ensures they will be readily employed and continue to challenge HUMINT collectors.

Consequently, we may need to accept these operational realities as our new normal and rethink our reliance on, and perhaps complacency with, seeking the holy grail of technology superiority. Ultimately, we need to reevaluate our tradecraft and TTPs, perhaps adopting old-school espionage practices that obviate the need for high-tech solutions or seeking hybrid solutions tailored specifically to the operational environment.[25] While these old-school practices may be more exacting and time consuming, we may not have many other great options to maintain our ability to collect HUMINT on our highest-priority national security issues. As such, it is paramount for HUMINT collectors to identify creative new solutions to meet these challenges.

Endnotes

1 See Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 143, for a discussion on HUMINT's intrinsic value at discerning plans and intentions, and comparisons with other forms of collection; Mark Pomerleau, "Is Technology a Threat to Human Intelligence? C4ISRNET, August25, 2017, 6; Caesar Kalinowski IV, "HUMINT Isn't Dead, It Just Smells That Way. Time for Us to Learn from the Past," Taskandpurpose.com, October 2, 2018.
2 Julian E. Barnes, Adam Goldman, and David E. Sanger, "CIA Informant Extracted From Russia Had Sent Secrets to US for Decades," New York Times, September , 2019; and Jim Sciutto, "Exclusive: US Extracted Top Spy From Inside Russia in 2017," CNN, September 9, 2019.
3 Lowenthal, *Intelligence: From Secrets to Policy*, 144.
4 IBID, 138-139. See also Jack Murphy, "How Technology is Changing the Future of Espionage," SOFREP, March 30, 2015.
5 See, for example, Lowenthal, *Intelligence: From Secrets to Policy*, 140; Murphy, "How Technology Is Changing the Future of Espionage;" Jeff Stein, "CIA's Secret Fear: High-Tech Border Checks Will Blow Spies' Cover," Wired.com, April 12, 2012; Edward Lucas, "The Spycraft Revolution," Foreign Policy, April 27, 2019; John Sano, "The Changing Shape of HUMINT," Intelligence Journal of US Intelligence Studies, Fall/Winter 2015; Kate Brannen, "To Catch a Spy," Foreign Policy.com, April 6, 2015.
6 Lucas, Edward, "The Spycraft Revolution," 3.
7 Pomerleau, "Is Technology a Threat to Human Intelligence?" 7-8.
8 Brannen, "To Catch a Spy," 1.
9 Stein, "CIA's Secret Fear: High-Tech Border Checks Will Blow Spies' Cover," 2-8; see also Murphy, "How Technology is Changing the Future of Espionage," 3-4.
10 Lucas, "The Spycraft Revolution," 4-5; Murphy, "How Technology is Changing the Future of Espionage," 2.
11 James Vincent, "Artificial Intelligence Is Going to Supercharge Surveillance," The Verge, January 23, 2018; Richard Harrison, "The Promise and Peril of 5G," The National Interest, March 21, 2019.
12 See, for example, Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame, and Lots of Cameras," The New York Times, July 8, 2018; Simon Denyer, "China's Watchful Eye," The Washington Post, January 7, 2018; and Anna Mitchell and Larry Diamond, "China's Surveillance State Should Scare Everyone," The Atlantic, February 2, 2018.
13 Lucas, "The Spycraft Revolution," 9.
14 Zach Dorfman, Jenna McLaughlin, and Sean D. Naylor, "Russia Carried Out a 'Stunning' Breach of FBI Communications System, Escalating the Spy Game on US Soil," Huffington Post, September 16, 2019.
15 Mark Mazzetti, et al., "Killing CIA Informants, China Crippled US Spy Operations," New York Times, May 20, 2017; Zach Dorfman, "Botched CIA Communications System Helped Blow Cover of Chinese Agents," Foreign Policy, August 15 2018; and Jenna McLaughlin and Zach Dorfman, "At the CIA, A Fix to Communications System That Left a Trail of Dead Agents Remains Elusive," US News, December 6, 2018.
16 Murphy, "How Technology is Changing the Future of Espionage," 2.
17 Jason Murdock, "'Drone Swarm' Used by Criminals to Disrupt an FBI Hostage Rescue Operation," Newsweek.com, May 4, 2018.
18 Scott Brunner, Deputy Assistant Director, Critical Incident Response Group FBI, Statement Before the Senate Homeland Security and Governmental Affairs Committee, June 6, 2018.
19 Yossi Melman and Dan Raviv, "Israel's Hit Squads," the Atlantic.com, February 2010; Paul Lewis, Julian Borger, and Rory McCarthy, "Dubai Murder: Fake Identities, Disguised Faces, and a Clinical Assassination," The Guardian, February 16, 2010.
20 BBC.com, "Russian Spy Poisoning: What We Know So Far," October 8, 2018 (https://www.bbc.com/news/uk-43315636).
21 Dmitry Kozlov and Sergei Grits, "Russia Says Drone Attacks on its Syria Base Have Increased," APnews.com, August 16, 2018; David Reid, "A Swarm of Armed Drones Attacked a Russian Military Base in Syria," CNBC.com, January 11, 2018.
22 For an excellent discussion of one model, the Partnership Intermediary Model, and the potential benefits of establishing DOD nonprofits, see W.D. Swearingen and J. Dennis, "US Department of Defense Technology Transfer: the Partnership Intermediary Model," the International Journal Technology Transfer and Commercialization, Vol.8/ Mps 2/3 2009. More generally, the myriad advantages discussed here are applicable to other DOD nonprofit entities.
23 Dorfman, "Botched CIA Communications System Helped Blow Cover of Chinese Agents," 1.
24 Sally French, "China Has 9 of the World's 20 Biggest Tech Companies," Market Watch, May 31, 2018; Mary Meeker, "China Now Has Nine of the World's Biggest Internet Companies—Almost as Many as the US," Vox.com, May 30, 2019.
25 For similar arguments, see Sano, "The Changing Shape of HUMINT," 78-79 and Kalinowski, "HUMINT Isn't Dead, It Just Smells That Way. Time for Us to Learn from the Past."

CHAPTER 32

Systems-of-Systems: Coping with Pervasive Technology in Operating Areas

Mark W. Maier and LTC Edwin Churchill

In this chapter, we define systems-of-systems (SoS), consider their role in special-operations missions, and speculate about how the future special operator will need to regard an environment that contains not only systems designed to either benefit or threaten, but also systems designed and operated for other purposes entirely that may be used in the SOF environment.

Introduction: An Environment of Systems-of-Systems

In 2018, in a curious case of genetic forensics, police in California had DNA samples from a serial rapist and murderer, identified as the Golden State Killer and known to have committed numerous crimes in the 1970s and 1980s. The cases were cold. The DNA profile appeared in no database, preventing identification of a suspect. An investigator thought to look at the growing databases of DNA data, largely crowdsourced and built significantly by genealogy hobbyists, from people tracking their ethnic and family origins. The DNA sample did not appear in any of these databases, but samples with sufficient match to indicate possible family relationships did. A team of law enforcement officers and private genealogists built large family trees from DNA and other public genealogy databases, then crossed that information with other evidence to narrow a list of possible suspects, eventually to a single person. The individual's DNA was obtained clandestinely by law enforcement and was a solid match. Law enforcement arrested and charged the individual with the crimes.[1]

The technique used in the Golden State Killer investigation has been used subsequently to solve numerous cold cases. From one perspective, this story shows how new technology enables a significant new capability. More interesting, however, is that 1) none of the component technologies used by investigators were intended for tracking criminal suspects and 2) the government did not own or operate most of the component systems. Investigators cracked the case by assembling independently owned and operated parts. The "system" that identified the subject emerged from the interaction of many systems. Nobody built the system that tracked the Golden State Killer; rather, it emerged from the interaction of systems built and operated for other purposes. This is a "system-of-systems" in operation.[2]

New technology has changed, and will continue to change, special operations environments. From small drones to miniaturized sensors, smart medical devices, satellite navigation, and countless other inventions, the special operator has myriad new tools to use but also faces threats from such tools. SoS will not be confined to the developed world; indeed, they might be more common in the developing world. Some of the most striking examples of SoS enabled capabilities are emerging in West

Africa. In Ghana, there is a widely deployed smartphone app that allows ambulances to navigate to the location of a smartphone that has made an emergency call with 25 centimeters accuracy, more accurate than available in most developed countries. Elsewhere in West Africa, there are many innovative medical systems that combine cell phones, apps, and logistics based on local resources, such as motorcycles, to deliver perishable resources, such as blood, reliably, despite difficult local travel conditions.[3]

Emergent SoS and their capabilities will be important to special operators (whether in the developed or developing world), as risks, threats, opportunities, and targets or as resources to defend. Unlike traditional systems, SoS will not have clear ownership or control. No central authority will exist to collaborate with, attack, or defend. Because no central authority owns or controls SoS, governments and militaries can build SoS using components owned and operated by others. Threats may appear by surprise; people or groups may be able to string together capabilities to accomplish something unexpected. Operatives may be able to leverage large investments by others to produce unexpectedly dangerous capabilities. It may be difficult to attack the underlying component systems because they may be part of local infrastructure, perhaps even part of US infrastructure.

What Is a System-of-Systems?

Most people understand a "system" to be a collection of components that jointly exhibit functions not possessed by any of the components. A transistor does not provide computational function. However, a collection of transistors forming a computer processor provides rich computational functions. Typically, a "system" has an owner and/or operator. Somebody specified the system, had it built and deployed, and operates it to gain desired capabilities. The system might be complicated with a great many components and interactions, but it has well-defined ownership and operational authority, and that authority manages the system for well-defined purposes. Military systems usually fall into this category, unless the acquirers have deliberately chosen to spin out control, partially or completely, to others to accomplish a higher-order goal.

As defined in "Architecting Principles for Systems-of-Systems"[4] and elaborated in subsequent literature by Sage and Cuppan and Sage and Biemer,[5] among many others, a "Collaborative System" or "System-of-Systems" is a collection of systems with three key features:

1. The systems interact with each other to produce results none of them can achieve alone. Jointly, the parts form their own system.

2. The SoS continues to fulfill useful purposes on its own (operational independence of the elements) even if a member is disconnected from the collective.

3. While interconnected, the constituent systems continue to be managed for their own purposes independently of the collective, at least in part (managerial independence of the elements).

An Alternative Perspective: China's Concept of "System Confrontation"

This chapter concentrates on how infrastructural systems not specifically owned and operated by militaries may be used as either threats against or opportunities for the SOF operator. From a broader perspective, a body of Chinese writing exists that describes military conflict as a confrontation of systems.[6] The writing discusses moving away from seeing military conflict as confrontations between specific platforms—for example, one aircraft type versus another, or a missile type versus a ship—and, instead, examining the confrontation in terms of larger targeting, strike, and countermeasure systems comprising aircraft, ships, missiles, sensors, and other components. During a large-scale, peer-to-peer military conflict, the SOF operator constitutes a component of reconnaissance and strike systems. We take this up in the discussions of unconventional and special reconnaissance missions and how different modalities may be enabled, or disabled, by the presence of the system-of-system environment.

Even when considering nation-state systems, one should notice most nations make wide use of commercial communications and computing infrastructure even for national security missions. The United States has long utilized its civilian communications infrastructure as part of important military systems.[7] Other nations do also, a fact sometimes exposed by outsiders.[8] So, the focus of this chapter on the exploitation of nonmilitary infrastructure as part of a SoS has a considerable history.

Why Now for Systems-of-Systems?

The SoS concept is not new; it has been part of the general environment for at least a century. Both transportation networks (such as railroads) and power networks are systems-of-systems. The most relevant systems-of-systems militarily are Command, Control, Communications, Computing, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems. These systems allow coordination among distributed forces, find and track opposition forces, and allow precision direct and indirect fires. Historically, C4ISR systems have been built, deployed, and operated by militaries as dedicated military systems. This is no longer the case, and it is likely to be less and less the case in the future (especially in special operations environments) because key building blocks for C4ISR systems are increasingly present in operating areas without being placed there by militaries. Pervasive digital communications systems, distributed computing, and sensing systems are now commonly present regardless of military deployment or presence.

Not many years ago, only nation-states would have satellite communication, space surveillance, and drones. Today, even a modestly funded nonstate group may have all the above. Some nonstate actors are figuring out how to integrate these technologies

and use them in innovative ways, a potentially dangerous development for the SOF operator. It could also provide new opportunities for exploitation, attack, and co-option.

Operating in the SoS Environment

The ancestor of today's SOF operator likely operated in an austere or "barren" environment with limited communications, power, and monitoring coverage. From World War II to the War in Afghanistan, SOF have operated in relatively technology-poor environments. The SOF operator's opposition had access only to communications, data, and computing capabilities far below what the operator could use. However, today's operator likely operates in an area blanketed by cell phones, satellite communications, space and other surveillance, and other networks. Operators can use those networks, and those networks can be used against them. If the networks can be used against them, operators may want to attack or co-opt the networks. If those networks are not attacked, the gap between the data and computing services the operator can access and those accessible to the opponent will have shrunk dramatically. Attacking the networks may have far-reaching consequences beyond the immediate battlespace.

To get a sense of the scope of global deployment of the building blocks for systems-of-systems, consider the following:

- As of 2019, approximately two-thirds of the world's population has mobile connectivity.
- Two-thirds of the population without internet access is in range of 3G and 4G mobile services.
- As of 2019, the Iridium satellite system is available globally to mobile devices; Globalstar devices are available to most of the world.
- By 2025, five or more global satellite providers of high-speed internet services to mobile and handheld devices could exist. Not all planned satellite communication networks will fly, but the success of even a fraction will ensure global competitive access. By 2025, other means of providing data service in barren areas, such as long-endurance aircraft or balloons, will likely be in use.
- Ultra-high-speed computing resources (e.g., Amazon or Google cloud services) are available everywhere internet services are available, meaning where most of the world's population lives.
- City and other local governments are increasingly deploying wide-area imagery surveillance networks.
- GPS precision location services are available globally. European and Russian GPS are, or are becoming, available. Chinese and Japanese built systems with regional, and potentially global, services are also coming on line.

- Companies have announced multiple global imaging satellite constellations with resolutions as good as one meter and revisit times as fast as 30 minutes (though deploying both simultaneously as a commercial system is unlikely).

As a result of the spread of the aforementioned technology, few places on the globe are largely "barren" of infrastructural services (at least data and computing infrastructure). Most rural areas will be significantly connected, even if they lack reliable grid power and clean water, and urban areas will be densely connected. Physically, satellite services reach the entire globe, although the limitations of radio propagation in dense jungles and complex terrain mean a few areas remain barren of service. Urban areas and the coastal zones, where most of the world's population lives, will likely be covered by overlapping satellite and terrestrial communications, overlapping location systems, subject to surveillance from multiple types of system, and thickly connected to cloud-computing services. Thus, extensive communications, computing, and surveillance capabilities will soon be in place, a full infrastructure onto which command, control, intelligence, and reconnaissance can be added. Such rich services will not be available in remote areas, but the expansion of satellite (and possibly balloon and aircraft) services will continue to shrink the areas entirely unserved and connect most operating areas significantly.

Emerging Space and Airborne System-of-System Components

Space and airborne (especially drone) components represent among the most important enablers of future systems-of-systems of concern to the SOF operator. Historically, space systems have been the province of governments. For most of the space age the sole exception has been geostationary communication satellites, primarily relevant to large, fixed, ground installations, not mobile operations. In the twenty-first century, the commercial viability of constellations (tens to hundreds of identical satellites) flying in low earth orbit (LEO) and operating together to provide services has ramped up dramatically and is poised to increase even more.

In 2019, three major such constellations—Iridium, Globalstar, and ORBCOMM—operated communications services to mobile terminals (devices from phone to pager size), with many more in various stages of development. As of 2019, companies have written numerous proposals for much larger low earth orbit constellations, mostly numbering in the hundreds of satellites and targeted at delivering high-speed internet services to underserved areas of the globe. In the late 1990s, companies such as Teledesic made similar proposals but never launched the systems. Many of the currently proposed constellations will also never launch, but some almost certainly will. If competing large LEO constellations go into operation, the environment for building distributed systems-of-systems will change radically. Multiple sources will exist for the required fundamental communications infrastructure, and those sources will not be controlled directly by nation-states.

Already, nation-states control multiple deployed positioning-navigation-and-timing (PNT) satellite systems. The best known, the US GPS, is poised to move to third-generation satellites that will provide more accurate and robust service to both civilian and military users. The Russian GLONASS and the European Galileo systems are in operation, albeit not always at full capability. As of 2019, China, Japan, and India operate regional systems. By the early 2020s, the Chinese BeiDou system will have global coverage. Thus, multiple sources of positioning data from space are already available, independent of any terrestrial infrastructure, with more coming.

The increasing internationalization and commercialization of space-based communication and PNT services enhances the SoS environment. If only one nation provided all the services, they would likely become targets in a peer-level conflict.[9] With multiple providers over different nations the situation is more complex. As noted previously, there are three to six PNT systems at various levels of development from nation-states or international consortia. Would a peer-peer conflict lead inevitably to all of them being targeted? A large constellation of wide-bandwidth communication satellites with overlapping antenna footprints has a signal processing structure similar to that of PNT systems. If the clocks on the satellites were synchronized precisely enough, the signal structure could also be used for positioning. It is easy to imagine more heterogeneous solutions for PNT that fuse partial information from commercial satellite systems and local infrastructure that break dependence on government-owned positioning systems.

While satellite communication and navigation services have been available globally and not restricted to government users for some time, the same is not true for remote sensing. Recently, a variety of proposals and deployments for global remote-sensing systems have proliferated. As of 2019, there are commercial systems with imagery capabilities better than 0.5 meters.[10] As an example of what may be available to the system-of-system designer in the near future, the PlanetScope/Skysat systems now in operation (and planned for expansion) provides comprehensive daily coverage with on-demand imaging with submeter resolution.[11]

Threats and Opportunities

This collection of communication and surveillance capabilities will be supplied by a system-of-systems in the classical sense. The components will be independently owned and operated. Some will be supplied by governments (local or foreign). Some will be supplied by corporations, some US-based and some not. Some may be supplied by nongovernmental, noncommercial organizations. Governments will likely have uneven, if any, control over suppliers.

From the SOF operator's perspective, we can think of the impact of the SoS and their components in several different ways. We can organize SoS by threat and opportunity or attack and defense.

- SoS as a threat: An opponent may fuse components into their own system

and use the SoS to threaten the SOF operator. The SOF operator must defend against the threat of a C4ISR and strike system built from the infrastructural components.

- The opportunity to use components as part of the SOF operator's capabilities.
- The need to defend those capabilities against attack. An element of FID may be to defend communication, computing, and surveillance infrastructure when targeted by a threat.
- The need to attack the infrastructure, possibly by nonkinetic means, because it is the target for tactical or strategic direct action.

We discuss each approach at greater length below. They involve building a surveillance-strike system (from other's components), being targeted by such a surveillance-strike system, or countering or disrupting such a constructed system. This needs to be understood in the context of the observe-orient-decide-act (OODA) loop (extensions to which are called "left-of-bang"[i] operations) and the emerging role of machine learning.

The OODA loop might have been articulated clearly and named in the 1970s, but it is far older.[12] Exploiting OODA superiority was as much a key for Subutai in the thirteenth century as it was to German development of "infiltration tactics" in World War I or the command of mechanized forces in Iraq. An information-rich and firepower-heavy expression of this in the late twentieth century was network-centric warfare.[13] Nation-states pursuing these concepts have done so by building dedicated systems that include wide-area secure communications (usually combining satellite-based and other modes), multimodal sensing systems, positioning and locating systems, information fusion and integration (requiring significant computational infrastructure), and integration of fire-control systems. Each component system is a dedicated government system, and the integrating elements are likewise developed by the government using the system.

The history of warfare since 1990 provides extensive lessons both in the effectiveness of such systems and how asymmetric opponents can degrade or avoid the capabilities. SOF operators have played key roles in both the overall network-centric system and attacking opponents net-centric systems (as in the early days of both Iraq conflicts). Most think of the OODA loop in the context of active combat. We observe the tactical environment, orient ourselves to the situation, decide what tactical action to take, and take it. However, if we apply this thinking only when shooting is happening, we are too late. One post-2000 development has been a shift in emphasis from using C4ISR to control lethal force to a more predictive and preemptive "left-of-bang" concept.[14] This concept means using the rich information

i "Left-of-bang" is shorthand for acting before ("to the left") something dangerous/lethal ("the bang") happens.

generated by surveillance of all types, coupled to machine learning and other pattern recognition, to predict, and enable countermeasures against, an attack or other violence. While the left-of-bang concept is different in operation and implementation, the infrastructure that supports it—data generated from many sensors aggregated with powerful computation—is the same.

The proliferation of nongovernmental communications, computing, and surveillance systems means constructing a lethal or nonlethal C4ISR system is no longer the exclusive capability of a nation-state. Nongovernment systems may well be better than government systems. First, since the military has typically built first-generation communications, computing, and surveillance systems, civilian entrants can take advantage of what has been learned in the process. Second, the commercial businesses are willing to throw away systems when they are no longer technically leading edge. The system turnover and technology insertion rate are typically much faster in civilian systems. Civilian actors have built complex information-gathering and -integration applications in health care, supply-chain management, marketing, and other fields. New capabilities enabled by the infrastructure are discovered, such as the criminal genetic forensics that opened this chapter. This is the systems-of-systems world that concerns the future SOF operator.

Being Targeted by the SoS

SOF operators have become concerned with being targeted by lethal network systems that could not have existed only a few years ago. As a historical example, consider the 1993 US operations in Somalia, culminating in the Battle of Mogadishu, made famous by the book and film *Black Hawk Down* (1999, 2001). If Mogadishu had been wired with extensive cellular networks, and if the militias had many wireless enabled video cameras and improvised explosive devices of sophisticated design, how much more hostile could the environment have been for American operators? It is easy to imagine catastrophically more dangerous scenarios in which traditional operations would be untenable. High-capacity cellular networks already exist, and they will be tied increasingly to ground infrastructure (they will be satellite supported and from multiple sources). Miniature surveillance devices, such as cameras, are deployed in many urban areas. Furthermore, the engineering knowledge for improvised explosives and other lethal devices continues to spread, with many new technologies possible. Therefore, the first challenge to consider for the SOF operator is defense against the SoS-enabled opposition capabilities. On the surface, the situation seems grim, but a variety of approaches can be taken, including:

- Not assuming the enemy is better than they are.
- Traditional means: jamming, spoofing, corruption, and destruction.
- Architectural attacks.
- Switch strategies and tactics.

Building Robust Systems Is Hard

Building an effective C4ISR system—one that operates reliably under stress and attack—is difficult. Building it on top of infrastructure you neither own nor control is even harder. Few complex systems work well under stressful conditions unless they have been tested under such conditions, which has historically been a major problem in engineering complex military, especially C4ISR, systems. It is difficult to create realistic test environments for C4ISR systems, especially ones that incorporate the full range of unpredicted opponent actions and countermeasures that will be encountered in real operation. Realistic testing is difficult with nation-state resources; it is nearly impossible for nonstate actors using public infrastructure.

Incompletely tested systems present challenges, such as unreliability, to both the possessor (the user of the system) and anybody seeking to counter it. But the system owner and those challenged by the system might have asymmetric views on the acceptable probability of success. The US military would probably regard as low quality a system with 50-60 percent probability of success. However, to a nonstate actor with different expectations, such a success rate might be acceptable. Nonetheless, an incompletely tested system may be harder to counter than a completed one because its behavior may be unpredictable and there may be limited or no opportunities to collect data on its operation.

The complexity of developing reliable complex systems is related to the issue of how artificial intelligence/machine learning (AI/ML) will play a role in future systems. The AI applications attracting the greatest attention are predominantly ML applications, software systems that learn to perform complex functions, sometimes at superhuman levels of performance, by observation. We can examine the operation of state-of-the-art ML systems that achieve superhuman performance in gaming.[15] Such software is constructed as a neural network that inputs the state of the "game" estimate and predicts (with probabilities) the outcome of the game (who wins, with what probability) coupled to a move generator that generates all legal next moves in the game. The move generator is not a neural network and is not trained; it is built based on game understanding. The combination is used to play many games with moves selected at random (known as Monte Carlo trials), but the random selection adjusts based on the neural network's prediction of likely outcomes (bias toward outcomes in which the player wins). A large body of game play is used to update the neural network predictions, and the process repeats. If the process converges, the neural network will be trained to predict outcomes accurately as a function of game state, and moves will be selected that maximize the probability of winning. In a variety of games, from chess to Go and poker, the process has resulted in programs with superhuman abilities.

The process described above depends on a simulation environment that mimics results in the real world accurately, relatively easy in a case such as chess. The game has a finite number of states; there is a deterministic process for generating moves; and the only potential mismatch between the Monte Carlo play and play against actual

humans is the possibility humans might access playing strategies that cannot be reliably discovered by the self-play search process that trains the neural network. For games such as chess and Go, this is apparently not an issue. However, if we try to apply the same logic to military systems in which the state and the move-generation process are largely unbound, by the time one tests the machine-learning algorithms in the real world, no recourse exists if the real-world differs in some critical detail from the simulated training environment.

Traditional Means: Jamming, Spoofing, Decoys, Corruption, and Destruction

All the traditional means of counter-command and control and counter-ISR are available for a SoS-based threat, with a few twists and with the limitations typical for SOF operations. For an SOF operation, bringing to bear the full set of resources used in a conventional operation would not be possible. Regardless, all the traditional means have some applications.

Jamming: Jamming the components of hostile SoS is an attractive option. First, jamming is nondestructive, so no risk exists of permanently destroying what may be important local infrastructure (unless the jammer is powered to the level of a directed energy weapon). Second, jamming SoS components is likely easier than in a conventional military context. While modern cellular systems do have some interference rejection capability akin to antijam design, no economic case exists to build in protection against deliberate jamming. Strong antijam protection in wireless transmission systems requires extra bandwidth and inefficient modulation, and both are at odds with the need in commercial systems to make the most effective use of expensive bandwidth.

Spoofing: This means inserting decoys or masking the real objects of interest so they appear to be things of noninterest. Using decoys is often an effective, if underrated, technique, especially when coupled to a rapid pace of operations and other techniques (such as jamming or destruction). When parts of the system are inoperative, operators tend to focus on what they can see; if the pace of operations is rapid enough, by the time decoys are recognized for what they are, the opportunity to act may have been lost or resources already expended.

Corruption: C4ISR systems generally rely on some form of information fusion. If the fusion itself can be attacked and corrupted, then the operational picture available to users will be corrupt and the whole system will likely be rendered ineffective.

Destruction: In conventional military operations, one might attack key nodes kinetically. This technique is available for SoS as well, though the targeted infrastructure has many users and its physical destruction may be operationally untenable for that reason. This concern is not new, as demonstrated by the development and use of the graphite-wire "soft bomb" technology as early as the first Gulf War.[16] This device scatters fine wires over an electrical substation to cause extensive short circuits. It brings down electric power in a region, but not permanently and without the actual destruction of infrastructure.

Architectural Attacks: Nonlinear Breakdown

A hostile C4ISR system used against SOF operators must be capable of tracking multiple objects of interest, discriminating between the objects of interest and those not of interest, and doing so sufficiently close to real time to be useful in conducting an operation. Such systems can work effectively when the environment complexity (e.g., number of objects, sensor measurement quality relative to object density) is relatively low; effectiveness can continue to stay high as the environment gets more complex, and then effectiveness can suddenly drop.[17] This phenomenon usually happens when the system or the operators start to associate measurements with objectives incorrectly. That is, a measurement that came from object A is credited to object B (and vice versa). Consider the operation of an air-traffic-control system: Suppose the identity of each airplane cannot be uniquely determined from the sensor return but has to be inferred from its original location or other measurements. When the aircraft density is low, each aircraft can be tracked individually and unambiguously. But, if the density is high enough, tracks will intersect, and identities may be swapped. If this starts happening, the quality of the situational picture will collapse.

More broadly this phenomenon reflects the tendency of users of situational-awareness systems to see what they expect to see and interpret out-of-the-ordinary occurrences in an expected context. This can be exploited by presenting a combination of an operational environment and some combination of spoofing and attack that results in gross misinterpretation of the situation by the C4ISR system's algorithms or by the operators looking at the algorithm results.

Switch Strategies

Finally, the most macrolevel approach to defeating an opposing C4ISR system assembled from infrastructural components is to switch strategies (i.e., use the opponents' resources to gain the information or cause the effect instead of intervening directly). If the environment of concern is rich with communications and sensing resources that another party is repurposing, re-repurpose those resources back at them, preferably remotely, and accomplish the operational aims. This perspective leads us directly to exploiting the opposing SoS instead of attacking it.

Exploiting SoS

SoS that use digital communications, surveillance sensors, and computing infrastructure are both threats to and opportunities for the SOF operator. The SoS is a large infrastructure of important capabilities that does not have to be deployed or maintained but are available for possible use by the SOF operator, nevertheless. Opportunities for the SOF Operator in this regard include:

"Warm Start" and Preparation of the Battlefield: Since infrastructural SoS do not have to be deployed or supported (they are already present), they can contribute to "warm start" and preparation of the battlefield. Both the risks and the burden of exploiting the infrastructure to gather information in advance are low, at least relative

to deploying government-unique systems. Given the importance of avoiding "cold start" for the SOF operator, this is an important opportunity.

Contribution to "Left-of-Bang" Operations: Achieving a "left-of-bang" capability means gathering either large volumes of data from which machine learning and humans can extract nonobvious patterns or acquire exquisite intelligence. A pattern-recognition approach requires large amounts of data, requiring large collection and communication networks and computational resources. Infrastructural SoS in the target's space are the logical sources for this kind of collection.

Future Unconventional Warfare: One of special forces' origin missions is "unconventional warfare," working with indigenous forces to attack or counter an opponent, usually a nation-state. Exploiting foreign SoS would fall under this category. Indigenous infrastructural systems do not have to be transported, installed, or supported. They exist already in the operational areas of interest, and their owners will be loath to turn them off or compromise their operation. The challenges of using them opportunistically include testing and assurance. There will be limited opportunity to experiment and test prior to use. There will not be an easy solution to this, although advanced extensive experimentation with representative non-US components will be important.

Working with or against preexisting SoS provides additional opportunities in unconventional warfare. First, the content of the SoS (e.g., social networks) is itself a battle space. To the extent we pursue hybrid warfare, enabled by SOF, the cyber battlespace will be of high importance. Many key targets will have targetable cyber profiles in the SoS, in which cases cyberattacks may be more effective than physical attacks. Second, in peer-to-peer conflict, the SoS cannot be neglected as a primary target because it comprises and operates so much strategic infrastructure.

Defending the SoS

The third SoS aspect connects to the FID mission. As an example, consider Russia's threat to Ukraine. Part of the conflict is directly military, namely Russia used hybrid warfare tactics[ii] to invade and occupy Crimea and other portions of the Ukraine.[18] But aside from military threats, Russia has engaged in complex attacks on Ukrainian infrastructure, including power networks, telecommunications, and election apparatuses.[19] FID has been thought of as counterinsurgency warfare. But future FID may focus on defending the infrastructure of SoS on which societies depend. Defense of Ukraine against the Russian "insurgency" involves many more aspects than the traditional counterguerrilla aspects.

Readers are already familiar with concept of attacking power networks and telecommunications networks and election systems. Future attacks could include focus on food or public health networks. FID has traditionally focused on counterinsurgency, counterterrorism, and other security and nation-building activities

ii Hybrid warfare does not mean indirect attacks, but direct attacks that target different sorts of infrastructure.

in the face of nonstate threats to nation-state order. In the future, SOF may defend against a nation-state threat, but one in which a nation-state uses hybrid attacks—some directed against the core infrastructure of a nation-state—instead of direct military threats. These future threats are unlikely to be kinetic, since kinetic attacks would be far too obvious. However, nonkinetic attacks are not necessarily less dangerous than kinetic ones.

Attacking an SoS

The SOF direct action mission is to attack high-value targets during times of conflict where those targets require SOF unique capabilities. An SoS in another nation-state might well be such a target and might fall into the SOF direction role in high-intensity warfare and especially to counter anti-access strategies. In some cases, SOF may be the preferred, or even only, alternative. Because of the infrastructural ties of typical SoS, the use of purely kinetic, destructive means may be not preferred. The long-term consequences may be too serious or the escalation risks too great. SOF approaches can more readily include nonkinetic means and more precise control of effects.

Conclusion

For the entire modern era, military and irregular forces have built their own systems and used other infrastructural systems, in many cases owned and operated by others, a phenomenon now referred to as building a system-of-systems. Before the 1990s, C4ISR components were almost exclusively military, while the shared infrastructure was logistical. In the decades since the 1990s, as mobile communications have become ubiquitous and space systems more widely available, SoS has expanded in scope to C4ISR and will certainly accelerate radically in the future. In the past, basic infrastructure such as roads and power extended only partially into developing areas; now, powerful communication, computing, and surveillance systems—often space-based and inherently global—stretch into otherwise remote areas. The continued development of these systems will enable the construction of complex intelligence and strike-support systems.

As with most technology and infrastructure changes, future SoS developments will be both a threat and opportunity, especially to and for SOF operators. First, the world will be increasingly connected through communications and surveillance systems, some areas more so than others. This will change the threats, necessary countermeasures, and opportunities for constructing our own systems. Second, SOF operators will face the problem of attacking versus preserving infrastructure. Third, SoS will open new frontiers for FID and direct action as those systems become targets, either to be defended or attacked.

Endnotes

1 Guerrini, C.J., et al. "Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique." PLoS Biology, 2018. 16(10): p. e2006906; Kolata, G., and H. Murphy, "The Golden State Killer Is Tracked Through a Thicket of DNA, and Experts Shudder." *New York Times*, 2018. 27; Phillips, C., "The Golden State Killer Investigation and the Nascent Field of Forensic Genealogy." Forensic Science International: Genetics, 2018. 36: p. 186-188.

2 Boardman, J., and B. Sauser. "System of Systems-The Meaning Of." In *System of Systems Engineering*, 2006 IEEE/SMC International Conference on. 2006. IEEE.

3 Johnson, N.B., Facilitating Innovation in Technology Startups in Ghana: A Multiple Case Study of the Technology Entrepreneurship Ecosystem in Ghana. 2018; Asuzu, C. "For Ambulances That Can Track You Down to 10 inches, Come to West Africa." Daily Dose 2019, https://www.ozy.com/fast-forward/for-ambulances-that-can-track-you-down-to-10-inches-come-to-west-africa/92873, accessed cited 5 July 2019.

4 Maier, M. W., "Architecting Principles for Systems-of-Systems." *Systems Engineering: The Journal of the International Council on Systems Engineering*, 1998. 1(4): p. 267-284.

5 Sage, A. P. and C. D. Cuppan, "On the Systems Engineering and Management of Systems of Systems and Federations of Systems." *Information Knowledge Systems Management*, 2001. 2(4): p. 325-345; Sage, A. P. and S. M. Biemer, Processes for System Family Architecting, Design, and Integration." IEEE Systems Journal, 2007. 1(1): p. 5-16.

6 Engstrom, J., "Systems Confrontation and System Destruction Warfare." RR1708, Rand Corporation, 2018.

7 DISA. *Global Combat Support System - Joint (GCSS-J)*. 2019, https://disa.mil/Mission-Support/Command-and-Control/GCSS-J, accessed 20 August 2019; "Akamai helps US Air Force Improve Geographic Data Delivery." Akamai, 2019, https://www.akamai.com/us/en/our-customers/customer-stories-us-air-force.jsp, accessed 20 August 2019.

8 "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App." Human Rights Watch, May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance, accessed 1 August 2019.

9 *Challenges to Security in Space*. 2019, Defense Intelligence Agency: Washington, DC. p. 46.

10 "About DigitalGlobe." DigitalGlobe, 2019, https://www.digitalglobe.com/company/about-us, accessed 20 August 2019.

11 "Planet Monitoring," PlanetLabs, 2019, https://www.planet.com/products/monitoring/, accessed 11 November 2019.

12 Ford, D. *A Vision So Noble: John Boyd, the OODA Loop, and America's War on Terror*. CreateSpace, 2010; McIntosh, S.E. "The Wingman-Philosopher of MiG Alley: John Boyd and the OODA Loop." Air Power History, 2011. 58(4): p. 24-33.

13 Alberts, D.S., J.J. Garstka, and F.P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. 2000, Assistant Secretary of Defense (C3I/Command Control Research Program).

14 Van Horne, P. and D. Campbell, *Left of Bang: How the Marine Corps' Combat Hunter Program Can Save Your Life*. Tantor Audio, 2015.

15 Silver, D., et al. "A General Reinforcement Learning Algorithm That Masters Chess, Shogi, and Go through Self-Play." *Science*, 2018. 362(6419): p. 1140-1144.

16 Fang, W., et al. "Analysis of Action Mechanism of Graphite Bombs and Reaction Method of Power System." In *2010 International Conference on Power System Technology*. 2010. IEEE; Jeler, G. E., and D. Roman. "The Graphite Bomb: An Overview of Its Basic Military Applications." Review of the Air Force Academy, 2016(1): p. 13.

17 Challa, S., et al., *Fundamentals of Object Tracking*. Cambridge University Press, 2011.

18 Chivvis, C.S., *Understanding Russian Hybrid Warfare*. Rand Corporation, 2017.

19 Maurer, T., and K. Geers, "Cyber Proxies and the Crisis in Ukraine." Cyber War in Perspective: Russian Aggression against Ukraine, 2015: p. 79-86; Sullivan, J. E. and D. Kamensky, "How Cyber-Attacks in Ukraine Show the Vulnerability of the US Power Grid." *Electricity Journal*, 2017. 30(3): p. 30-35; Jaitner, M., and P.A. Mattsson. "Russian Information Warfare of 2014." In 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace. 2015. IEEE.

CHAPTER 33

The Whole World Is Watching: Special Operations in a Ubiquitous Surveillance Environment

George duMais

A growing commercial intelligence, surveillance, and reconnaissance (ISR) market will soon make global situational awareness possible for both state and nonstate actors. The availability of commercial ISR offers special operations forces (SOF) opportunities to enhance their situational awareness significantly, but it also requires them to take extraordinary measures to thwart the use of commercial ISR against them.

The Expansion of Commercial Overhead Capabilities

Omnipresent tactical surveillance via in-place terrestrial sensors and drones is already a fact of life for SOF. But surveillance is expanding rapidly beyond the local to persistent global coverage by not only a few countries with national satellite programs but also a host of both US and foreign civilian firms. The boom in the commercial space industry is leading to the development of a robust and sophisticated civilian overhead ISR network that will, by 2030, drastically alter the way all military operations, including those by SOF, have to be conducted. Given the rapid growth in the commercial space industry, anyone, anywhere will soon be able to obtain affordable, nearly real-time imagery and radio frequency (RF) data about any location on the earth. In addition to the increase in available raw data, companies are developing commercial analytic tools and services to interpret and fuse raw data with other sources at impressive speeds. Global situational awareness is becoming a commercial product.

Commercial overhead surveillance systems have been evolving in size, variety, and sophistication. Commercial overhead imagery has been available for several decades. Until recently, however, such systems had low resolution, large data latency, and long revisit rates. In addition, the high cost of such imagery meant only governments or large corporations could use it practically on a large scale. A new generation of small satellites, compact sensors, and inexpensive launchers is altering the market. Not only has the capability of imagery sensors increased,[i] but also additional modes of sensing are in use.[1] For example, at least 17 commercial hyperspectral sensors are now on orbit or scheduled for launch.[2] Also, four high-resolution (less than one meter) commercial synthetic-aperture radar (SAR) systems exist, which offer day-and-night all-weather imagery.[3] At least one firm also offers commercial RF data services, such as RF tag and beacon tracking and frequency-usage monitoring.[4] Moreover, revisit rates are decreasing rapidly. For example, Planet Corporation images the entire globe at least once a day, and BlackSky intends to provide on-demand imagery to clients within a half hour.[5]

Networks and data-analysis services have also evolved. For example, firms such as OneWeb and Amazon have announced plans for large-scale space-based networks to

i As of 2019, 18 commercial imagers with submeter resolution have been developed, some of which have video capabilities.

provide high-speed data analysis and internet services on orbit. Furthermore, Orbital Insight and BlackSky sell analytic services that fuse nearly real-time overhead data with other sources of real-time information to provide high-speed situational updates on and predictions for everything from crop yields and petroleum reserves to revenue projections for various retailers and industries.[6]

Many nontraditional and non-US firms are playing significant roles in these developments. For example, eight of the 17 commercial hyperspectral sensors currently on orbit or scheduled for launch belong to Satellogic, an Argentinian firm; similarly, Spanish, Italian, and South Korean firms have launched very-high-resolution (<0.5m) SARs.[7] Additionally, several nonaligned or potentially adversarial countries strongly encourage the domestic development of commercial space industries, indicating the profusion of overhead data will likely mirror the global spread of the internet or the smartphone. Moreover, the proliferation of overhead products, along with exploitation tools and myriad distribution networks, means commercial ISR will be extremely robust and hard to disrupt. The complexity and number of provider pathways will make denying or disabling access to these goods and services extremely difficult.

The Exploitation of Commercial Overhead Imagery by Nontraditional Actors

The growing availability and affordability of overhead imagery has already affected how many nations and nongovernmental organizations (NGOs) use space-based reconnaissance data. For example, the NGO Oceana uses commercial imagery and automatic-identification-tracking signals received by commercial satellites to identify illegal open-ocean fishing; using artificial intelligence, they can even identify the type of fishing methods being used.[8] Additionally, terrorist groups have long used satellite imagery. In 2002, the Central Intelligence Agency director testified before Congress that terrorist organizations, as well as foreign military and intelligence agencies, used commercial imagery to plan and execute their activities.[9] According to press reports, during 2006 raids of insurgents' homes in Iraq, British military personnel discoved numerous Google Earth images and maps apparently being used to identify weaknesses of, and plan attacks on, British and allied bases in the area.[10] In the near future, drug cartels, and other international organized crime syndicates, may use commercial space data for not only operational planning but also private indicators and warnings systems about law-enforcement activities.

Legitimate uses of surveillance technology will effect military planning and operations, including those of SOF. Current activities by NGOs, news media, academics, and various watchdog groups can and are impacting military and intelligence issues. For example, 38North, a group of academics who study North Korea, has begun using commercial satellite imagery to analyze activity at North Korean missile and nuclear sites. Figure 1, taken from the 38North website, is an image used in the group's analysis of activity at the Yongbyon nuclear complex.[11] Similarly, ThePrint, an online Indian newspaper, provides commercial imagery of China to a retired Indian army officer who specializes in photo interpretation; he uses the imagery to identify and analyze

Chinese military facilities. Figure 2 shows one of the images he used in his analysis of a purported Chinese electromagnetic pulse (EMP) test site.[12]

Analysis of satellite imagery by news media and watchdog groups has started to effect public perception of official reporting. For example, in 2019, India staged airstrikes in the Pakistan-held Kashmir region against what it claimed to be terrorist targets. India also stated the strikes had destroyed their intended targets; however, two independent websites used Planet Corporation imagery to analyze the area where the strikes occurred, and both published analyses of the imagery disputing the official Indian version.[13] Nongovernmental analysis of satellite imagery has also influenced actions by military or paramilitary groups. A 2012 incident in Sudan shows how such analysis and publication can effect operational outcomes. During the border conflict between Sudan and South Sudan, the Harvard-based Satellite Sentinel Project (SSP) released an image that showed a construction crew building a tank-capable road leading toward an area occupied by the Sudan People's Liberation Army (SPLA), the army of the Republic of South Sudan. SSP's goal was to warn civilians about the approaching tanks so they could evacuate. However, the SPLA saw the images and, as a result, attacked the road crew, killing some of them and kidnapping the rest.[14]

While no known groups exist that publicly post similar analysis of US-military–related installations and activities, one must assume such observation and analysis is happening and will become more prevalent in the future. National security analysis is becoming a do-it-yourself enterprise.

Figure 1. Commercial image and annotation appearing on the 38North website and used to monitor activity at North Korean nuclear facilities.

Figure 2: Commercial image and annotation taken from the ThePrint website, used in its photo analysis of a purported Chinese EMP test facility.

Implications of Commercial ISR for SOF

The proliferation of commercial space capabilities offers considerable opportunities for SOF but also causes serious challenges to operational security and force protection.

The Plus Side

On the positive side, the wealth of commercial overhead (and related) data promises to be an extremely useful supplemental source of intelligence for planning and operational purposes. These resources represent a new level of open-source information that can combine with traditional ISR sources to give a more complete and timelier picture of what is happening in areas of interest. They also offer SOF the opportunity to gather intelligence analysis more proactively than possible previously; SOF can work with commercial firms to develop focused information gathering and analysis that may not be readily available through traditional means. By using commercial sources creatively, SOF may establish their own specialized channels of information tailored specifically to both their immediate and long-term needs. Moreover, combining both traditional ISR information and commercial data will provide

a more robust intelligence-validation process, resulting in heightened confidence in situation assessments.

The US government neither owns nor controls commercial ISR sources, meaning SOF cannot rely on their availability in times of crisis or conflict. But the growing number of companies offering off-the-shelf spaceflight hardware and software provides an alternative path: the development and deployment of affordable organic space assets for SOF use. The growing affordability and expanding capabilities of small satellites mean SOF will be able to develop constellations of small satellites tailored to specific operational scenarios and functions, with the expectation these constellations can be deployed in a timely fashion to support specific missions. This possibility will increase sharply as launch-on-demand services, such as those planned by Rocket Lab and SpaceX, become available. Additionally, as organic assets, these satellites can be optimally configured to perform specific missions. Since they will be under the complete control of the operational unit, there will be no need for deconfliction with other users or the long lead times normally required to obtain tasking priority.

The Challenges

Special operations require stealth, secrecy, and surprise. Ubiquitous overhead surveillance will make all three harder to achieve.

Perhaps the most significant change from the ubiquity of overhead surveillance will be the "loss of home-field advantage." In the future, it will not be possible to know with confidence whether SOF training exercises, mission rehearsals, or other sensitive activities in CONUS are being monitored from above. In all likelihood, everyday activities at known SOF facilities will be monitored, and any changes in routine, tempo, location, or configuration will be detected and analyzed. Moreover, overhead data will be fused with terrestrial data (from cell phones, social networks, and other sources) to identify and track SOF personnel, provide detailed analysis of activities at known SOF facilities, and identify and expose classified locations and activities.

Under these circumstances integration of overhead security with cyber, physical, and other operational security measures will become critical. Additionally, denial and deception (D&D) will become an increasingly important element of SOF operations. The use of concealment, camouflage, decoys, and obscurants will have to become more sophisticated and widespread than it is currently. For example, surfaces of decoys will have to be designed with spectral signatures identical to those of real objects when viewed by overhead hyperspectral sensors. Also, such decoys must have some active capacity, such as the ability to mimic some of the behavior (such as the vibrational signature) of real equipment.

Tactical and strategic D&D must merge. Practicing D&D for a particular mission, operation, or campaign only will no longer be enough; it will be required throughout the entire operational regime, including logistics and training, transport, and acquisition. Thus, SOF may have to increase the use of underground facilities, and virtual reality

may often have to substitute for physical settings. Elaborate methods of communication and social-media management and misdirection will need to be employed on an unprecedented scale. It may be necessary, for example, to prepare for—or appear to be preparing for—numerous missions at once to create confusion and doubt about intentions. SOF components will need to monitor commercial overhead capabilities and activities diligently, looking not only for explicit postings of concern but also less direct indicators of interest in their activities, such as unusual tasking behavior or changes in the distribution patterns of commercial firms providing analytic services based on overhead data. SOF must also develop tactical counter-space capabilities. Furthermore, SOF will likely need portable equipment and methods for defeating overhead surveillance, including jamming, spoofing, and inserting false data. Special operations competencies will have to expand to include counter-space skills.

Conclusions

Like all new technologies, ubiquitous overhead ISR is a two-edged sword. It offers great opportunities to enhance SOF capabilities but also presents a unique set of challenges for negating its use by adversaries.

I have argued both offensive and defensive uses of space assets and counter-space capabilities must be established to develop operational and analytic expertise to maximize the benefits of commercial ISR and to minimize the threat it presents to SOF missions. Because SOF operations have different focus points than those of the strategic ISR mission (for example, national technical means of verification, nuclear detonation detection, strategic warnings and indications), the evolution of SOF overhead-related requirements will probably be significantly different from that of national-level ones. Therefore, as a result of the increase in 24/7 commercial ISR and associated analyses, strategic overhead reconnaissance and surveillance will largely become detached from tactical ISR. This means overhead support to the warfighter will increasingly become the duty of warfighters themselves (including SOF), rather than a support function provided to them by the intelligence community.

Finally, while I have set out the general features of the expected impact from commerical ISR technology, the field will likely evolve in unexpected ways. Not all of its implications can be foreseen at this time. Therefore, SOF operators must begin investigating the possibilities for, experimenting with, and mastering the use of this novel technology as soon as possible to be at the forefront of both exploiting it and minimizing vulnerability to it.

Disclaimer: The views, opinions, and findings expressed in this article are solely those of the author and do not necessarily represent the views of FTS International.

Endnotes

1 Aerospace Economic and Market Analysis "Commercial Satellite" Cheat Sheet; Aerospace Corporation 2019.
2 Aerospace Economic and Market Analysis "Commercial Satellite" Cheat Sheet; Aerospace Corporation 2019.
3 Aerospace Economic and Market Analysis "Commercial Satellite" Cheat Sheet; Aerospace Corporation 2019.
4 HawkEye 360, 2019, https://www.he360.com, accessed 19 September 2019.
5 Planet Labs Inc., 2019, https://www.planet.com, accessed 19 September 2019; BlackSky, 2019, https://www.blacksky.com, accessed 19 September 2019.
6 BlackSky, 2019, https://www.blacksky.com, accessed 19 September 2019; Orbital Insight, 2019, https://orbitalinsight.com, accessed 19 September 2019.
7 Aerospace Economic and Market Analysis "Commercial Satellite" Cheat Sheet, Aerospace Corporation 2019.
8 Fantozzi, Joanna, "Google and Oceana Team up to Map Illegal Fishing," 17 November 2014, https://www.thedailymeal.com/news/eat/google-and-oceana-team-map-illegal-fishing/111714, accessed 19 September 2019.
9 DCI Testimony: Converging Dangers in a Post 9/11 World, Testimony of Director of Central Intelligence George J. Tenet, Before the Senate Select Committee on Intelligence, 6 February 2002, https://www.cia.gov/news-information/speeches-testimony/2002/senate_select_hearing_03192002.html, accessed 19 September 2019.
10 "Google, British Military Discuss Google Earth Use in Attacks," Neowin, 16 January 2007, https://www.neowin.net/news/google-british-military-discuss-google-earth-use-in-attacks, accessed 19 September 2019.
11 "North Korea's Yongbyon Nuclear Complex: No Sign of Operations," 38 North, March 15, 2019, https://www.38north.org/2019/03/yongbyon031519/, accessed 19 September 2019.
12 Bhat, Vinayak, "These futuristic Chinese Space Denial Weapons Can Disable or Destroy Opposing Satellites," ThePrint, 23 March 2019, https://theprint.in/defence/these-futuristic-chinese-space-denial-weapons-can-disable-or-destroy-opposing-satellites/210212/, accessed 19 September 2019.
13 "Satellite Images Suggest India Fabricated 'Successful' Attack on Terror Camp," Zero Hedge, 6 March 2019, https://www.zerohedge.com/news/2019-03-06/satellite-images-suggest-india-fabricated-successful-attack-terror-camp-pakistan; accessed 19 September 2019; "Balakot Airstrike: Forensic Satellite Imagery Analysis," Great Game India, 2 March 2019, https://www.voltairenet.org/article204302.html, accessed 19 September 2019.
14 Beam, Christopher, "Soon, Satellites Will Be Able to Watch You Everywhere All the Time," MIT Technology Review, June 26, 2019, https://www.technologyreview.com/s/613748/satellites-threaten-privacy/, accessed 19 September 2019.

CHAPTER 34

The Growing Importance of Subterranean Warfare and the Integration of General-Purpose Forces in Subterranean Operations

LTC Michael Alexander

The SubT Domain

As the US Army prepares to face an evolving operational environment, a broad spectrum of new threats greatly complicate the battlespace. Recent combat experience in Iraq, Syria, and Afghanistan, as well as ongoing national security threats from North Korea, Iran, and elsewhere suggest that innovation in underground facilities (UGFs) presents a major challenge for US forces. Adversary groups and nations are leveraging complex terrain to exploit operational advantage. The US must match such innovation to defeat enemies who use UGFs and subterranean (SubT) environments for military purposes.[1] This chapter outlines the UGF challenge and suggests ways to address it.

Operationally, the subterranean environment comprises tunnels and UGF that can be constructed in naturally occurring environments, such as caves and caverns, as well as human-made structures, ranging from simplistic tunnel systems to extremely complex facilities designed for advanced military applications.[2] Much has been learned from UGFs constructed for smuggling purposes, as well as historic experiences with UGFs in Vietnam and elsewhere. For our purposes, we are interested in UGFs that are utilized for military activities.

Because of geographic limitations and the need to conceal activities from US intelligence collection, US adversaries have utilized underground tunneling and construction technology to design and create increasingly sophisticated subterranean structures.[3] A wide range of regular and irregular forces are innovating in the construction and use of "hard and deeply buried targets" (HDBT) and UGF, which can include modified natural and human-made structures ranging from hardened-surface bunker complexes to deep tunnels. These facilities typically incorporate the attributes of "concealment, self-sustainment, multifaceted communications, strong physical security, modern air defenses, and protective surrounding—often in mountainous or urban terrain to enhance their suitability for military application."[4]

In contrast to the rudimentary UGFs employed by insurgent groups such as the Vietcong, modern HDBTs are often well-connected networks housing operational capabilities used to support leadership protection, intelligence, planning, weapon production, basing, and command and control of ground operations. In the case of weapon production, UGFs can be used to support assembly, storage, and deployment facilities for weapons of mass destruction (WMD) and antiaccess/aerial denial defense systems.[5] In Syria and Iraq, ISIS utilized tunnel systems to initiate attacks on coalition forces and launch drones for intelligence collection activities.[6] The role of state sponsorship for nonstate actors such as al-Qaeda, Hezbollah, Hamas, or

ISIS often determines the level of investment and sophistication of their UGFs and associated logistical support for operations utilizing them.

The use of UGFs by foreign governments and nonstate organizations to conceal and protect critical military and civilian assets has increased in recent years, according to the intelligence community. Countries such as China, North Korea, Iran, Syria, Russia, Pakistan, and Lebanon (in this case used by Lebanese Hezbollah) all have active underground programs.[7] A significant trend has emerged in which countries of concern are basing ballistic and cruise missiles and other systems designed for antiaccess/area denial weapons within UGF.[8] In light of this trend, US forces have begun preparing to counter these efforts, driven in part by priority missions such as counterterrorism and counterproliferation that could require US combat forces to enter UGF.

The Department of Defense (DOD) estimates 10,000 known or suspected HDBTs exist worldwide. Of this number, roughly 20 percent of these facilities support a major strategic function and are in or near highly concentrated urban areas. These HDBTs are used to protect senior leaders, command-and-control functions, and storage of WMD, among other purposes. Some are reportedly buried in hard rock at depths greater than 300 meters.[9] US strategy cannot afford to accept the invulnerability of these critical facilities and must therefore develop options for holding them at risk, and striking them if necessary. Both deterrence and defense depend on it.

Overwhelmingly, the US strategy for holding UGF at risk depends on specialized aerial-delivered munitions such as the Massive Ordnance Penetrator (MOP). The limitations of this technology have motivated the DOD to develop more options, specifically involving the application of ground forces to clear HDBT and UGF. To address this issue, special operations forces (SOF) have maintained a small force with limited capabilities, but the need for a more robust force with a broader range of capabilities is clear. However, the growing number and diversity of UGF are outpacing US efforts to develop response options. As the intelligence estimates demonstrate, the number of UGF targets requiring US ground-force-response options are on the rise because either the depth of the structure negates penetrator weapons effectiveness or the likelihood of a potential release of chemical, biological, or radiological containments makes kinetic strikes highly undesirable.[10] When considering the continued proliferation of UGFs and the limits of kinetic weapons to destroy these facilities, expanding US ground-force-defeat options should be a top priority.

New Directions and Possible Solutions

Widespread use of tunnels and UGF to gain tactical advantage is becoming more sophisticated and increasingly effective, increasing the likelihood that US forces will encounter military-purposed subterranean structures on future battlefields. However, three main factors limit the DOD's current abilities to address this trend: 1) Current counter-UGF capabilities are centered on precision-strike weapons, 2) limited SOF ground-force options exist, 3) and locating and characterizing UGFs is difficult.

To overcome these obstacles, DOD, the Army, and SOF need to expand conventional-force UGF options. In addition to providing needed technology and resources, existing capabilities are available to address many of the shortfalls. For example, specialized training could be expanded to larger segments of the force, including general-purpose ground forces. Such training would cover the following areas:

- Mission Command: UGFs present a degraded environment for navigation, communications, visibility, and control. Advancements in communications are needed to maintain command authorties and guidance in underground structures. Sensors and autonomous vehicles can help navigate where visibility is impaired. Equipping and training ground forces in the use of these technologies is essential.
- Intelligence: To address the problem that overhead systems cannot reliably detect underground structures and related activities, dedicated, advanced overhead systems should be available to inform ground forces of the existence and characteristics of UGFs. Drones, multispectral imagery, and ground-penetrating radar all provide critical information on UGFs, but too often such information and analysis is not available in real time to ground forces. This type of reach-back support is especially relevant for troops who unexpectedly encounter UGF and must engage enemies who are utilizing them. In addition to technological breakthroughs, training in these intelligence capabilities and how to access them could improve situational awareness and real-time decision-making for US forces encountering UGFs. Timely intelligence is especially critical where the presence of WMD is suspected.
- Movement and Maneuver: UGFs often present a baffling maze of channels, chambers, obstacles, barriers, and hidden compartments—made even more treacherous by booby traps and other defensive measures. Expanded training is needed to familiarize more US forces with these physical challenges and provide them with a suite of proceedures and defeat/bypass options for use against UGFs. Breaching tools should be a focus of innovation, as well as robotics.
- Force Protection: Wherever possible, US forces should have advance familiarity with acoustic thresholds and blast overpressure limitations of UGFs, especially in relation to various US and foreign weapon systems. Relatedly, the characteristics of air quality inside UGFs and their associated HVAC capabilities should be available to US forces, along with appropriate protective gear to enable operations in toxic environments. A specialized UGF training program could better prepare a larger number of US forces to cope with these contingencies.

Several USG organizations are making progress on various aspects of the subterranean warfare challenge. The US Army Asymetric Warfare Group, DARPA, the National Ground Intelligence Center, SOFWERX, and other innovation hubs are sponsoring research and development to address the UGF challenge. Several training centers such as the US Army Muscatatuck Urban Training Center in Indiana are cultivating new doctrines and operational concepts for subterranean warfare.[11] Advancements in autonomous vehicles will be central to many of these innovations. However, these advancements and innovations will have limited impact unless they are extended to a much wider population of general-purpose forces (GPF), in addition to the specialized units who have traditionally benefited from them. Similar to counterterrorism and counterproliferation operations, the integration of GPF with SOF would greatly advance our preparedness to conduct subterranean operations.[12]

As the likelihood grows of US forces encountering military-purposed subterranean structures, key pieces of an effective response are missing. Gaps in doctrine and training prevent the types of improvements outlined here, incuding the requirment for interoperability of SOF and GPF.[13] The path forward depends on making SubT warfare a training requirement for both SOF and GPF. This process could begin with the TRADOC G-2 Intelligence Support Activity (TRISA) defining the subterranean environment as a training priority for both GPF and SOF. From this training, a habitual partnership with specific GPF and SOF units could be developed. The training plan should include integrating best practices and sound Tactics, Techniques, and Procedures (TTPs) from the USSOCOM community and an update of the Subterranean Handbook to address historic and emerging challenges of SubT warfare.[14]

The Path Forward

The Army is capable of implenting the measures outlined here. Its own Joint Capabilities Integration Development Systems process lays out a method that could be used to prepare for future SubT warfare. Here is a brief summary of how this process could work.

- Doctrine: Current publications should be updated and integrated into training and planning.
- Organization: Key positions could be empowered to ensure the development and integration of SubT technologies and TTPs. This will be critical with respect to interoperability.
- Training: Require development of programs of instruction, mission rehearsal exercises, and home-station training concepts. Performance will be judged on preparedness for SubT operations.
- Material: Specialized equipment such as the technologies cited above must be prioritied for R&D and fast-tracked for rapid deployment.
- Leader Development and Education: Add to selected officer/ noncommissioned officer courses modules on the UGF threat and begin

development of tactical competence in this operational environment. Support Professional Military Education research on SubT warfare. Conduct table-top exercises (TTX) to explore a wide range of UGF defeat scenarios.

- Personnel: Citations and advancement to incentivize SubT warfare skills, knowledge, and experience.
- Facilities: Build additional underground training facilities and use advanced simulation techniques to model and red-team different UGF scenarios.15

If integrated with current SubT qualified SOF, GPF must be capable of conducting decisive operations, including synchronized combined-arms maneuver in a joint/combined and interagency environment to gain access to and seize control of targeted UGFs. This will be especially important for WMD sites, where procedures to confirm or deny the presence of WMD materiel, establish conditions for exploitation and elimination activities (by more technologically equipped and specialized forces), defend against ongoing hostilities, and exfiltrate US forces along with any seized articles. To achieve this, a wider population of GPF must understand the mission, develop core competencies, integrate maneuver and technical forces, assess C2 requirements (for information, data flow, and communications), practice operational sustainment, train in underground facilities, and master the use of new technologies developed to support the SubT mission.

If projections for the proliferation of UGF and more extensive use of the SubT domain hold true, the steps outlined here would provide the United States with the robust SubT warfare capabilities that are required to achieve US national security objectives.

References

Asymmetric Warfare Group. *AWG Subterranean Brief.* 2012. Retrieved from AWG Unit Archives, Fort Meade, Maryland.

Bowman, M. *Information Paper: Subterranean Warfare.* Fort Meade, Maryland. 2009. Retrieved from AWG Unit Archives.

Elliott, C. *Information Briefing: Subterranean Warfare.* Fort Meade, Maryland. 2012. Retrieved from AWG Unit Archives.

Tucker, P. (2018) Underground May Be the US Military's Next Warfare Fighting Domain. Retrieved from Defense One, https://www.defenseone.com/technology/2018/06/underground-may-be-us-militarys-next-warfighting-domain/149296.

National Ground Intelligence Center, Land Warfare Capstone Threat Assessment: The Future Operational Threat Environment, Volume IV.

DARPA, Subterranean Challenge, https://www.subtchallenge.com.

Endnotes

1 Elliott, C. (2012) *Information Briefing: Subterranean Warfare*. Fort Meade, Maryland. Retrieved from AWG Unit Archives.
2 Tucker, P. "Underground May Be the US Military's Next Warfare Fighting Domain." *Defense One*, June 26, 2018, https://www.defenseone.com/technology/2018/06/underground-may-be-us-militarys-next-warfighting-domain/149296/, accessed January 27, 2020.
3 Asymmetric Warfare Group. (2012). *AWG Subterranean Brief*. Retrieved from AWG Unit Archives, Fort Meade, Maryland.
4 Asymmetric Warfare Group, *AWG Subterranean Brief*, 2012.
5 Asymmetric Warfare Group, *AWG Subterranean Brieff*, 2012.
6 Tucker, "Underground May Be the US Military's Next Warfare Fighting Domain," 2017.
7 Elliott, *Information Briefing*, 2012.
8 Elliott, *Information Briefing*, 2012.
9 Asymmetric Warfare Group, *AWG Subterranean Brief*, 2012.
10 Elliott, *Information Briefing*, 2012.
11 National Ground Intelligence Center, Land Warfare Capstone Threat Assessment: The Future Operational Threat Environment, Volume IV.
12 Elliott, *Information Briefing*, 2012.
13 Asymmetric Warfare Group, *AWG Subterranean Brief*, 2012.
14 Elliott, *Information Briefing*, 2012.
15 Asymmetric Warfare Group, *AWG Subterranean Brief*, 2012.

CHAPTER 35

Chaos and Constraint: Special Operations and "The Convergence"

LTC James D. Leaf

> *"The price you pay for the refusal to make an assessment is that when the reality occurs it will be much less manageable"*
>
> ***—Dr. Henry A. Kissinger, Fort Bragg, 2015[1]***

In a world buffeted by change, the emerging operating environment (EOE) will be the most complex and lethal yet experienced by US special operations forces (SOF). Complex factors are bringing global change comparable to the introduction of the printing press to Europe half a millennium ago, which spread knowledge and upended institutions, society, and kingdoms.[2] In the emerging environment of the twenty-first century, the Cold War is long over, the post-9/11 global war on terror is winding down, and powerful rising and revanchist nations are challenging the United States and the world order it created. In this setting, US SOF finds itself at the vanguard of US foreign policy, conducting legacy missions altered by the emerging "new normal."

As change sweeps the world, it brings chaos globally, while institutional limitations constrain governments, militaries, and other organizations as they attempt to adapt. In this emerging global setting, any opponent—nation-state militaries and security organizations, nation-state proxies and surrogates, nonstate actors, and even individuals—will have access to any advanced technology. In short, they will be able to have "statelike" capabilities, which will challenge SOF in every warfighting domain. Opponents with equal or overmatching statelike capabilities will be a norm. This is the world of "The Convergence," the point where the gap between nonstate- and state-actor capabilities diminishes and the risk to force and mission success increases significantly. To ensure mission success, US SOF must "harden." It should prepare to face and thrive against statelike actors because this level of capability will be ubiquitous in the twenty-first century, regardless of opponent.

Thought Piece: "Convergence" 1950s Style

In March 1954, the North Vietnamese guerrillas introduced statelike capabilities—massed artillery and antiaircraft guns—against the French at the battle of Dien Bien Phu. To achieve this, it took the North Vietnamese months and the work of thousands of its personnel tunneling through mountains and dragging cannons by hand. The artillery was foreign military aid from the Soviet Union and other nations. Such was "Convergence" in the 1950s. In the twenty-first century, this can be done with a credit card, bitcoin, and access to Amazon or the "dark web." How does US SOF prepare for such a situation?

One approach to gain understanding of the EOE is to forecast using a near-term, five-to-seven-year focus. Or using US Department of Defense (DOD) budgetary jargon: "Program Objective Memorandum" (POM); this time frame can also be refered to as "POM+." This gives current decision-makers and practitioners concrete information to use when making resource decisions and incentivizes the forecaster; in five years, the forecaster's work can be "graded" for accuracy. While valuable, using a longer forecast perspective risks being of limited immediate practical value for decision-makers, no matter how insightful the analysis. It lacks a "so what?" What does the busy SOF leader do with analysis of "urbanization" or "demographic shifts" in 2050? How does such information help future-focused decision-making happening now?

This is important because "Convergence" is happening now. The twenty-first-century operating environment will depart dramatically from the past. Complex global factors are not only rapidly changing our daily lives but also the future US SOF battlefields. The specific missions our nation's leaders will expect of SOF in the near future are unlikely to change much, but the "new reality" of the twenty-first century EOE will reshape them. Legacy SOF missions will continue, but the environment in which they will occur will be different.

Global Themes: "Chaos and Constraint"

Throughout history, technology has been a driver of change. In our era, the rate of technological advancement and accompanying change is exponential. This unrelenting pace brings sudden and radical transformation that disorders traditions, norms, and beliefs. People and institutions struggle in this tumult. This is chaos.

A natural result of this chaos is the breakdown of economic, political, and diplomatic institutions that have been the foundation of the global post–World War II order. This phenomenon upends the lives of individuals and nations. Government institutions resist change and are slow moving and bureaucratic, undermining adaptation and reform attempts. These dynamics constrain nations. In this chaotic world, a nation so constrained risks failure to understand, let alone succeed at, core missions like national defense.

Global Factors

Globally, many significant factors occur and interact in unpredictable ways to shape the EOE. To better comprehend the EOE, US SOF should focus on technology spread, global competition, expanded competitive space, urbanization, resource realities, and legacy institutions. The global competition between powerful nation-states is expanding the competitive space, from the bottom of the oceans to outer space. This competition helps drive technology proliferation, which increases the risk of capability overmatch and domain superiority. Operating with increasingly constrained resources while conducting twenty-first-century operations in urbanized landscapes with twentieth-century institutions will increase the challenges US SOF will face.

Technology Spread

States no longer drive technological innovation. Gone are the Cold War days when DOD, Department of Energy, and NASA programs drove technological innovation. These days, the commercial sector—represented by Google, Apple, Amazon, and others—dominate and make available advanced technology to anyone who can buy, borrow, or steal it.

Thought Piece: Who Uses What?

Early in the twentieth century, the British army implemented a groundbreaking and complex capability by creating the Royal Machine Gun Corps, a new branch of technicians to use a new technology.

Like the machine gun, are drones, cyber operations, or robotics things best left to specialists or capabilities every soldier will use eventually? In the emerging world of the Internet of Things and proliferation of artificial intelligence, can any soldiers or units afford to be "offline?"

Advanced military technology is also proliferating as nations compete for regional and global position. In the global competition between nuclear-armed nations, the importance of surrogates to achieve policy goals in lieu of uniformed military forces will increase, and so will their capabilities. US SOF will face relatively indistinguishable and, at times, possibly superior capabilities, regardless of the opponent. Therefore, the decades-old assumption is gone that the United States possesses technological and capability overmatch. Technological superiority and overmatch are not US birthrights. The low cost, availability, and ease of use of advanced technologies allows adversaries to purchase and field new technologies rapidly. ISIS "beta tested" this reality with their unexpected use of drones in Syria in 2017. In the emerging EOE, this phenonenom can be expected regarding the capability of any enemy.

Thought Piece: "Gray Zone" or Great Game?

The "Great Game" was a sixty-year competition in central Asia between the Russian and British Empires in the nineteenth century. It was short of major war but far from peaceful. It featured the use of spies, proxies, surrogates, and mercenaries and included four "minor" wars, the deposition of local leaders, the destruction of a British field army, and changes to national boundaries as the British and Russians created and annexed nations. Observers have labeled our era of state competition for local and even global supremacy the "gray zone." In reality, is this actually a new "Great Game"? In a global competition conducted mostly outside of declared war zones, how is SOF to be used, and does it have the capabilites and, more importantly and perhaps less understood, the authorities to operate outside of declared war zones?

Global Competition

The 2018 US National Defense Strategy describes unambiguously: "Long-term strategic competitions with China and Russia are principal priorities for the Department [of Defense]." This ongoing global competition is a continuous economic, diplomatic, information, and military effort to gain and maintain positional advantage: a form of global siege warfare. Nuclear proliferation makes full-scale interstate war unlikely. States will employ military capabilities, proxies, surrogates, and other means to secure geopolitical advantages rather than traditional destruction of enemy forces on a battlefield. Critical infrastructure, societal cohesion, and even basic government function are targets. In this environment, US SOF utility is wide ranging. The highest long-term concerns for the United States are Russia, China, and terrorism. This is noted not to limit SOF to these threats but to highlight the relevance of US SOF with regard to these threats.

Russia is a shadow of the former Soviet Union. It is not a US "peer competitor" but a well-armed and capable rogue nation willing and desirous to disrupt the international order and the United States' global position, but it knows it cannot control either. Given the limitations of Russia's power and its dangerous nature, US SOF can play a critical role in countering Russian actions, especially in "phase 0."

The size of China's population, economy, and publicly stated global ambitions make China unlike any other competitor the United States has ever experienced. China's military transformation from an ill-equipped, largely ground-focused military to one using advanced technology with regional, global, and space impacts is arguably the biggest modern national security concern. Equally true is that the Chinese military lacks the United States' recent and institutional military experience and last fought (and lost) a war in 1979. There has been no Chinese Grenada or Eagle Claw, let alone a Desert Storm. More broadly, China is trying to transition from a land to a maritime power. History records such efforts as rarely succeeding. Nonetheless, countering China's ambitions will test US ability to maintain its global position and the current global order. Given the stakes involved, SOF has a crucial role in what could be the critical US strategic security concern of the twenty-first century.

In the EOE, terrorism remains a priority. Its occurrence is unpredictable, it targets civilians, and its impact is disproportionate. The impacts of 9/11 are well known and profound. In earlier decades, terrorism deeply impaired both the Jimmy Carter and Ronald Reagan presidencies. In 2019, US SOF killed the leader of and eliminated the physical "caliphate" in Syria and Iraq of ISIS, an organization unheard of before 2014. This counter-ISIS campaign came three years after a US president had fulfilled a campaign pledge to withdraw all US forces from Iraq. Terrorism remains a US priority because of its unpredictable nature and risk of significant impact. With capabilities developed and optimized by continuous operations since 2001, SOF can be ideal leaders for countering terrorism in the twenty-first century EOE.

Success in the Twenty-First Century Requires Change for US SOF

The Cold War and especially World War II are the cultural and intellectual touchstones for how Americans view conflict. Our government's structure and national security policy-making functions are legacies of those conflicts. Another is represented by the organizations, major platforms, activities, and functions of our military. The EOE requires a departure from these cherished and well-understood traditions. For the twenty-first-century global nation-state competition, something more relevant to examine than the post–World War II United States might be the limited dynastic conflicts of eighteenth-century Europe, when war's goals were limited and nations competed but did not seek to destroy the existing order. "Tech wizards" of that day like the engineer Sébastien Le Prestre de Vauban or a military innovator such as Frederick the Great may not resonate with Americans the way George S. Patton or William Halsey do. However, how these leaders and organizations leveraged techology and developed means to achieve objectives without the destruction of opponents are worthy subjects to explore.

Expanded Competitive Space

Having largely created the world order, the United States is now defending the status quo while multiple powerful competitors look to disrupt it and their place within it. For the US military, the domain dominance of the post–Cold War unipolar world is gone. For US SOF, operating in contested domains against opponents with roughly equal capabilities will be the norm. However, this is not a significant departure historically for what US SOF has done or been expected to do, operating in denied areas, outnumbered and at a tactical disadvantage. US SOF have experienced this phenonenom and were as in fact created to operate successfully within a contested enviornment.

However, SOF leaders and practitioners must better understand and analyze the EOE. In a global competition between powerful nation-states, the competition reaches everywhere. Space is one critical domain. Both in the commercial and governmental realms, human activity in space is growing and diversifying. Commercially available small and inexpensive satellites are now a reality.[3] In 2019, India joined the United States, Russia, and China as nations who have successfully targeted and destroyed a satellite. In time, will commercial antisatellite systems also be available? How might great-power competition in space affect SOF operations? US leaders should heed Chinese military writing that speaks of targeting communication, early warning, and reconnaissance satellites to "*Blind and deafen the enemy*" (italics added).[4] SOF must understand and prepare for operational impacts to US forces as it prepares its personnel and develops capabilities for the twenty-first century. The Air Force, Navy, and recently established Space Force will dominate US space efforts, but SOF should also understand this domain, contribute to its requirements, and, where appropriate, make niche additions to organic capabilities.

Thought Piece: The New High Ground?

China's ambitions for a permanent space presence are unambiguous. Prominent in these plans is the moon because, "Whoever first conquers the Moon will benefit first."5 A permanent moon base gains access to the moon's resources, supports deep-space travel, denies adversary access, and enables creation of a space-based solar-power system for the earth.6

A solar panel array built on high ground illuminated nearly year-round on the moon's poles could provide the steady power source required to make a permanent moon base a possibility. These areas, called the "peaks of eternal light," may be key terrain in twenty-first century state competition.7 Created to operate in denied areas and for missions with strategic impact, SOF could have a role in securing this new ultimate high ground. What capabilities would such SOF require?

Urbanization

Since World War II, the modern world has urbanized dramatically. As of 2018, 55 percent of the world's population was urban.[8] For the fist time ever, most humans live in cities, the result of an urban population surge from 751 million in 1950 to 4.2 billion in 2018.[9] Analysis published in 2018 places over 12 percent of the earth's population living in one of 33 megacities (10 million inhabitants), with the United Nations projecting the number of megacities will increase to 43 by 2030.[10] Correspondingly, post–Cold War conflict has been largely urban: Khafji, Grozny, Sarajevo, Brazzaville, Baghdad, Mumbai, Beirut, Aleppo, Mosul, Raqqa, Gaza, Mogadishu, Donetsk, and Sanaa. War is a human endeavor, and a rapidly urbanizing world naturally features fighting where the people are: cities.

This ubiquity of urban landscapes means SOF will operate in them. Megacities, increasing in both size and number, are complex operating environments. These cities can serve as incubators of disruptive social movements and supply terrorist and criminal networks with a near limitless pool of unemployed, underemployed, disillusioned, and left-behind individuals. SOF operating in these cities will have to navigate in mazelike terrain at street level, underground, and in multistory structures that will degrade C4 systems. Enemy advanced technology, urban sprawl, and a desire to minimize civilian casualties will limit US SOF technological overmatch, firepower, and other legacy advantages.

Resource Realities

An obvious component of national defense is the ability to fund it. For financial and demographic reasons, the United States faces significant challenges in the near future.

Government Accounting Office (GAO) analysis found that by the end of 2018, the debt-to-GDP ratio of the US federal budget was predicted to exceed the historical World War II–era high of 106 percent in 13 to 20 years.[11] GAO analysis projects that

the depletion of key entitlement funds will start in 2026.[12] In 2019, GAO analysis showed that Health and Human Service (Medicare, Medicaid), Social Security Administration, Veteran's Administration, Defense, and debt-payment spending consumed over three-quarters of the federal budget.[13] The longer term outlook is even less positive. Before the Covid-19 pandemic, GAO projected the debt-to-GDP ratio would exceed 100 percent by 2030 and continue to increase well beyond historic highs.[14] At the same time, significant demographic changes are also occurring. By 2030, the entire baby-boomer generation, 20 percent of the US population, will be at least 65 years old.[15] By 2030, the US population will no longer be "triangular" (i.e., many young people and fewer old) and instead become "square," with the under-18 population and over-65 populations being nearly symmetrical (75.4 and 73.1 respectively).[16] These demographic trends will continue throughout the twenty-first century with impacts on everything from military recruiting, entitlement spending growth, and tax-revenue collection.

In the decades ahead, the combination of finance and demographic realities will constrain US defense resources and require pragmatic and difficult decisions regarding priorities and reforms in acquisition, pay, pensions, and force structure. The costs of defense have grown consistently, even as the size of the overall defense force has shrunk. Costs for operations and maintenance and compensation for both active-duty and retired military personnel have grown dramatically, with the latter cost doubling since 2000.[17] It is an unfortunate but a certain planning assumption that, barring a significant state-on-state conflict, the US defense budget will not increase significantly. Sustaining present force structures and capabilities will likely prove difficult. Also, of concern for SOF are the impacts on recruiting as the US population ages and the pool of available and interested young people decreases. What the United States needs a "commando" to be and to do will likely be different in the twenty-first than the twentieth century. Adhering to legacy conceptions of SOF is an unaffordable luxury in an environment of constrained resources and numerous and capable opponents.

Thought Piece: What Are Commandos Now?

In earlier eras, "special operations" meant special capabilities (e.g., rifled muskets), techniques and tactics (e.g., patrolling, close-quarter battles), and/or missions (e.g., working with indigenous forces, counterterrorism) that later proliferated to the wider force. In the twenty-first century, what does it mean to be a commando, and what unique capabilities and missions does a commando have?

Legacy Institutions

Starting late in World War II, the victorious allied nations led by the United States laid out the diplomatic and economic framework and institutions of the postwar order. US defense, intelligence, and foreign policy institutions are creations of the era and have remained largely unchanged since then. Created for the Cold War, security institutions, policies, and systems focused on maintaining global stability. Nuclear conflict was a real and immediate possibility. Other than strategic air and naval forces, US military would primarily operate within declared war zones operating overtly under United States Code, title 10.

These legacy systems are problematic for a dynamic world of global competition between nuclear-armed great powers where full-scale war is limited but competitive acts—intelligence, cyber, information, space, maritime, and surrogate/proxy activities—will be routine. In this "gray zone"—the normal state of affairs between nations when not at war—legacy Cold War institutions and systems constrain SOF as a tool of national power. For the twenty-first century, SOF ability to operate outside war zones agilely in the emerging global environment would increase its utility to policy makers. To do this, a paradigm shift of the sort that occurred in the late 1940s, with the passing of the national security act of 1947, would be a good first step.

Conclusion

The twenty-first century will be singularly challenging for the United States and the world order it helped create. Complex factors are changing nearly every aspect of nations, institutions, and people's lives. Powerful nations (e.g., Russia and China), rogue nations, and nonstate groups seek to undermine or displace the United States. The emerging operating environment is complex, highly lethal, and one where anyone can access advanced technology and have "statelike" capabilities. This is the world of the "The Convergence." By 2030, what capabilities can a "mere" guerrilla force possess? The possibilities are limitless and troubling.

The years ahead will test the United States. The US military will be critical in countering nations in competition short of war, to prevent war, and, if necessary, to wage war in the event of conflict. US SOF will be at the forefront to support national policy and the joint force. Starting now, SOF must "harden" to face the most dangerous threat: the state actor. It is clear where enemy capabilities are heading, and, knowing this, SOF must prepare to meet this coming reality.

Endnotes

1 This quote derives from a speech Kissinger gave to the author's unit.
2 For a deeper exploration of this idea see, Ferguson, Niall. *The Square and the Tower: Networks, Hierarchies, and the Struggle for Global Power*. Penguin Books, 2019.
3 Thompson, Amy. "SpaceX Launches 60 Starlink Satellites on Thrice-Flown Rocket, Sticks Landing." *Space.com*, Space, 24 May 2019, https://www.space.com/spacex-launches-60-starlink-internet-satellites.html.
4 For a discussion of the role of China's Strategic Support Force see "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," US Department of Defense, 2019.
5 China in Space: A Strategic Competition? US-CHINA Economic and Security Review Commission, https://www.uscc.gov/hearings/china-space-strategic-competition.
6 Garretson, Peter. "Space Force Defenses Must Stretch to the Moon." *TheHill*, The Hill, 5 Aug. 2019, https://thehill.com/opinion/national-security/456214-space-force-defenses-must-stretch-to-the-moon.
7 Freeman, Marsha. "China Opens a New Page in Lunar Exploration." *China Aerospace Studies Institute*, Air University, Jan. 2019,
8 *Global Strategic Trends: The future Starts Today*, 6th edition, United Kingdom Ministry of Defense, 2018. See discussion of urbanization trends and megacities pages 64-66.
9 Summarized in the "World Urbanization Prospects 2018: Key Facts" p. 2, United Nations, Department of Economic and Social Affairs Population Division "*World Urbanization Prospects*" 2018.
10 "World Urbanization Prospects," 16.
11 Dodaro, Gene L. "The Nation's Fiscal Health: Actions Needed to Achieve Long-Term Fiscal Sustainability," Testimony before the Committee on the Budget, US Senate, Government Accounting Office , June 26, 2019, https://www.gao.gov/assets/700/699992.pdf.
12 Dodaro, "The Nation's Fiscal Health," 3.
13 "Financial Audit: FY 2019 and FY 2018 Consolidated Financial Statements of the US Government," US Government Accounting Office. February 27, 2020, 35.
14 "Financial Audit: FY 2019 and FY 2018 Consolidated Financial Statements of the US Government," 157.
15 "Demographic Turning Points for the United States: Population Projections for 2020 to 2060," US Census Bureau, March 2018, 4-5.
16 "Demographic Turning Points for the United States: Population Projections for 2020 to 2060," 4.
17 Kosiak, Steven M. "Is the US Military Getting Smaller and Older? And How Much Should We Care?" Center for a New American Security, March 2017, 2-9.

CHAPTER 36

Few Weapons Are as Deadly as a Good Clock: Military Implications of 1:10^19 PNT

Robert G. Kennedy III

A soldier must shoot, move, and communicate

—US Army doctrine.[1]

Preface and Approach

The organizers of this book defined "strategic latency" as "the inherent potential of S&T to produce powerful tools capable of changing the balance of power." Fair enough. They elaborate: "we use the term 'strategic latency' to describe technologies that have significant potential to be transformed by a nation, group, or individual for strategic effects." This writer had thought of "strategic latency" as a portmanteau of "*strategic* surprise" (e.g., Pearl Harbor, Sputnik, or 9/11) combined with the concept of *latency* from epidemiology, or that which is inherent in technological shifts. These shifts, playing out over timeframes of four decades, more or less, usually surprised people with unanticipated/unintended consequences during the evolution of the innovation. Even the architects/inventors can be surprised and generally have little to no appreciation of the full ramifications of their invention.[2i] In the United States today, social media is the most salient example, an instrumentality turned against its owners by adversaries, like the airliners of 9/11 were.

What might special operators have to deal with by 2050? To see one facet of this possible future, we turn to the humble watch, in particular, the emergence of distributed position, navigation, and timing (PNT) infrastructure at the $1{:}10^{19}$ level, made possible by quantum metrology. ("Watch" is used in the same tongue-in-cheek sense that those pocket supercomputers are called "phones.")

This chapter is a work of synthesis. In it, we combine epidemiological and systems engineering approachs to innovation. Not all innovations succeed, as a look at the Dead Media Project illustrates.[3] How to sort the wheat from the chaff? This is the kernel of systems engineering. Assessing the future is less about verification than validation—*verification* seeks to answer the question, "did we build the thing right?," whereas *validation* answers the question, "did we build the *right thing*?" The answer to the second question cannot be known for a long time. Despite the breathtaking change in human affairs since the Industrial Revolution, certain constants exist that we can learn from, to put bounds around what our readers, including special operators, may expect, and by when.

i For example, Alexander Graham Bell imagined the telephone as a means to bring high culture, such as live music concerts, to people in the hinterlands (i.e., a bit like cable radio today). Because industry could not imagine large numbers of women working in nondomestic or technical roles, the first telephone operators were teenage boys who turned out to be foul-mouthed terrors. It took no time for the nascent phone industry to fix that mistake by replacing the boys with much more responsible well-mannered people, i.e., cultured middle-class women. Additionally, without doubt, Bell did not imagine phone sex numbers.

The Nature of Technological Revolutions

Historical Overview and Examples

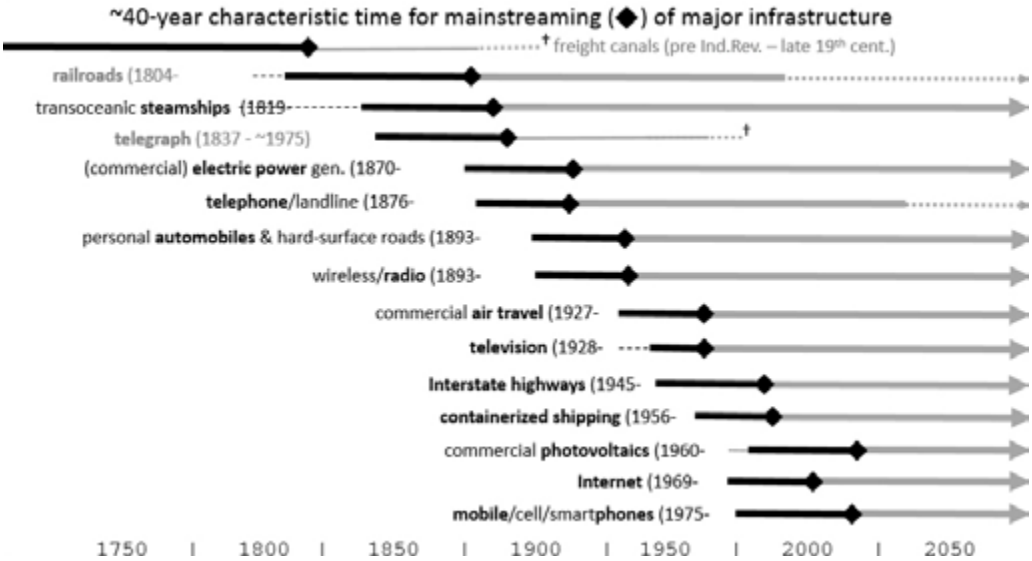


Figure 1. 40-year characteristic time for mainstreaming (◆) of major infrastructure in the United States.[4]

Figure 1 illustratres both a common *timescale*, 40ish years, from invention to widespread adoption ("mainstreaming") and that the *timing* (sequencing, phasing) of the political and economic impacts is predictable. Cesare Marchetti's studies of long economic cycles and diffusion of innovation and Arnulf Grübler's examination of diffusion of infrastructure showed these phenomena follow *logistic curves*.[5] In addition, there is *network effect*, also known as "Metcalfe's law," in which marginal value of innovation grows as N-squared. Fax machines in the 1980s are a good example of this law.[6ii] Full appreciation of a revolution often occurs only a considerable time after its inception, as noted in the footnote about Alexander Graham Bell and the telephone.

About the S-Curve, and Regions on It

Where did "learning curve," or "experience curve," come from? It started with an obscure paper in Franklin D. Roosevelt–era sociological agronomic research. A 1943 study of the adoption of hybrid corn seed in Iowa by Bryce Ryan and Neal Gross solidified prior work on diffusion into a paradigm that would be cited consistently in the future, in numerous contexts, and enter common speech.[7] The study also introduced terms such as "early adopter."

ii "An example put forth by Rogers in *Diffusion of Innovations* was the fax machine, which had been around for almost 150 years before it became popular and widely used. It had existed in various forms and for various uses, but with more advancements in the technology of faxes, including the use of existing phone lines to transmit information, coupled with falling prices in both machines and cost per fax, the fax machine reached a critical mass in 1987, when "Americans began to assume that 'everybody else' had a fax machine."

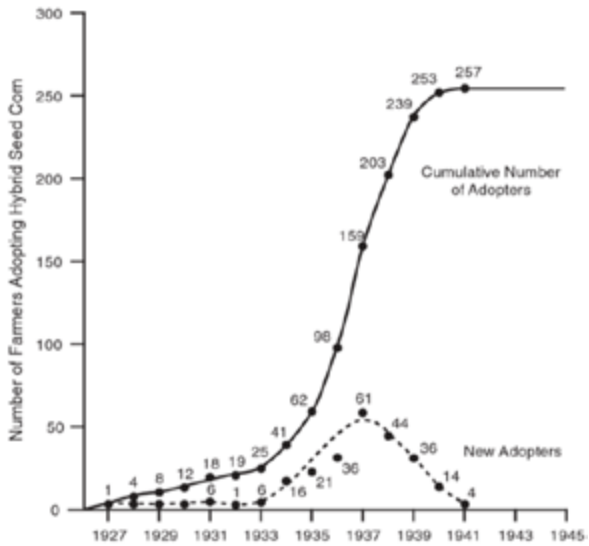
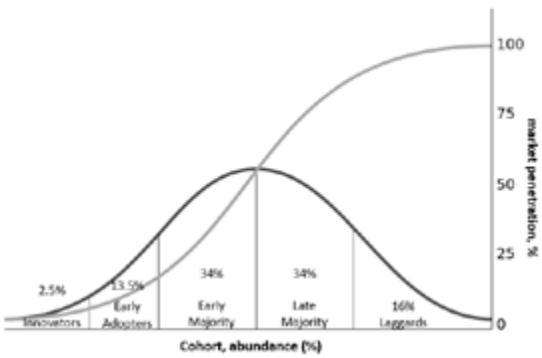


Figure 2. Sigmoid, or "S," curve, introducing social terms from Ryan & Gross (1943).[8]



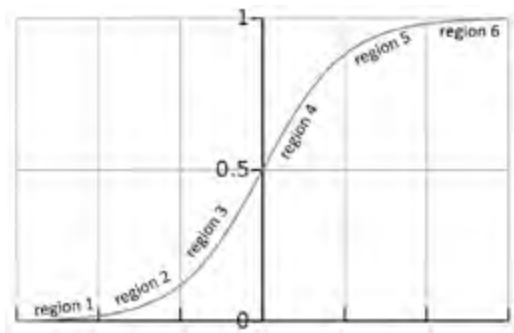


Figure 3. Sigmoid curve or "S-curve," with social cohorts from Ryan and Gross, left.
Innovation cohort is dark gray, market penetration in light gray. Figure 4. Regions on the logistics curve, right.[9]

As early as 1890, in *The Laws of Imitation*, Gabriel Tarde described the spread of new ideas through "imitative chains" and "imitative contagion."[10] He identified three main stages by which innovations spread:

- The first corresponds to difficult beginnings, during which the idea has to struggle within a hostile environment full of opposing habits and beliefs;
- The second corresponds to the properly exponential growth of the idea, with $f(x) \alpha 2^x$;
- The third is logarithmic, with $f(x)=\log(x)$, corresponding to when the impulse of the idea gradually slows down while, simultaneously, new opponent ideas appear. This halts or stabilizes the progress of the innovation, which approaches an asymptote.

Human experience progresses naturally from past to future. We resist noticing changes and altering our perception of the world. We typically do not appreciate where we are on the sigmoid curve. (Consider for example, the "Duckweed Problem," in which a body of water is being overtaken by the fast-growing aquatic weed. At only 10 percent coverage, say, an unscientific observer does not realize the lake is only three doublings away from ecological crisis.) As a result, we tend to emphasize past behavior of the curve and not look ahead to its changing nature.

In *region 1* of Figure 4, the innovation has occurred, but life stays the same. There is not enough absolute change to be observed by ordinary people. Consider the Human Genome Project (Figure 5), which was initially projected to take 100 years. Doublings existed, but they were not recognized, since doubling a small number yields a result that is still small.

In *region 2*, change is detectable by experts but not recognized as exponential, even though it is and always has been exponential, like all organic processes. The introduction of a "better mousetrap" stimulates an enormous amount of research and development, which leads to dramatic improvements in quality and quick reductions in unit cost. Hence, the terms "learning curve" or its inverse, "experience curve," are synonyms for "logistic curve."

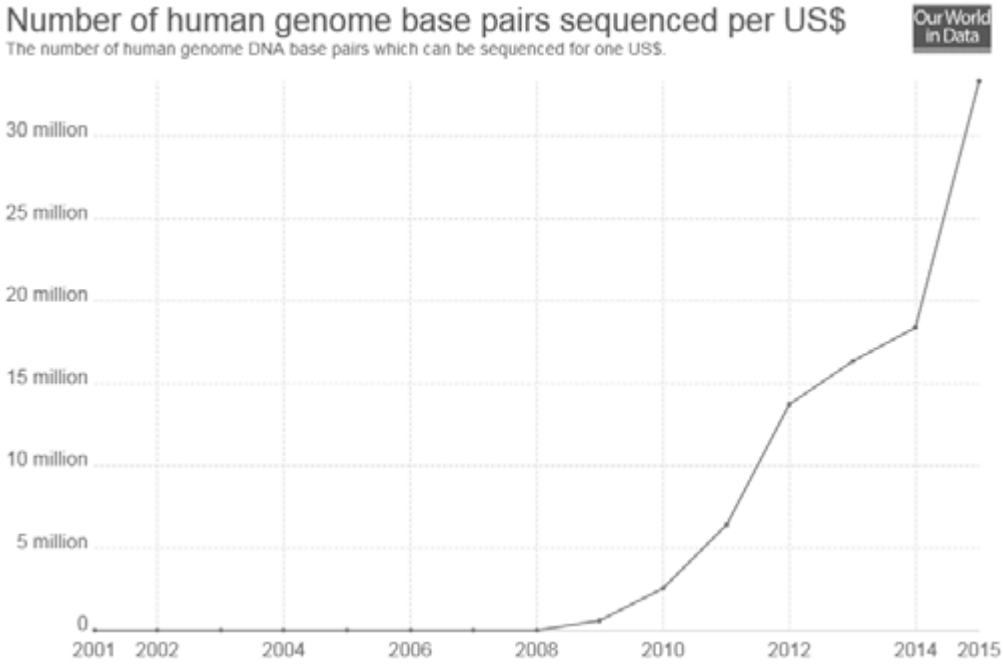


Figure 5. Gene sequencing on logistics curve.[11]

Explosive exponential growth is the theme in *region 3*.[iii] The investments in region 2 lay the groundwork for a period of rapid industry growth. Everyone, including nonexperts, recognizes the phenomenon, much like the growth of the stock market in the years before October 1929. There appears to be an infinite amount of work to do. Production capacity to meet the demand is limited by hiring and training constraints. Halfway between this region and the next, the savvy observer notices growth is slowing 1 or 2 doublings before the midpoint, which is 1 doubling period away before everyone really notices. Easy opportunities for product improvement or cost reduction ("low-hanging fruit") become exhausted. At the far end of this zone, there are no margins because every penny of cost is being wrung out of production, like $1 solar power or $2-per-gigajoule fracked gas. Only bottom feeders are hiring.

Region 4 spans from the inflection point halfway to saturation. The derivative (slope) of the curve is maximum at the inflection point. It forms a normal distribution that has a fairly narrow width, on order of two doubling periods (half-width is one doubling period). The rate of growth in absolute terms begins to invert (slow down) after the inflection point then crash because the product or process are in widespread use with few remaining potential new customers. Half the workers are laid off every doubling period. The only new starts are extremely low-margin heroic schemes to give the increasingly idle stranded capacity something to do, like the Depression-era Works Progress Administration (WPA) projects.

Region 5 is everything after that, an exponential decay to *Region 6*: saturation. Using the penetration of solar in the nation's electricity sector as an example of this region, this author believes this level is equivalent to 40 percent of all generated electricity, say 2,000 terawatt-hours. This proportion may increase if a good method of storing electricity is developed. If that innovation comes before the crash, it would extend the life for the solar industry; if not, the carpetbaggers will clean up, as they did after the stock market crash of 1929.

With respect to the technology that is the subject of this chapter—quantum metrology enabling PNT at the 10^{-19} level—this writer assesses humanity is just entering region 2.[12] At this level, especially as a ubiquitous distributed infrastructure, PNT should be considered still *latent* with full *strategic* effects yet to play out and become visible.

Time and Space

The Admiralty and the Longitude Problem, or, Few Things in Life Are as Useful as a Good Clock

A clock is nothing more than a way to count beats. First, find a simple local physical phenomenon—be it the falling of a droplet of water, the swinging of a pendulum, the staccato oscillation of an escapement, or the buzzing of a crystal of quartz. Next,

iii As a result of the COVID-19 pandemic, a lot more Americans have developed a feel for this phenomenon.

relate that counting to an objective external phenomenon, such as the motion of celestial bodies. The key is that the external phenomenon be *regular*—reasonably frequent and observable everywhere—and the local phenomenon be *reliably repeatable*, regardless of variations in local conditions such as heat/cold, altitude, humidity, or motion. The combination is called *frequency stability*. Put the two together, and you have a clock. (In physical terms, the clock mechanism is its own reference frame; so without the external relationship, you have a metronome.)

Centuries ago, hundreds of seafarers per year died as a direct or indirect result of navigational error. While mariners have known how to determine their latitude for at least three millennia, utilizing a variety of simple astronomical devices, doing the same for longitude eluded all until three centuries ago. At that time, the best clocks in the world, based on the anchor escapement mechanism, were accurate to 10 seconds per day, or roughly about one part in 10,000 ($1{:}10^4$).[13] In response to the Scilly disaster of 1707, in which the Royal Navy lost four top-of-the-line warships and at least a thousand sailors because they did not know where they were and crashed into a submerged hazard, the British Admiralty established the Board of Longitude, and offered £20,000 prize[iv] to solve the longitude problem.[14]

Unlike the simple exercise in geometry with celestial bodies to find one's position in the north-south direction, finding one's position in the east-west direction boiled to a problem of time, to wit, *measuring* time to an unprecedented degree of accuracy. The solution was a marine chronometer, i.e., a ruggedized clock suitable for oceangoing sailing ships, precise to better than one part in a million ($1{:}10^6$). Such a clock loses about one second every 12 days. These machines became *ubiquitous*—one essential feature of a true technological revolution—when, by the mid-1700s, the autodidactic genius John Harrison had shrunk the size of the instrument from bigger than a steamer trunk (the "H1") to a large pocketwatch (the "H4"). (Along the way, by necessity, he invented numerous mechanisms still in use today.)

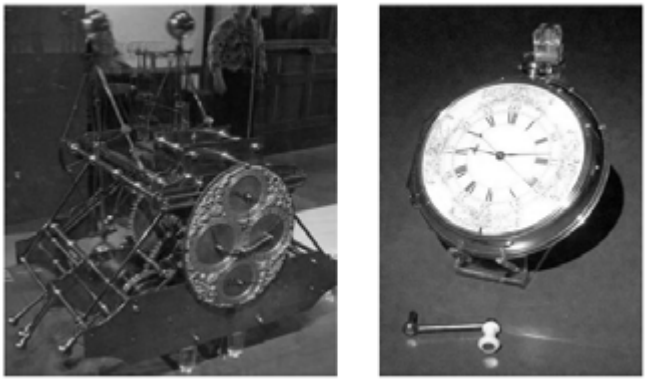


Figure 6. Harrison's H1, left, and H4, right.[15]

Britain's world-spanning empire was based on its navy, for which no real rival existed for well over a century.[v] Had Napoleon Bonaparte come from a naval instead

iv Equal to $3 million today; for "determining longitude within 30 nautical miles (56 km; 35 mi)."

v Another world-spanning maritime commercial power protected by the seas; that is, the United States.

of a (land-based) army background, he might have been more appreciative of another nautical innovation of the time, steam power, as (apocryphally) proposed to him by the American Robert Fulton, and history would be different. (Napoleon did commission Fulton to build the world's first submarine, the man-powered *Nautilus*, which sailed the Seine in Rouen in 1800.)[16]

A Brief History of Timekeeping

At the turn of the century, just as Guglielmo Marconi was developing his radio, a Yankee pocketwatch mass produced by the Waterbury Clock Company could be had for one dollar[17] (a lot of money at the time; about a day's wage for a skilled worker). On the eve of World War I, the winding stem of the watch was relocated from the 12 o'clock to the 3 o'clock position, with two metal loops added to the outside case to hold straps, and the wristwatch was born. By the time radio became mainstream between World Wars I and II, the nature of the oscillating heart inside a timepiece had changed from mechanical (escapement) to electronic (vibrating quartz crystals); further, a timepiece's precision had improved and form factor had shrunk dramatically again.[18] More important for our purpose, by the 1960s, the cost of such precision had dropped so far that a wristwatch by Timex (successor to Waterbury) could still be had for a dollar. (By this point, after six decades of inflation, about an hour at minimum wage, a truly democratic price point.) On the fashion front (i.e., not "cheap"), the Swatch (contraction of "second watch," "not one's primary watch") was developed in response to the "quartz crisis" of 1970s and 1980s, when Asian companies built giant machines to produce high-precision digital wristwatch guts by the million at an extremely low marginal cost, which allowed digital watches to outsell traditional mechanical watches made by European companies.[19]

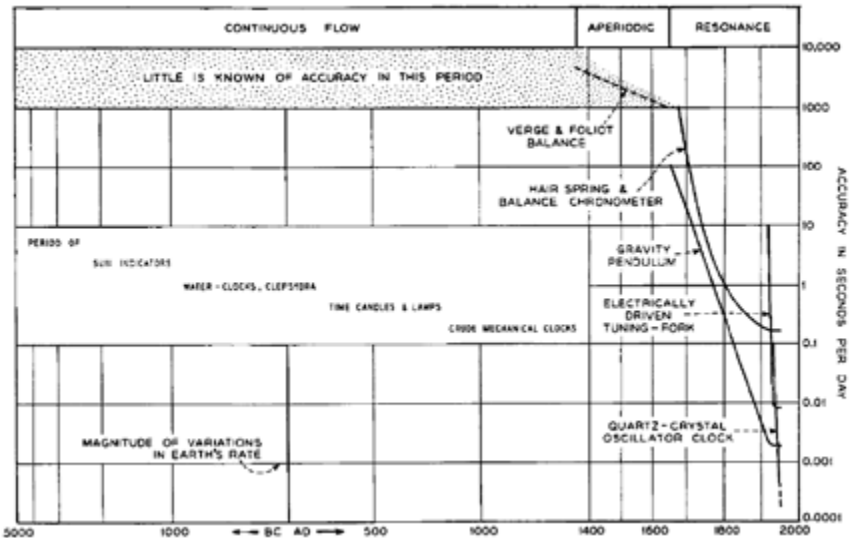


Figure 7. Accuracy of timekeeping through history, from Warren Marrison's 1947 Gold Medal address to British Horological Society in London.[20]

Shortly after World War II, about the time Warren Marrison was giving his Gold-Medal–acceptance address to the British Horological Society for his seminal work on quartz oscillators, Isidor Rabi, one of the Manhattan Project physicists, suggested that a clock could be made based on atomic transitions. A decade later, away from hoi polloi, scientists at the National Institute of Standards and Technology laboratory in Boulder, Colorado and elsewhere learned to measure vibrations of molecules and, then, vibrations of electron shells around atoms. Step by step, the state of the art in timekeeping precision progressed by six more orders of magnitude over Harrison's achievement, to $1{:}10^{12}$, or one in a trillion. Such a clock loses about 1 second in 30,000 years, about five times longer than all recorded history. About the time that cheap Timex watches appeared on people's wrists specialized, atomic clocks based on cesium became commercially available, for use as industrial calibration standards, to coordinate the machines underpinning humanity's increasingly complicated interwoven global society and to support the calculations that led to the Moon landings. These clocks were at the heart of the first generation of navigation satellites (hence the old name "Navstar") in the Global Positioning System (GPS).

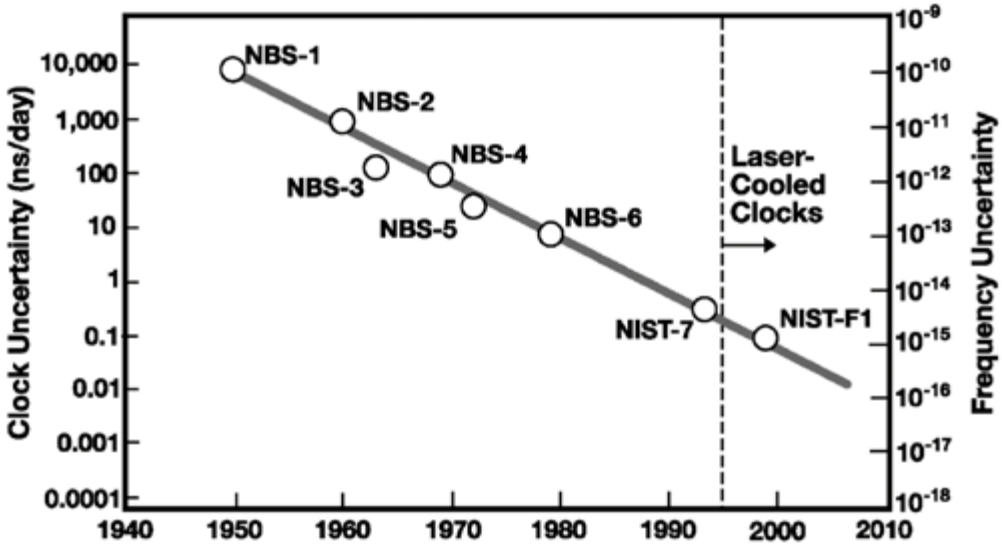


Figure 8. Comparison of atomic clocks at National Institute of Standards and Technology (NIST) since World War II.[21]

A generation later, by the time the 1989 Nobel Prize in Physics was awarded to Norman F. Ramsey for developing atomic clocks, accuracy had improved several orders to a level of $1.7{:}10^{15}$, or 2 parts in a quadrillion. Such a clock loses about 1 second in 20 million years, not as far back as the dinosaurs, but long before humans, or even hominids, appeared on the scene.

Optical transitions are even quicker than electronic ones. Therefore, devices based on optical phenomena promise to be even more accurate by an order of magnitude

or two, which places that lost second before the dinosaurs, or even before the emergence of photosynthesis.

All the foregoing occurred in the realm of pretwentieth-century classical physics, the science pioneered by Isaac Newton for the macroscopic world that we can see. "Quantum" is a term used to distinguish phenomenon that operate in the subatomic world according to the principles of quantum mechanics (Werner Heisenberg) and relativity (Albert Einstein). Quantum devices are emerging that have demonstrated a frequency stability in the lab of 1 part in 10^{19}.[22] Theoretically, a clock running on this principle (which does not exist yet) would lose about 1 second in 300 billion years, 20 times longer than the age of the universe.

What can practically be done with a quantum clock? We can attempt to forecast the effect of precision measurement in time by analogy with the known and soon-expected effects of precision measurement in space presented in the next section.

A Brief History of "Spacekeeping"

Immediately after World War II, people were considering how to obviate expensive terrestrial infrastructure with satellites in space. For example, in 1945, Arthur C. Clarke (not yet famous) invented[23] the geosynchronous communications satellite ("comsat"), revealing his novel idea to the world[24] in a hobbyist magazine. A year later, the obscure *R and D* department (later to become famous as the RAND Corporation) of the Douglas Aircraft Company wrote a report for the US Army Air Force[vi] about stationing surveillance assets ("spysats") in space.[25] In the early 1960s, Soviet scientists in the OKB-1 design bureau of the legendary Chief Designer S. P. Korolyov developed the *Molniya* ("Lightning") series of telecommunications satellites[26] flying in eponymous orbits to obviate the expense of long-distance landlines.[vii] Using advanced technology to bypass traditional costly infrastructure becomes important to our narrative later.

GPS is fundamentally nothing more than a bunch of really good clocks. In the early 1990s, positioning from the GPS constellation ("satnav") for military users provided a precision (hence "P-code") of about 30 meters (m), while satnav precision for civilians using the same system was deliberately degraded to ~100 m ("selective availability" or "SA"). In 2000, the US government switched off SA, making military-grade positioning freely available to all users with a compatible device. No doubt the emergence of competing systems (e.g., Soviet Union's/Russia's GLONASS[viii] and the European Union's Galileo), had much to do with the decision (not to mention China's BeiDou or Japan's

vi Prior to its spinoff as a coequal branch of the US military in the Harry Truman administration's National Security Act of 1947.

vii From the Soviet Union's perspective, being situated far to the north, a ***Molniya*** orbit provides a viable alternative to out-of-view geosynchronous earth orbit (GEO) over the equator. Both orbits are highly inclined to serve high latitudes and highly elliptical to maximize long dwell times over the service area at apogee. Unlike single comsats in GEO, continuous coverage must be provided by multiple birds in sequence like a carrousel.

viii For ГЛОбальная НАвигационная Спутниковая Система, or globalnaya navigatsionnaya sputnikovaya sistema.

satnav augmentation system QZSS,[ix] or regional systems such as India's IRNSS[x]). The trend of redundant competing systems will also only accelerate in a multipolar world.

Since the events described above, the basic precision of satnav without augmentation has improved to about 10-15 m. In the late 1990s, static ground-based systems emerged that appropriated the nominal GPS signal, averaged out errors over time, and rebroadcast another, better signal within a limited area, such as airports, at first providing ~1 meter accuracy, but recently with centimeter (cm) accuracy.

In practical terms for a motorist:

- 100-meter accuracy is enough to know which major highway or city block one is on;
- 30 meters is enough to know which cross street is coming up—and, hence, when to slow down for the turn—but not enough to actually make the turn with eyes closed;
- 10 meters is enough to make the turn successfully if no other cars are around;
- 1 meter is enough to make the turn into one's own driveway and still stay out of the neighbor's front yard; or,
- 1 centimeter is enough accuracy to do confidently all these things with eyes closed (or even asleep)—that is, under full automation. The Society for Automotive Engineers developed a humorous mnemonic for the five levels of automation [xi]

For nonhuman operators (i.e., robots):

- 1-meter is enough to land a commercial plane on autopilot, which was one of the first uses of differential GPS; and,
- 1 meter is just about enough for an airborne drone to deliver a pizza through the correct apartment window.

What could a robot do with wide-area 1-cm accuracy? What does it portend for special operators when virtually everyone has such capability, when the change has fully proliferated throughout all infrastructure and every environment is permeated with it, like author Vernor Vinge's "locators"?[27]

ix For Quasi-Zenith Satellite System.

x For Indian Regional Navigation Satellite System.

xi Level 0: Automated system issues warnings but has no sustained vehicle control.
Level 1 ("hands on"): Driver and automation share control of vehicle.
Level 2 ("hands off"): Automated system takes full control of vehicle (accelerating, braking, and steering).
Level 3 ("eyes off"): Driver can safely turn attention away from driving.
Level 4 ("mind off"): As above, but no driver input required for safety (i.e., driver may sleep or leave seat).
Level 5 ("steering wheel optional"): No human intervention is required at all (e.g., robotic taxi).

At about the same time as the proliferation of GPS into civil life, soon after the end of the Cold War, space-based photoreconnaissance, previously almost exclusively a military province, also underwent technical, economic, and political revolutions in resolution, response time, and, most important, cost (free) and availability (ubiquitous). Almost exactly the same political dynamic occurred for space-based imaging as for satnav, at about the same time and for similar considerations: better to liberate a disruptive technology and hope to retain some control over its direction than to abandon the stage to other actors.[28] (This writer had the honor to be instrumental in that.[29]) Result? Companies like Google and Planet Labs provide (what once was) a fusion of satnav and military-grade imagery of any place on Earth, at near-real-time availability, all conveniently displayed (plus an admixture of near-real-time user feedback; see Metcalfe's Law) to three billion users[xii] on their pocket supercomputers (which they insist on referring to as "phones").

The Quantum World

For two identical clocks to keep the same time or "stay in phase," they must be in the same gravitational field. For ordinary everyday purposes, Earth's gravitational field is the same everywhere. But for sufficiently accurate devices, this assumption is not true. The pull of Earth's gravity falls slightly with altitude or increases slightly over mountains or toward the poles. The effect of gravitation also changes according to the speed of the clock if it is moving, as has been demonstrated to many decimal places in low earth orbit, such as in the recent "NASA twins" experiments.[30][xiii] Time, space, and gravity are just aspects of the same thing, the Einsteinian space-time continuum, connected by general relativity (GR). As a clock is moved faster, or up out of a gravity well, local time slows down. A clock up high runs slower than a clock down low, but until recently, this effect was not easily measurable. When atomic clocks on the big GPS satellites were operating at the one-in-a-trillion level based on macroscopic devices, their operators had to correct for local variation in the gravitational field using GR. Easy enough to do when you have an accurate enough clock.

This connection of time and gravity via GR works both ways. GR in the form of aerial "gravity surveys" has been used for decades by geophysicists to prospect for oil, minerals, or geothermal resources. Earth's seabed was mapped using satellites, detecting the subtle shifts in timekeeping aboard the satellite to find hidden mass concentrations, such as seamounts or chasms, below the waves. It has often been said that we know more about the moon above our heads than the ocean floor. however, the resolution of this underwater topography is constantly improving, with oceanographers announcing remarkable new discoveries almost every month. This is why Google Maps displays such pretty topography beyond the shore, rather than the featureless blue of globes a generation ago.

xii Almost half the world's population. Thus, in the middle of the logistics curve.

xiii Astronaut Scott Kelly is now a bit younger than his identical twin brother, Mark Kelly, on the ground.

This trend will only continue, but beyond the macroscopic and microscopic into the subatomic realm, wherein quantum mechanics rules. Recall that Harrison's H4 got a sailor to within 56 km of his true position. Today, with state-of-the-art 10^{-14} clocks, we can identify a difference in altitude of 3 m (10 feet), one story in a building, using GR. We call this fusion of time and space the quantum world, hence the term "quantum clocks." With quantum clocks at the 10^{-19} level, the entire surface of the Earth could be accurately mapped to better than 1-centimeter absolute accuracy.

Ubiquity and Decentralization

The famous "atomic clock" in Boulder, Colorado is a *centralized* system that broadcasts a time/frequency reference signal everywhere for terrestrial computer networks. The trouble with a central system is that communication can be cut or the central transmitter physically destroyed by hostile action. Likewise, GPS "birds" in space are big, about the size of a car. Satnav from space can be knocked off the air in a limited area on the ground by relatively low-power jammers; the platforms in space would be physically vulnerable as antisatellite (ASAT) capabilities continues to proliferate. After the United States, openly demonstrated ASAT capability, three countries—Soviet Union/Russia, China, and India, in that order—followed suit. There is little doubt ASAT capability is much more widespread, either clandestinely (Israel is at the top of this writer's list) or latently by a dozen others, especially against targets in closer orbits.

The long secular trend of miniaturization continues in the satellite realm, too. Planet Labs operates hundreds of imaging satellites in polar sun-synchronous orbits, each occupying a "3U form factor,"[xiv] (i.e., no bigger than a loaf of bread). They provide "line scan of the entire Earth" once a day, at submeter resolution, replacing a capability once needing a bird the size of a bus. Various companies have announced grandiose plans for constellations of thousands or tens of thousands of satellites. Most of these birds would be even smaller *chipsats*. However, an essential difference of future highly precise timekeeping is that it will be *distributed*. This is not merely a difference in degree (i.e., quantitative) but in kind (i.e., qualitative).

Based on an invention about two decades ago, the first prototype chip-scale atomic clock (CSAC) was demonstrated by NIST, in an effort funded by DARPA to "*provide improved location and battlespace situational awareness for dismounted soldiers when the global positioning system is not available*" (italics added).[31] In 2011, atomic clocks on a microchip began to be manufactured in large numbers.[32] At just 16 cubic cm and 35 grams (a little over an ounce), Symmetricom's[xv] SA.45 miniaturized atomic clock is smaller than a York Peppermint Pattie, consumes a tenth of a watt, and cost $1,500 when introduced ($2000 now, but expected to drop to $200 in volume). It gains/loses half a microsecond per day (i.e., an accuracy of about $1{:}10^{11}$). A radiation-hardened

xiv NASA defines a 1-U cubesat as occupying a volume of 10 x 10 x 10 cm, or 1 liter.

xv Acquired by Microchip Technology Inc. of Chandler, Arizona.

(rad-hard) variant (Figure 9) made by Microsemi[xvi] is now qualified for use in space. Its makers anticipate eventual integration into a smartphone.[33]

Figure 9. Space-rated rad-hard chip-scale atomic clock.[34]

Phased-Array Radars (PARs) and Software-Defined Radios (SDRs)

The frequency (v), expressed in hertz (Hz), and wavelength (λ) of an electromagnetic wave is related by the simple equation: $v \times \lambda = c$ (the speed of light, ~300,000,000 meters per second). The higher the frequency, the shorter the wavelength (one handy memnonic is that light travels one foot in a billionth of a second):

- A 100-megahertz (MHz) signal—such as that received by a car radio—measures 3 meters from crest to crest.
- A 1-gigahertz (GHz) signal (for cell phone use) is ten times shorter—30 cm; about 1 foot.
- A 1-terahertz (THz) signal is a thousand times shorter—0.3 millimeter (mm)—about 7 sheets of paper—or 300 "microns" (µm; millionths of a meter)—and is called submillimeter radiation.
- Infrared (IR) radiation (i.e., heat) extends from about 1 mm to near IR at:
- The red end of human vision, roughly 0.7 µm, or 700 nanometers (nm, billionths of a meter); the blue end of human vision is about 0.4 µm, or 400 nm.
- Below this wavelength is ultraviolet (UV) radiation, extending down to about 10 nm, where it is called extreme (EUV).
- Below this is X-ray region, of increasingly higher energy, from "soft" to "hard."
- Note the Active Denial System, a sublethal directed-energy weapon sometimes nicknamed "pain ray," developed and fielded by the United States, operates at 95 GHz, or a wavelength about 3 mm.

xvi Also acquired by Microchip Technology Inc. of Chandler, Arizona.

Anyone who has been at an airport or on a big ship has likely seen a rotating metal radar dish in which the beam of radio-frequency (RF) energy is steered mechanically. Typically, these operate in the microwave region, somewhere between 300 MHz (1 m) and 300 GHz (1 mm). PARs accomplish this steering to an arbitrary bearing and/or elevation electronically, a process called "scanning." A series of static antenna are pulsed in sequence so as to emit a synchronized series of spherical waves that build up a considerable amount of RF energy by superposition, in effect an artificial beam pointing in the desired direction, as shown in Figure 10. In exchange for a tolerable loss of efficiency (some RF energy spreads uselessly in space), the physical response of PARs ("slew rate") becomes almost instantaneous because of the elimination of the massive slow mechanical steering apparatus.

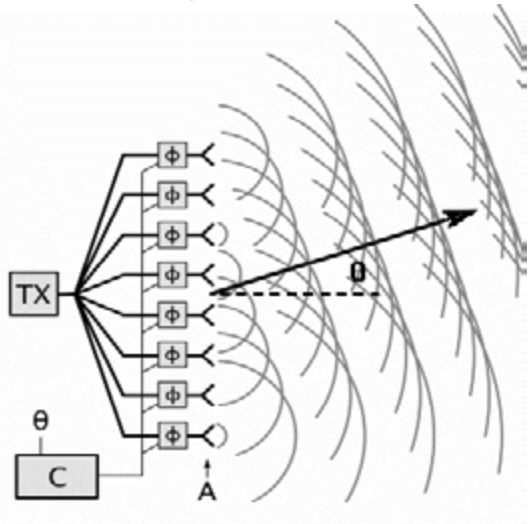


Figure 10. A phased array process.[35]

The phasing trick depends on precise synchronization, which is to say, good clocks. For a phased array operating at a given wavelength, the rule of thumb is that any errors in synchronization need to be no more than 1/10 that wavelength. For airport radars, this corresponds to a timing precision of three billionths to three trillionths of a second. Current CSACs on the market can already satisfy this. Though demonstrated in the lab over a century ago, PARs did not take off practically until the Cold War. They are well known to the military, especially for early-warning or battle-management applications. Complete multielement PARs, working in the 30-50 GHz range (i.e., centimeter wavelength), were implemented by DARPA on a single silicon chip in 2007. This leads to the next important piece.

Another technological development during the Cold War was SDRs, in which discrete physical hardware components—such as detectors, filters, amplifiers, modulators/demodulators, and mixers—are instead instantiated in *software*, i.e., bits not atoms. At around the same period, fractal antennas were developed both to get around the size and weight limitations of traditional antennae and because traditional fixed-length

antennae can best receive or emit only one wavelength and are less efficient at every other. SDR and fractal antenna made the mobile-phone revolution possible.

We now have all the pieces.

If 1-centimeter accuracy is enough to "drive" blindfolded, what services might be cheaply available when the timing component of PNT improves by *another six orders of magnitude* and, furthermore, becomes *distributed* and *ubiquitous*? Would people take a millionfold improvement in these combined technologies for granted, as they learned to do with computers and communication? Technological revolution or technological dead end? The answer depends on the degree of acceptance of the innovation and the uses (or misuses) to which the improvement is put. To see what we may become, looking in that "mirror darkly," we must turn to science fiction.[36]

Conclusion: Implications for the SOF in 2050

What You (or the Bad Guys) Might Do with Really Good Ubiquitous Clocks

Drone swarms have already been demonstrated, flying uncannily accurate formations in a series of high-profile public-relations stunts, such as the Opening Ceremony at the 2018 Winter Olympics in Pyeongchang, South Korea.[37] By 2050, this sort of demonstration will be old hat, and will probably be how most people will get their fast food delivered.[xvii] However, this writer has something more ominous in mind.

Since the days of the Manhattan Project, it has been known that small explosions can be coordinated to shape big pressure waves precisely. Back then, the key was timing the point detonations with small switches called klystrons. The idea is to coordinate multiple hits, each by itself sublethal, with distributed assets individually below the threshold of detection, into a simultaneous strike that is lethal, capitalizing on the n-squared scaling effect of multiple hits, as seen in trauma medicine.[xviii] The key for maximizing shock value is simultaneity, which, in turn, requires exquisite coordination. To the best of this writer's knowledge, an attack mode fully extrapolating this concept has been explored only in science fiction—for example, in Kim Stanley Robinson's *2312* (2012).[38] This writer conjectures (i.e., asserts without proof) the phenomenon of the shock effect of simultaneity exists across scales, analogous to

xvii A trend no doubt to be greatly accelerated by the COVID-19 pandemic.

xviii The Injury Severity Scale has a sum of squares in the calculation. "Baker and associates evaluated 2,128 victims of motor vehicle crashes over a 2-year period in Baltimore. For each patient, the anatomic areas with the highest AIS scores were tabulated. In analyzing these data, a nonlinear relationship was found, such that mortality increased disproportionately with AIS rating of the most severe grade. Also, patients with similar scores sometimes differed greatly in injury severity. For example, a patient with a ruptured spleen (AIS 4) and a pneumothorax (AIS 3) will have different survival probability, compared with a patient with an aortic rupture (AIS 5) and a rib fracture (AIS 2), even though they both have a total score of 7. So, a linear equation would not predict outcomes. Because the simplest nonlinear relationship in mathematics is quadratic, they applied this model to the data and found better correlation of severity and mortality. By taking the sum of the squares of the three highest AIS scores, the best correlation was achieved." See https://www.orthobullets.com/trauma/1055/trauma-scoring-systems accessed 25 Oct 2019, and http://www.acrm.org.my/ntrd/documents/literatures/1999.%20Trauma%20Scoring%20Systems%20%20A%20Review.pdf accessed 25 Oct 2019

Lanchester's laws governing small-unit combat.[39] A sufficient number of simultaneous attacks against a formation would get inside the target command's OODA[xix] loop.

The energy carrier need not be material—for targets within short range in a terrestrial environment, the attack can be conducted with energy, either as shock waves propagating through a medium (e.g., Joe Haldeman's "shatterguns"[40]—which could be implemented now with state-of-the-art clocks) or as directed radiant energy outright. The amount of energy contained in ionizing radiation is surprisingly small—a lethal dose (LD) sufficient to kill 90 percent of those receiving it (LD_{90}, 60 grays of radiation, times 70 kilograms for an average adult human) amounts to just 4,200 joules or 1,000 small calories (which is 1 large calorie, same as in a Tic Tac breath mint). This tiny bit of energy would not even noticeably warm up a cup of coffee.

Recall that the "pain ray" operates at 95 GHz, in the middle of the range of airport radars (and microwave ovens), and that existing CSACs with 1-part-in-100-billion precision are sufficient for synchronizing emitters in this range. The existence of these pieces, albeit separately, suggests an awful synthesis or fusion is already possible. This chapter conjectures it is only a matter of time before someone implement a "pain PAR" with SDR. One can further imagine such devices could be mass manufactured, borrowing techniques from the photovoltaic industry, particularly thin-film solar, which can be installed almost as readily as carpet or wallpaper. As unappealing as it is to contemplate a building, say, or vehicle that can remotely and soundlessly inflict pain on trespassers automatically (or heaven forfend, innocent passersby further off), the scenario gets worse.

Improving timing precision by another six to seven orders of magnitude, which has already happened in the lab, can transform the merely unpleasant into a truly lethal capability. Instead of 3-mm software-defined pain phased arrays (SDPPAR—needs a catchier moniker), are 3-*nano*meter (soft X-rays) emission networks possible? Compared to days of yore, when conversion efficiency of electricity into photons was on the order of a percent or two, light-emitting diodes have become highly efficient (and cost effective). Furthermore, the range of radiation that can be generated efficiently by solid-state LEDs continues to expand. A low-pressure mercury-vapor lamp now converts about 60 percent of its input to useful UV-C photons,[41] and even 300-nm UV would be a serious hazard to eyes and skin. While ionizing radiation is strongly absorbed by metal as well as air, limiting the putative weapon's range, long-wave ultraviolet can pass through sea-level air for quite a long ways, otherwise sunburns would not occur.

A helpful way to think of phase-coherent directed-energy weapons is "radio astronomy in reverse." Instead of gathering miniscule amounts of energy from a vast area concentrated into a useful signal, small amounts of emitted energy are coordinated from widely dispersed sources—perhaps even individually undetectable sources—in order to arrive at the target simultaneously with devastating effect, and with no warning and no fingerprints.

xix Short for "observe-orient-decide-act."

Initially manufactured as discrete components like CSACs are now, a mesh of SDPPAR nodes could be embedded in a thin-film fabric appliquéd to walls. Mostly photovoltaic in function, the substrate would generate and store electricity for the distributed nodes. PV generation might even be their ostensible purpose, totally unremarkable in the not-too-distant future, with the lethal-capability bit kept clandestine. Walls obviously can have a lot of surface area—some all-glass skyscrapers in London are notorious for melting plastic cars parked across the street.[42]

If one can process ultraviolet, one can certainly process light at visible wavelengths. One can imagine a change in absorbed scene could wake up the ever-watching array. As the absorbed imagery meets certain fuzzy criteria (e.g., silhouette, color) the weapon arms itself and, upon a close enough match, discharges. If the system were able to process sound (even though that is a longitudinal wave, not transverse like electromagnetic), then language detection is a possibility, making the biblical *shibboleth* real once again. Furthermore, these criteria could be messaged any time after installation as a "software patch," making the system completely protean.

Processing visible light in either direction means the weapon could project photons to form an arbitrary image, not just absorb photons to charge itself up. Perhaps obnoxious ubiquitous "active surface" advertising, or active camouflage, might be the path on the technological roadmap to this destination.

Further in the future, the devices will have gotten smart enough to self-bootstrap their internodal network after application (locating themselves in 3-space with respect to each other using just GR without the need for external references), like Vinge's "localizers." At that point, individual nodes might be small enough to pass through a nozzle; thus, a lethal energy-weapon coating could be sprayed on walls like shotcrete, and even later than that, sprayed on walls like Vinge's polka-dot paint[xx] in the hands of young hooligans, because hi-tech almost always proliferates to consumers in the developed world and then the developing world. This kind of graffiti would really send a message! Consider that such a capability as described could also process human gaits, which are as unique as fingerprints. Now imagine a two-way wanted poster that zaps its subject if he is unlucky enough to walk by it at the post office.

Imagine a milieu completely imbued with such automation, and then consider if that entire environment were to become hostile (like in the last installment of *Hunger Games*)[43] with the reader immersed in it, a *Durchseuchung*[xxi] of death.[44] Invoking Clarke's third law, such a capability would appear magical to the unsophisticated or unprepared recipient. It might fairly be called a "Finger of God."[45]

xx Vernor Vinge, *Marooned in Realtime*, St. Martin's, 1986. In this future sci-fi murder mystery, the "Low-Techs" used a graffito, "low tech don't mean no tech," applied in polka-dot spray paint, to let the detective know the antiproliferation regime of the "High Techs" was leaky and that one of the "High Techs" was cheating.

xxi "Infestation," a wonderful word to use at every opportunity.

Where SOF Might First Encounter this Phenomenon

Where might SOF encounter such state-of-the-art, yet distributed innovative lethal applications? The great powers would be the first to deploy them. But after the cat is out of the bag, then what? Based on this writer's personal experience building cutting-edge technology teams in east Africa, the entire continent could be early adopters.

Africa is the avant-garde of five great demassifications[46] of bureaucracies underway, leapfrogging sclerotic state systems that do not work anyway. It is the center of decentralization:

- Phone (the continent has leapfrogged landlines, going straight to cell)
- Banking (already done—mobile money)
- Roads (sidestepping with drones and novel yet simple three-word addressing schemes[47] to deal with the typical lack of physical addresses and the intractability of lat/lon to eight decimal places for ordinary people)
- Power and clean water (solar)
- Health care (essential community preventative health amplified with smartphone apps)

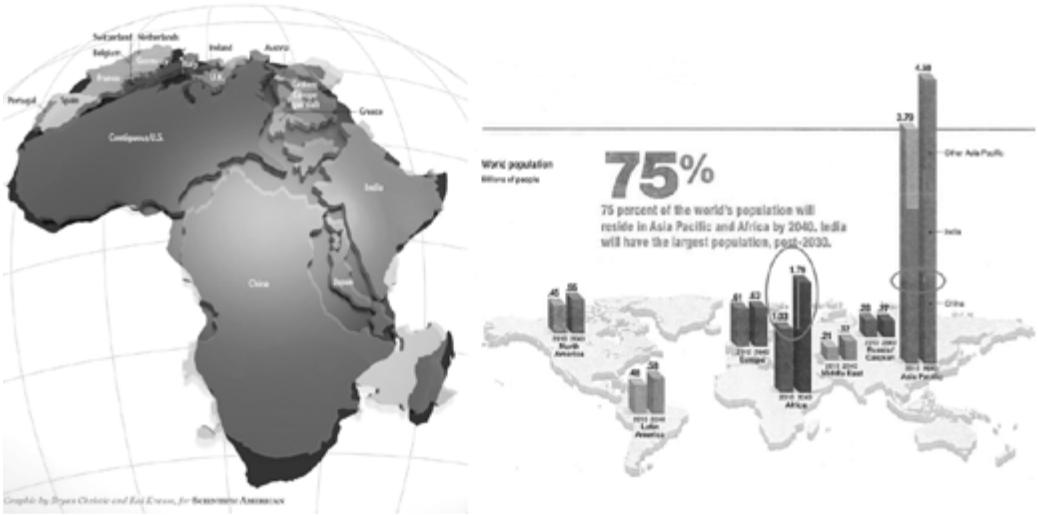


Figure 9. Africa is way bigger than many people think, left, and where most of the young people will be, right.[48]

By 2040, two out of three young people will live in Africa. Any enterprise not paying attention to the continent is by default not paying attention to the future. Africa has thousands of languages. Setting aside the former Soviet Union, China, and India, the African continent has the most space and the most scope for things to happen that would be of professional interest to the special operator. So, one can expect Africa is where conflict and other matters requiring the attention of special operators will be focused.

Recommendations

A far more detailed examination of technological progress in this seemingly unsexy but enabling area is warranted, with particular watches on:

- events in the commercial off-the-shelf (COTS) world that would change the environment,
- determination of the numeric threshold (by accuracy) that enables particular devices or operations, and
- what may be possible to engineer for military-only applications supported by a COTS economy.

Acknowledgements

This work benefited greatly from early review and substantive contributions by Mr. Kent Leonard, formerly of Bowditch Navigation Systems; Mr. Eric Hughes of Narthex; Mr. David Woolsey of the University of California, Berkeley; Dr. William "Ches" Cheswick, formerly of Bell Labs; and Dr. Dwayne A. Day of the National Academies Space Studies Board. I am in their debt; however, all mistakes are my own.

Endnotes

1 Owen, Austan R. "Shoot, Move, Communicate," US Army, February 28, 2012, https://www.army.mil/article/74635/shoot_move_communicate.
2 Marc Goodman, *Future Crimes*, Doubleday, 2015.
3 Dead Media Project, https://www.deadmedia.org/; Kennedy, Robert, "Dead Media Reloaded: A Hypothesis Concerning Writing Systems, Plague, and History," Philosophical Society/ORICL Lecture, Summer Quarter, 2004, http://ultimax.com/whitepapers/deadmediarev.html accessed 23 Oct 2019.
4 Graphic by author.
5 Cesare Marchetti, "Pervasive Long Waves: Is Society Cyclotymic?" Aspen Global Change Institute, 1996. Archived from the original (PDF) via Wayback Machine http://www.agci.org/dB/PDFs/03S2_CMarchetti_Cyclotymic.pdf on 31 Oct 2019; Grübler, Arnulf, "Time for a Change: On the Patterns of Diffusion of Innovation." Monograph # RR-97-3, International Institute for Applied Systems Analysis, Laxenburg, Austria, January 1997, reprinted from Daedalus, Journal of the American Academy of Arts and Sciences, from the issue entitled, "The Liberation of the Environment," Summer 1996, vol. 125, no. 3, pp. 19-42.
6 Holmlöv, Kramer, P.G., and Karl-Eric Warneryd. In M. Carnevale, M. Lucertini, and S. Nicosia, eds., *Modeling the Innovation: Communications, Automation, and Information Systems*, Amsterdam: Elsevier Science, 95-108 MR(E) 1990; Rogers, Everett. Diffusion of Innovations, 5th Edition. Simon and Schuster, 2003.
7 Ryan, B., and Gross, N. "The Diffusion of Hybrid Seed Corn in Two Iowa Communities," *Rural Sociology* 8(1): p.15-24, 1943.
8 Credit: Wikimedia Creative Commons License, modified by author, 2019. https://en.wikipedia.org/wiki/Critical_mass_(sociodynamics)#Fax_machine_example.
9 Credit for both: Wikimedia Creative Commons License, 2019, modified by author. https://commons.wikimedia.org/wiki/File:Logistic-curve.svg; https://commons.wikimedia.org/wiki/File:Diffusion_of_ideas.svg
10 Tarde, Gabriel. 1890. *Laws of Imitation*, translated from the second French edition by Elsie Clews Parsons, New York: Henry Holt & Company, Sept. 1903.
11 Credit: NHGRI Genome Sequencing Program, 2015, modified by author, 2019. https://ourworldindata.org/technological-progress; Wetterstrand KA. "DNA Sequencing Costs: Data from the NHGRI Genome Sequencing Program (GSP)," https://www.genome.gov/sequencingcostsdata, accessed 2017-07-11.
12 Keith Crane, et al, "Assessment of the Future Economic Impact of Quantum Information Science," Institute for Defense Analysis, August 2017.
13 Richard de Grijs, *The Importance of High-Precision Timekeeping*, IOP Publishing Ltd., November 2017.
14 Dava Sobel, *Longitude: The True Story of a Lone Genius Who Solved the Greatest Scientific Problem of His Time*, Walker & Company, 1995.
15 Credits: Wikimedia Creative Commons License, 2011. https://commons.wikimedia.org/wiki/File:H1_low_250.jpg; https://commons.wikimedia.org/wiki/File:H4_low_250.jpg
16 Burgess, Robert F. 1975. *Ships Beneath the Sea*. McGraw-Hill.
17 "Quality Timekeeping Since 1854," Timex, https://www.timex.com/the-timex-story/ accessed 22 October 2019.
18 Warren A. Marrison, "The Evolution of the Quartz Crystal Clock," *Horological Journal*, British Horological Institute, London, 1947, as reprinted in The Bell System Technical Journal, Vol. XXVII, pp. 510-588, copyright 1948, AT&T.
19 Simon Winchester, *The Perfectionists: How Precision Engineers Created the Modern World*, HarperCollins, 2018.
20 Credit: AT&T *Bell System Technical Journal*, 1948.
21 NIST, 2019.
22 Rachel Berkowitz, "Synopsis: A Time Crystal Without a Driver," https://physics.aps.org/synopsis-for/10.1103/PhysRevLett.123.210602, accessed 26 Nov 2019, in re: Valerii K. Kozin and Oleksandr Kyriienko, "Quantum Time Crystals from Hamiltonians with Long-Range Interactions," Phys. Rev. Lett. 123, 210602, 20 November 2019.
23 Arthur C. Clarke, "Extra-Terrestrial Relays—Can Rocket Stations Give Worldwide Radio Coverage?" *Wireless World*. Vol. 51 no. 10. pp. 305–308, October 1945.
24 Arthur C. Clarke, "A Short Pre-History of Comsats, or: How I Lost a Billion Dollars in My Spare Time," 1966 essay in *How the World Was One: Beyond the Global Village*, Gollancz: London 1992, pp. 151-188.
25 Robert M. Salter, Jack Lipp, eds., "Preliminary Design of a World-Circling Spaceship," Douglas Aircraft Company Project RAND, Report No. SM-11827, 2 May 1946, found in John M. Logsdon, et al., eds., *Exploring the Unknown*, Vol. 1, NASA SP-4407, pp. i-viii, 1-16, 211-212. At https://history.nasa.gov/SP-4407/ETUv1.pdf, accessed 30 Dec 2019.
26 Boris Chertok, series ed. and trans. by Asif Siddiqi, *Rockets and People, Volume III, Hot Days of the Cold War*, p.454, NASA History Division, 2009.
27 Vernor Vinge, *A Deepness in the Sky*, Tor books, 1999.
28 White House, Presidential Decision Directive/NSC-23, "US Policy on Foreign Access to Remote Sensing Space Capabilities," Washington DC, 09 Mar 1994; declassified https://clinton.presidentiallibraries.us/items/show/12747, accessed 30 Apr 2019.

29 Robert G. Kennedy, "Memoir of a Fly on the Wall: Post-Cold War Conversion in Commercial Remote Sensing" (illustration and text). *Journal of the British Interplanetary Society—Space Chronicle*, vol. 59, supp.1, pp.29-37, ed. Dwayne A. Day. June 2006; United States Congress, "Commercial Remote Sensing in the Post-Cold War Era: Joint Hearing before the Committee on Science, Space and Technology and the Permanent Select Committee on Intelligence of the United States House of Representatives," 103rd Congress, Second Session, February 9, 1994. No. 124, Committee on Science, Space and Technology, US Government Printing Office, Washington DC.
30 Zimmer, Carl. "Scott Kelly Spent a Year in Orbit. His Body Is Not Quite the Same," *New York Times*, 11 Apr 2019. https://www.nytimes.com/2019/04/11/science/scott-mark-kelly-twins-space-nasa.html.
31 "Miniaturized Atomic Clock to Support Soldiers in Absence of GPS," UK Ministry of Defense, October 3, 2012. https://www.defense-aerospace.com/.
32 Willie D. Jones, "Chip-Scale Atomic clock" *IEEE Spectrum*, 16 Mar 2011.
33 UK Ministry of Defense, "Miniaturized Atomic Clock to Support Soldiers In Absence of GPS," https://defense-aerospace.com, 3 October 2012, accessed 22 October 2019.
34 Credit: Microsemi Product Catalog. https://microsemi.com/product-directory/embedded-clocks-frequency-references/5207-space-csac , accessed 20 Jan 2020.
35 Adapted from "File: Phased array animation with arrow 10frames 371x400px 100ms.gif," Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Phased_array_animation_with_arrow_10frames_371x400px_100ms.gif
36 Vernor Vinge, Rainbow's End, Tor Books, 2006; Lawrence Sanders, *The Tomorrow File*, Corgi, 1975.
37 Barrett, Brian. "Inside the Olympics Opening Ceremony World-Record Drone Show" 9 Feb 2018. https://www.wired.com/story/olympics-opening-ceremony-drone-show/.
38 Kim Stanley Robinson, *2312*, Orbit, 2012.
39 Davis, Paul K. 1995. "Aggregation, Disaggregation, and the 3:1 Rule in Ground Combat." RAND, Monograph #MR638. https://www.rand.org/pubs/monograph_reports/MR638/app.html#fn11.
40 See for example, the "six-pack of shatterguns" (cheap handheld shaped charges phased to induce hypervelocity turbulence) in Joe Haldeman, *Buying Time*, Avon, 1990.
41 Personal conversation with David Woolsey, 17 May 2020. See also http://davidwoolsey.com/AttO/AttO_blog/Entries/2020/5/20_Covid-19__Virus_vs_UV-C.html.
42 "'Walkie-Talkie' Skyscraper Melts Jaguar Car Parts," BBC News, 2 Sep 2013, https://www.bbc.com/news/uk-england-london-23930675.
43 Suzanne Collins, *Mockingjay*, Scholastic books, 2010.
44 Hans Zinsser, *Rats, Lice, and History: Being a Study in Biography, Which, After Twelve Preliminary Chapters Indispensable for the Preparation of the Lay Reader, Deals With the Life History of Typhus Fever* (Reprinted in 1963, 1996 (Black Dog & Leventhal Publishers), and 2007 (Transaction Publishers).
45 Vernor Vinge, *True Names*, Dell, 1981.
46 "Demassified Media," Oxford Reference, https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095709307 accessed 25 Oct 2019; Alvin and Heidi Toffler, *The Third Wave*, Bantam Books, 1980.
47 "What 3 Words," https://what3words.com/, accessed 22 October 2019.
48 Fischetti, Mark. 06 Jun 2015. *Scientific American*, https://blogs.scientificamerican.com/observations/africa-is-way-bigger-than-you-think/, left image; Chevron Strategic Plan, 2014, right image.

CHAPTER 37

Megacities and Special Operations Forces

Margarita Konaev

The future of US special operations forces (SOF) is intertwined deeply with the future of conflict and violence in the world's largest cities. By 2030, the United Nations estimates 43 megacities will exist around the world, where nearly 9 percent of the global population will live.[1] Megacities—cities with a population of over 10 million inhabitants—are the strategic centers of gravity and engines of economic growth for nations and even entire regions. Global cities like New York, Tokyo, Los Angeles, London, and Shanghai will lead the world in projected GDP because of their strong banking and finance sectors, international transportation and commerce hubs, massive entertainment industries, and technological innovation ecosystems. But megacities in the developing world are also claiming their place as emerging economic powerhouses. The high-quality talent pool in Bangalore, India, for example, has turned the city into a breeding ground for tech start-ups, while a single district in Lagos, Nigeria, can be a market the size of an entire country like Botswana.[2]

That said, unplanned urban population growth is overwhelming existing infrastructure. Many developing countries are struggling to provide their urban residents security, housing, water and sanitation, health, education, and functional transport networks. People continue flocking to Tehran, Iran, for instance, but the city's population now exceed its capacity by more than 70 percent—meaning that it can provide only 2.3 million of its 8 million residents with basic services.[3] Around 75 percent of homes in Kinshasa[i] are in slums. Meanwhile, Jakarta, Indonesia, with a projected population of 38 million by 2035, is likely to lose its status as Indonesia's capital because rising sea levels and poor water infrastructure management are effectively sinking the megacity.

As the world's urban population has grown, we have also witnessed an upsurge in violence and conflict in cities. Wars in Syria, Iraq, Yemen, Ukraine, and Gaza have led to immeasurable human suffering and the wholesale destruction of cities. Mass protests against government corruption, rising inequality, and unemployment have engulfed Baghdad, Beirut, and Santiago.[ii] The predominantly urban-based Mexican drug war shows no signs of abetting, whereas Brazil, plagued by extreme criminal violence, is home to 14 of the world's most violent cities. Cities across Europe and Africa have repeatedly been targeted by terrorists linked to or inspired by the Islamic State, while the threat from far-right extremism is on the rise across Western Europe and the United States.

i In the Democratic Republic of the Congo

ii In Iraq, Lebanon, and Chile, respectively.

The urbanization of violence and conflict around the world, coupled with the growing risk of natural disasters fueled by climate change hitting densely populated coastal areas, means US forces will increasingly be called upon to conduct a range of military operations in cities and megacities. US SOF—tried and true in hostile, denied, and politically or diplomatically sensitive envrionments—possess the core capabilities for achieving mission objectives in these urban settings.

The economic, political, and environmental significance of megacities, especially those located in strategically important regions for the United States, necessitate unique considerations and capabilities. The combination of high population density and high cell-phone penetration in urban environments, for instance, makes it difficult to operate unobtrusively. As such, SOF small footprint and experience in conducting low-visibility operations in contested environments is crucial for reducing the risks of detection and political blowback. Precise tactical-level training, unique technical and military capabilities, and detailed intelligence allow SOF to use force accurately and discriminately, which is essential in densely populated urban areas with a high risk of civilian casualties and collateral damage. Knowledge of cultures and languages and relationships with local allies and forces are also vital attributes, considering the diversity and complexity of human relationships and networks in large cities and megacities. Moreover, since they are often at the forefront of employing emerging technologies in battlefield conditions, SOF can leverage advances in military robotics, autonomy, and artificial intelligence (AI) to shape the operational environment in megacities in their favor.

Still, to say megacity operations will strain even the most prepared and well-equipped forces is an understatement. There are no historical examples of US operations in a megacity. Nonetheless, American urban operations in Manila, Huế, Mogadishu, Fallujah, Ramadi, Baghdad, and, most recently as part of the coaliton campaign against the Islamic State, Mosul and Raqqa[iii] reinforce the conventional wisdom about urban warfare being a protracted, resource intenstive, highly violent fight that results in massive military and civilian casualties and widescale destruction of cities.[4] But even Baghdad, with a 2003 population of approximately 6 million, does not compare to the scale, density, and complexity of massive population centers like Cairo, Dhaka, or Mexico City.[iv]

For SOF, the key challenges in megacity contingencies will likely be avoiding detection amid robust urban surveillance networks and large numbers of people eager to share any and all information online, sustainment in high-attrition conditions with limited logistical support, and crafting and disseminating impactful messages for psychological and information operations in a highly contested information envrionment. The SOF community is certainly familiar with these

iii Manila, Philippines; Hue, Vietnam; Mogadishu, Somalia; Fallujah, Ramadi, Baghdad, and Mosul, Iraq; Raqqa, Syria.

iv In Egypt, Bangladesh, and Mexico, respectively.

challenges. But the difference in scale between megacities and other urban areas can become a difference in kind.

Understanding Megacities

Special operations forces have two main sets of missions. The first are precision-strike activities that include the rapid deployment of forces for activities such as raids, kill/capture operations, hostage rescue, and strategic sabotage or to secure critical materials or facilities. The second set refers to special warfare, focusing on psychological operations and providing support to host-nation forces or nonstate actors whose political or military objectives align with US interests. Should a megacity contingency arise, each mission set can be used independently, in conjunction with, or in support of conventional military operations.

Regardless of the mission, operating effectively in cities and megacities requires an understanding of these environments. Military strategists and urbanism scholars typically conceptualize megacities as a "layered and interacting series of complex adaptive systems involving actions, interactions, and transactions," or as a "complex living organism with its own flows, networks, and rhythms."[5] Many frameworks exist for categorizing the factors that characterize the megacity environment and, in turn, shape the conduct and success of military operations writ large and special operations in specific. One straightforward approach, developed by the chief of staff of the US Army Strategic Studies Group, hones in on context, scale, density, connectedness, and flow.[6] The following discussion contextualizes these factors for SOF.

Context

History, culture, geography, and politics at the local, regional, and international levels are all important factors to consider when developing a contextualized understanding of a megacity. The economic development and population growth of cities—whether slow and planned or rapid and largely uncontrolled—influence the quality of urban infrastructure, the ability of the government to provide basic services, and the relationship between local and national authorities and the city's vulnerable and disenfranchised populations. These factors, in interaction with weak or corrupt state structures, economic crises, and high rates of unemployment and inequality, are often linked to urban unrest, violence, and conflict. Research on the 1992 Los Angeles riots, for example, shows the growth of the nonwhite community and inequality indicators such as nonwhite unemployment and the relative nonwhite homeownership rate correlated with the outbreak of riots.[7] Planning for special operations should therefore pay close attention to the socioeconomic, ethnic, racial, and political nuances that underpin the relationship between the local authorities, the population, and relevant threat actors.

The national, regional, and global significance of megacities is another significant dimension for SOF to consider. Seoul, for example, is a megacity where the US military has maintained a presence for over six decades and is required to protect

under the Mutual Defense Treaty with South Korea. Seoul is the political, cultural, and economic center of a key US ally, with more than 25.6 million people residing in the greater metropolitan area, including thousands of US citizens. In an event of a conflict with North Korea, actions needed to defend Seoul would span the entire spectrum of military operations.[8] Therefore, SOF will likely play multiple roles, including deploying as part of an early contingency response to assist with noncombatant evacuation of US citizens, intelligence and fires support, sniping, directing close air support, and countering weapons of mass destruction operations.

Geography affects the drivers of instability in cities and will influence the type of missions SOF could be called upon to execute. Large population centers are predominantly concentrated on the coasts, and, thus, they are more vulnerable to severe weather events; megacities like Shanghai, Dhaka, Calcutta, and Manila are some of the cities most at risk of flooding. Meanwhile, Tokyo, Los Angeles, Tehran, and Mexico City are particularly vulnerable to earthquakes. Rapid population growth, uncontrolled planning zones, and unsustainable environmental policies amplify the adverse effects of climate change, increasing the risk of natural disasters. Where US strategic or economic interests are at stake, SOF could be called to support humanitarian relief efforts and assist with the evacuation of US citizens.

Scale

The scale of megacities—the size of their populations and land areas—differentiates them from other urban environments and presents unique challenges to military operations and specific considerations for SOF. Most basically, urban warfare doctrine has traditionally called for isolating and enveloping a city, with forces advancing from the periphery inward to either besiege the urban area until the enemy surrenders or penetrate and storm the city to capture it if necessary.[9] The scale of megacity populations, however, raises serious questions about the feasibility of this approach.

Furthermore, as urban populations have grown, the land area covered by cities and megacities has expanded at an even higher rate. Urban sprawl is indicative of poor land management and inefficient energy consumption, a cause of pollution, and an amplifier of inequality and exclusion, with long-term potential to exacerbate social and political unrest and vulnerability to natural disasters and other health hazards.[10] Again, attempting to control physically a population of tens of millions of people spread over hundreds of square miles in a highly complex urban environment necessitates a military force the size of which few, if any, nations could muster, let alone sustain. For instance, the US Army Field Manual 3-24 Counterinsurgency, based on analyses of historical counterinsurgency campaigns such as the British in Malaya and Northern Ireland, advises a ratio of 20 to 25 soldiers for every 1,000 people in the area of operations. Based on this formula, counterinsurgency operations in a megacity of 20 million would require 400,000 soldiers.

Force-sizing calculations are perhaps less relevant from an SOF perspective. But the issue of scale is imperative. SOF are not structured for attrition warfare or

traditional force-on-force tactics and have limited assets of their own. Therefore, many SOF missions require support from other forces, including airlift, intelligence, communications, influence activities, medical, and logistics. The scale of megacities will inevitably strain the ability of the conventional forces to provide such support to SOF. This, in turn, will affect both SOF ability to operate effectively, and, more fundamentaly, policy decisions about whether SOF capabilities are appropriate altogether.

Density

Density is the overarching element of the urban environment, and it affects all types of operations in a megacity.[11] Both population and vehicle density limit movement and maneuverability even for small, agile forces. Millions of cell phones, laptops, tablets, and other web-enabled devices produce a signal-dense environment that creates bandwidth congestion, reduces the effectiveness of signals-intelligence collection, and complicates signals-based targeting.

As Russell Glenn puts it, density is reflected not only in "the number of structures, firing positions, avenues of approach, enemy, noncombatants, friendly force units, key terrain, and obstacles per cubic kilometer" but also in "the number of small unit engagements, troop movements, and interactions with noncombatants per minute within that space."[12] More structures, people, and activity also mean that situations change rapidly, requiring the unit commander to make decisions faster.[13] SOF are well trained for dynamic environments and high-paced engagements. But the cumulative effects of urban density can create a sensory and capability overload that should not be underestimated when planning the scope and contours of SOF megacity missions.

Connectedness

Modern cities are connected to their external environment (national and global) through a complex web of goods, services, people, information, and capital. These connections underpin national and global trade, commerce, finance, migration (legal and illegal), entertainment, and myriad other economic and social transactions across the world, all conducted at an ever-increasing pace and on a continuously growing scale. Cities are also connected internally through the urban and periurban network of roads, rail lines, waterways, and power lines, as well as through the flow of information enabled by the proliferation of cell phones and the widespread availability of internet access.

Real-time global news coverage by traditional media outlets deepens connectedness. The advent of social media, however, has fundamentally altered how people access, consume, and share information. The influence of traditional news networks is arguably declining compared to the growing power of "citizen journalists" sharing real-time content from their neighborhoods and cities to millions of followers on YouTube, Facebook, Instagram, and Twitter.

Damaging the conduits of physical connectedness between cities and their surroundings can have severe humanitarian consequences, which, in turn, likely

complicate military operations and SOF missions. In 2018, for example, the International Crisis Group warned that a United Arab Emirates–backed attack on the port city of Hodeida in Yemen would not only harm the city's population but also leave "an estimated 18 million highland Yemenis without supplies of staples like wheat and rice, or fuel, which Yemen imports by sea," predominantly though the Hodeida port.[14] Such disruptions to urban infrastructure and services have ramifications for special operations—from interruptions to communications and reliable intelligence to alienating local partners and undermining the legitimacy of core messages in psychological and influence operations.

The connectivity among cities enhances their economic and strategic importance. Combined with media saturation and the flow of real-time information, connectivity threatens SOF's ability to conduct discreet operations that deliberately reduce the signature of US involvement. These dynamics also have a negative impact on psychological and information operations in support of beleaguered governments. Indeed, state information efforts are now at a serious disadvantage when competing with individuals or opposing groups on social media.[15]

Flow

Flow is the movement of people, resources, or things into, around, through, or out of the megacity. Food, water, commodities, people, money, vehicles, information, and services all flow constantly, but these flows differ in terms of points of origin, length, duration, intensity, direction, and route, as well as with pulses within the flows.[16] Legal and necessary flows maintain and protect the healthy, sustainable functioning of the city. But cities also inevitably experience the illicit flow of guns, drugs, contraband, and trafficked people that special operations forces could be sent to block or interdict. Notably, illicit flows are often deeply embedded within licit flows. This is especially true in areas where criminal elements are thoroughly intertwined with the local economy and effectively control the slums, as is the case with organized crime and drug trafficking in Mexican cities such as Tijuana and Acapulco, Rio de Janeiro in Brazil, or Cali in Colombia.

Making sense of the various flow systems and understanding how disruption or even abrupt changes in flows can impact lives and livelihoods is essential when preparing for special operations in megacities and other dense urban areas. For instance, points where different flows converge, such as transportation hubs and markets, are both essential for the city's health and vulnerable targets for attack. Because of the density of people and the interconnectedness of urban structures and infrastructure, even rapid direct-action operations can interrupt normal flows, which risks exposing SOF to hostile local residents and political backlash. Restoring the flows in the aftermath of a terrorist attack, military action, or a natural disaster should be a priority and a key element of successful messaging in psychological and information operations.

SOF Capabilities and Challenges in Megacities

Special operations in urban environments vary significantly depending on the mission set and whether SOF are deployed independently or as part of a larger campaign. That said, SOF capabilities in both special warfare and more conventional surgical strike activities are uniquely positioned for a range of missions in megacities and other dense urban areas.

Small SOF units are organized, trained, and equipped for decisive tactical success. The intense physical and mental training of SOF emphasizes small-unit tactics and close combat for high-tempo engagements in austere environments with limited support. This training is relevant because success in modern urban warfare requires a high degree of skill and experience in small-unit tactics and specialized training for the physical and psychological challenges of intensive, highly violent, and fast-paced fighting in close quarters.[17]

Moreover, because of the nature of urban terrain, ground operations often become decentralized as forces needs to advance through the city's streets, alleys, and courtyards; enter buildings and underground tunnels; and proceed through a maze of corridors, stairways, and rooftops. These conditions demand leaders at lower levels of command to make independent decisions in complex and highly uncertain environments. Rigorous SOF training and mission rehearsals inculcate and reinforce unit cohesion, which enables discipline, trust, and effective leadership in high-risk situations. Therefore, SOF's operational formation, training, and core capabilities are well matched for urban environments.

SOF excel in adaptability, improvisation, and innovation, valuable skills in cities and megacities—constantly changing, adapting, and complex systems—particularly at times of unrest when atypical movements of people disturb normal rhythms and flows. These changes affect communications and transportation networks and exude pressure on the city's infrastructure. As the Mosul Study Group observed, "even by the hour of the day, operations physically changed the landscape, the populace migrated, and the electromagnetic spectrum adjusted."[18] These changes have immediate implications for situational awareness, intelligence, and targeting decisions. The urban environment is alive, and the ability to adapt, change course, and act quickly and decisively is essential for conducting effective operations.

Special operations forces are also distinguished by their close knowledge of the regional and local dynamics in their area of operations and their ties with local partners and proxy forces. Their expertise and relationships help secure intelligence, build trust in civil-military interactions with the local population, and execute synchronized and mutually supportive security-force assistance missions effectively. The premium on such capabilities is even higher in urban missions, considering the political, economic, social, ethnic, racial, religious, and cultural diversity of megacities and the complexity of social networks that characterize these massive population centers.

Finally, SOF, and particularly US Army Civil Affairs, Psychological Operations, and Special Forces have a deep understanding of the human domain and are well-suited for population-centric conflicts.[19] The presence of a sizable civilian population is the distinct feature of the urban environment and arguably the most challenging aspect of urban military operations. Understanding the demographic and cultural characteristics of the urban population is essential when planning operations. But managing the media and communications landscape and influencing the perceptions of different social groups is a highly complex undertaking. SOF interoperability with conventional US forces and ability to collaborate effectively with international allies and partners, as well as local partners and proxies, are critical for conducting psychological operations, administering civil affairs, and influencing the perceptions and behaviors of the local population.

That said, special operations cannot solve all security challenges in dense urban areas and megacities. Moreover, changes in the security and information environments point to potential contingencies in megacities for which SOF are not well prepared. As one example, Africa has seen a dramatic expansion of SOF activities since 2014. Special Operations Command Africa has about 1,000-1,200 operators and enablers in approximately a dozen nations with the primary goal of countering terrorism and enhancing stability by, with, and through African partners. Meanwhile, urbanization in Africa is unfolding at an unprecedented rate, with 14 cities expected to surpass the 10 million person threshold by 2050. And as Africa urbanizes, violence, conflict, and terrorism across the continent are also shifting to cities.[20]

Insofar as SOF remain active in Africa—even if their mission is merely to maintain a posture to respond to crises that could affect US citizens, interests, or security in a narrow sense—they will likely operate in cities and megacities. Special operations in African cities and megacities—where 75 percent of the population lives in slums, governance is contested, transportation and communication systems are fragmented, and unregulated urban growth has amplified a host of social, ethnic, and political grievances—will require significant sustainment and logistical support. There is, however, little sustained conventional US military activity in Africa, and, therefore, no conventional logistics network for SOF to leverage.[21]

SOF are among the most expeditionary of all military forces, capable of providing their own specific sustainment. In the twenty-first century, however, SOF have been engaged predominantly in mostly overt and highly kinetic counterterrorism activities in Iraq and Afghanistan, where conventional US forces maintained a sizable presence and provided extensive logistical support. Furthermore, the scale and density of megacities inevitably undermines SOF self-sufficiency. Surgical strike activities require fine-grained and continuously updated intelligence, precise and discriminate application of force, and reliable transportation for safe exit—all of which require close support. And as the Army Special Operations ADP 3-05 manual makes clear, deficiencies in supportability could affect the chances of mission success or even invalidate the feasibility of using SOF.[22]

Even with extensive logistical support, special warfare missions to train, assist, enable, and support a partner nation's security forces or nonstate actors in the context of urban military operations present additional challenges. Indeed, local partners and proxies often pay a terrible price when fighting in cities. For example, the Iraqi Counter Terrorism Service, a force of less than 8,000 elite troops built and trained by the United States, suffered up to 60 percent casualties in Mosul.[23]

Despite these challenges, the indirect approach to employing SOF through missions such as psychological operations and support to nonstate proxies or threatened governments via military training, is expected to see more play in the era of great-power competition.[24] Since Russia's annexation of Crimea in 2014 and the war in eastern Ukraine, NATO special forces have been working with SOF partners in the Baltic republics of Estonia, Latvia, and Lithuania as well as Poland to help train their forces to fight a war of resistance against a potential Russian invasion and occupation. US SOF are also working with these countries as well as Romania, Ukraine, and Georgia to help strengthen their national capabilities, including the development of their own special operations forces.

US national security decision-makers must better understand the limits and costs of special warfare missions in urban settings. In thinking about deterring and fighting a peer adversary like Russia, the US military has arguably not paid enough attention to defensive urban operations.[25] Defense has the advantage in urban warfare. But if the destruction of Grozny, Chechnya, and the indiscriminate bombardment of Syrian cities indicate anything, the costs of Baltic capitals like Tallinn, Estonia, and Riga, Latvia, mounting a defense against Russian aggression will be high.[26]

Finally, the complexity of SOF efforts to disrupt the enemy's ability to command and control forces and to influence the population will be magnified in megacities because of the sheer numbers and diversity of social groups and the intricacy of networks. Moreover, the high population density and connectedness of megacities combine with ubiqutous cell-phone use, widespread access to the internet, and the growing power of social media to create an environment ripe for misinformation, disinformation, and adversary influence operations.[27]

During Israel's 2014 Operation Protective Edge, for instance, Hamas took advantage of Gaza's high levels of cell-phone penetration to communicate with citizens about how to post messages in support of its campaign using a number of hash tags, including #GazaUnderAttack, #PrayForGaza, and #StopIsrael.[28] Fact-checkers, however, soon noticed some images from #GazaUnderAttack were from previous conflicts or from violence not involving Gaza.[29] While Israel maintains a relatively sophisticated public-relations apparatus, its messaging had a limited effect on the internationals stage, let alone in Gaza. Regardless of their profiency in psychological and information operations, SOF will likely face some of the same challenges governments currently experience in trying to maintain uniformity of message and keep pace with ongoing events in crisis situations in urban environments.

The Promise and Perils of Emerging Technologies

Special Operations Command can lead in operationalizing and deploying emerging technologies such as AI and machine learning to increase the speed and accuracy of intelligence processing and exploitation, enhance situational awareness, and improve decision-making in high-stakes environments, including megacity contingencies. In fact, the most high-profile example of AI on the battlefield to date, Project Maven, used computer vision and machine-learning algorithms to comb through hours of full-motion drone surveillance videos looking for suspected terrorists and insurgents to provide intelligence for drone strikes or special operations raids in the campaign against the Islamic State. Maven used SOF data to train their algorithms, and SOF integrated the technology into their forward-most locations.[30]

SOF are either already using or could potentially apply a number of promising technologies in urban missions. For one, cities produce immense amounts of data. With advances in big-data analytics, machine learning, image recognition, and natural language processing, military and intelligence analysts can exploit thousands of publicly available datasets for insights into the demographic, social, economic, and logistical characteristics of cities and their populations.[31] Naval Special Warfare elements and Army SOF are already using the Army's One World Terrain software that compiles detailed 3D digital maps from drone scans of specific areas of interest. The 3D software allows operators to do both line-of-sight and route analysis to avoid detection and battle-damage assessments to limit collateral damage, critical activities for urban operations planning.[32] Wall-penetrating radars, through-wall virtual imaging, and other see-through-wall technology that allow soldiers to detect people and potential threats inside closed rooms could be a game changer in an urban fight.[33] For command-and-control applications, AI could be used to fuse data from different platforms and military assets and distill into a common and comprehensive operating picture, which could improve and accelerate decision-making in time-sensitive missions.[34] Future advances in recommender systems technology could provide SOF with options based on real-time analysis of the battlespace, shifting computation support from reactive to predictive.[35]

Technology, however, can be a double-edged sword for SOF in urban environments. Facial recognition, biometrics, and signature management technologies already make conducting low-visibility military activities harder, and AI is likely to make it even more difficult for SOF to operate in the shadows during proxy conflicts or in other politically sensitive settings.[36] Remaining in the shadows will become effectively impossible in megacities. China, which has six of the world's 33 megacities, has an estimated 200 million surveillance cameras—four times as many as the United States.[37] Moscow, which already has 160,000 cameras watching the city's 12 million people, aims to integrate AI and facial recognition technology to be able to search for people on different wanted lists, to count people, and to evaluate behavior. Persistant urban surveillance, coupled with cell-phone penetration and real-time sharing of information

on social media channels, could deny SOF both the element of surprise and the ability to operate discreetly.

Furthermore, nonstate actors have proved capable of using civilian technology to their advantage in complex urban environments. During the 2008 Mumbai attacks, for example, Pakistani terrorists from Lashkar-e-Taiba used Skype, cell phones, and satellite phones to communicate with their commanders in Pakistan, who, in turn, provided real-time updates to the assualt team based on information circulated on Twitter, by satellite, and on cable news. The Indian forces were unable to cut communications between the assault team and their command-and-control node in Karachi, which allowed the terrorists to withstand the early loss of their team leader, evade Indian police and counterterrorism units, and besiege one of the world's largest cities for almost three days.[38]

In Mumbai, terrorists used easily available civilian technology to gain advantage in the city. But it is possible to imagine a scenario of armed groups or adversary states using the city's own technology to further their military or political objectives. Cyberattacks on critical infrastructure, such as Russia's attacks on Ukraine's power grid, can upend the city's normal flows, fueling confusion, fear, misinformation, unrest, and other unpredictable disturbances that could seriously undermine SOF ability to execute their mission in an already complex and dynamic environment. Planners must weigh the costs and benefits of relying on potentially vulnerable technologies in an environment where the terrain, the people, and the technology itself can quickly turn hostile.

Conclusion

Megacities both fascinate and deeply alarm the US defense community. This can partly be explained by the fact that, as the Chairman of the Joint Chiefs of Staff Gen. Mark Milley noted, "the Army has been designed, manned, trainned, and equipped for the last 241 years to operate primarily in rural areas."[39] While conventional US forces have seen their share of urban combat in the twenty-first century, they are not optimized for it. SOF, on the other hand, bring a range of core capabilities that have proved valuable in urban missions, including extensive training in small-unit tactics under physically and mentally grueling conditions, a small footprint in politically sensitive environments, and deep exterprise in the human domain.

But policy makers should also be cognizant of the limits SOF will likely face in megacity contingencies. First, although generally self-sufficient, SOF in megacities will inevitably require sustainment support because urban operations amplify attrition rates on people and equipment. Potential deficiencies in logistical support should lead planners to reassess the scope or viability of the mission. Second, when employing SOF for unconventional warfare, foreign internal defense, or security-force assistance in the context of urban operations, policy makers and military planners should prepare for high losses among partner or proxy forces and significant collateral damage. These losses will affect SOF's ability to yield strategic results.

Third, urban operations are marked by a highly contested information environment where nonstate actors and ordinary civilians impacted by the military operations often have an advantage over states. SOF psychological and information operations will be particularly demanding and complex in these environments, requiring nontraditional thinking in terms of both messaging and partners. Finally, while SOF should lead in operationalizing emerging technologies for megacity missions, attention should also be paid to countering adversary use of AI-enabled intelligence and surveillance capabilities and resilience in communications-degraded environments. Designing an SOF strategy for the future requires a thorough understanding of the megacity environment, the type of capabilities SOF can leverage for megacity missions, and the limits of SOF in these environments.

Endnotes

1 United Nations, Department of Economic and Social Affairs, Population Division (2018) World Urbanization Prospects: The 2018 Revision. https://www.un.org/en/events/citiesday/assets/pdf/the_worlds_cities_in_2018_data_booklet.pdf.

2 Toesland, Finbarr. "Africa's Megacities a Magnet for Investors." Africa Renewal, United Nations. April 2019-July 2019, https://www.un.org/africarenewal/magazine/april-2019-july-2019/africa%E2%80%99s-megacities-magnet-investors; "These Will Be the Most Important Global Cities in 2035," World Economic Forum, 31 October 2019, https://www.weforum.org/agenda/2019/10/cities-in-2035/.

3 Wainwright, Oliver, "'Like LA with Minarets': How Concrete and Cars Came to Rule Tehran," Guardian, 9 January 2019, https://www.theguardian.com/cities/2019/jan/09/like-la-with-minarets-how-concrete-and-cars-came-to-rule-tehran.

4 David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (New York: Oxford University Press, 2013); W.G. Robertson and L.A. Yates (eds). *Block by Block: The Challenges of Urban Operations* (Forth Leavenworth: US Army Command and General Staff College, 2003); L. DiMarco, *Concrete Hell: Urban Warfare from Stalingrad to Iraq* (Oxford: Osprey, 2012).

5 Phil Williams and Werner Selle, Military Contingencies in Megacities and Sub-Megacities (Carlisle, PA: US Army War College Press, 2016) https://www.armyupress.army.mil/Portals/7/Primer-on-Urban-Operation/Documents/military-contingencies-in-megacities-and-sub-megacities.pdf.

6 Marc Harris, et al., "Megacities and the United States Army: Preparing for a Complex and Uncertain World," June 2014 https://www.army.mil/e2/c/downloads/351235.pdf ; Michael Bailey, Robert Dixon, Marc Harris, Daniel Hendrex, Nicholas Melin, and Richard Russo, "A Proposed Framework for Appreciating Megacities: A US Army Perspective," Small Wars Journal. 24 April 2014 https://smallwarsjournal.com/jrnl/art/a-proposed-framework-for-appreciating-megacities-a-us-army-perspective-0.

7 Dipasquale, Denise, and Glaeser, Edward L. "The Los Angeles Riot and the Economics of Urban Unrest." *Journal of Urban Economics* 43.1 (1998): 52–78.

8 Adamson, William G. "Megacities and the US Army," Parameters 45(1): Spring 2015.

9 ATP 3-06 / MCTP 12-10B, *Urban Operations*, Department of the Army, 7 December 2017.

10 UN-HABITAT, World Cities Report 2016—Urbanization and Development: Emerging Futures, 2016.

11 Joint Publication 3-06, Joint Urban Operations, Joint Chiefs of Staff, 20 November 2013.

12 Glenn, Russell. Heavy Matter: *Urban Operations' Density of Challenges*. Santa Monica, RAND, 2000.

13 Alice Hill, *Future War in Cities: Rethinking a Liberal Dilemma* (New York: Frank Cass, 2004).

14 International Crisis Group, "How to Halt Yemen's Slide into Famine," Middle East Report, No. 193, November 21, 2018.

15 Russell W. Glenn, "Short War in a Perpetual Conflict: Implication of Israel's 2014 Operation Protective Edge for the Australian Army," June 2016. https://www.army.gov.au/sites/g/files/net1846/f/arp9_glen_short_war_in_a_perpetual_conflict.pdf.

16 P. Williams and W. Selle, Military Contingencies in Megacities and Sub-Megacities, Carlisle Barracks: United States Army War College Press, 2016. P. 63-64.

17 Margarita Konaev, The Future of Urban Warfare in the Age of Megacities," Ifri, March 2019.

18 Mosul Study Group, "What the Battle for Mosul Teaches the Force, US Army," September 2017, p. 10 https://www.armyupress.army.mil/Portals/7/Primer-on-Urban-Operation/Documents/Mosul-Public-Release1.pdf.

19 Charles T. Cleveland, James B. Linder, and Ronald Dempsey, "Special Operations Doctrine: Is It Needed?" PRISM, Vol. 6, No. 3. 7 December 2016 https://cco.ndu.edu/News/Article/1020147/special-operations-doctrine-is-it-needed/.

20 C. Raleigh, "Urban Violence Patterns Across Africa States," *International Studies Review*, No. 17, 2015, pp. 90-106.

21 Katherine Graef, "Low Density Logistics: Sustaining Special Operations Forces in Africa," Small Wars Journal, 8 August 2018 https://smallwarsjournal.com/jrnl/art/low-density-logistics-sustaining-special-operations-forces-africa.

22 ADP 3-05 Army Special Operations. (Washington, DC: Department of the Army, July 2019) https://fas.org/irp/doddir/army/adp3_05.pdf.

23 Michael Knights and Alex Mello, "The Best Thing America Built in Iraq: Iraq's Counterterrorism Service and the Long War Against Militancy," War on the Rocks, 19 July 2017, https://warontherocks.com/2017/07/the-best-thing-america-built-in-iraq-iraqs-counter-terrorism-service-and-the-long-war-against-militancy/; Amos Fox, "What the Mosul Study Group Missed," Modern War Institute. 22 October 2019 https://mwi.usma.edu/mosul-study-group-missed/.

24 Christopher Marsh, James D. Kiras, and Patricia J. Blocksome, eds. Special Operations: Out of the Shadows, (Boulder: Lynne Rienner Publishers, 2019).

25 Johnson, David, "Urban Legend: Is Combat in Cities Really Inevitable?" War on the Rocks. 7 May 2019, https://warontherocks.com/2019/05/urban-legend-is-combat-in-cities-really-inevitable/.

26 David A. Shlapak and Michael Johnson, "Reinforcing Deterrence on NATO'S Eastern Flank: Wargaming the Defense of the Baltics," RAND, 2016 https://www.rand.org/pubs/research_reports/RR1253.html.

27 Russell Glenn, Eric Berry, Colin Christopher, Thomas Kruegler, Nicholas Marsella, "Proceedings of the "Multi-domain Battle in Megacities Conference," April 2-4, Fort Hamilton, New York.

28 "Gaza Conflict: the social media front line," The Week 18 July 2014, https://www.theweek.co.uk/middle-east/59554/gaza-conflict-the-social-media-front-line.

29 Ian Burrell, "Israel-Gaza conflict: Social Media Becomes the Latest Battleground in Middle East aggression—But Beware of Propaganda and Misinformation," The Independent (July 14, 2014), https://www.independent.co.uk/news/world/middle-east/israel-gaza-conflict-social-media-becomes-the-latest-battleground-in-middle-east-aggression-but-9605952.html.
30 Freedberg, Sydney J., "Fix It Before It Breaks: SOCOM, JAIC Pioneer Predictive Maintenance AI," Breaking Defense 19 February 2019 https://breakingdefense.com/2019/02/fix-it-before-it-breaks-socom-jaic-pioneer-predictive-maintenance-ai/.
31 Dixon, Robert, "Bringing Big Data to War in Megacities," War on the Rocks, 19 January 2016 https://warontherocks.com/2016/01/bringing-big-data-to-operations-in-mega-cities/.
32 Freedberg, Sydney J. "Special Ops Using Army's Prototype 3D Maps on Mission: Gervais," Breaking Defense 13 October 2019 https://breakingdefense.com/2019/10/ste-army-3d-mapping-software-so-good-special-ops-uses-it-for-missions/.
33 South, Todd, "This Device Could Help Soldiers See through Walls in the Urban Fight," Army Times 24 October 2019 https://www.armytimes.com/news/your-army/2019/10/24/this-device-could-help-soldiers-see-through-walls-in-the-urban-fight/.
34 Konaev, Margarita, "With AI, We'll See Faster Fights, but Longer Wars," War on the Rocks, 29 October 2019.
35 Vijay N. Gadepally, et al., "Recommender Systems for the Department of Defense and Intelligence Community," Lincoln Laboratory Journal, Vol 22 No. 1, 2016.
36 Daniel Egel, et al., "AI and Irregular Warfare: An Evolution, Not A Revolution," War on the Rocks, 31 October 2019 https://warontherocks.com/2019/10/ai-and-irregular-warfare-an-evolution-not-a-revolution/.
37 Mozur, Paul, "Inside China's Dystopia Dreams: A.I., Shame and Lots of Cameras," New York Times 8 July 2018.
38 David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (New York: Oxford University Press, 2013).
39 Tan, Michelle, "Army Chief: Soldiers Must Be Ready To Fight in 'Megacities,'" Defense News, 5 October 2016 https://www.defensenews.com/digital-show-dailies/ausa/2016/10/05/army-chief-soldiers-must-be-ready-to-fight-in-megacities/.

What Have We Learned? Strategic Latency and the Future of Special Operations Forces

Zachary S. Davis

"In my technicolor childhood
We burned incandescent dreams
Illuminatin' on these future things
That didn't turn out like we thought they would
Now we're doin' things we never dreamed we could"

"Bit Logic," by the Bottle Rockets (2018)[i]

Introduction

Think differently, or face the consequences. Many of the assumptions we have taken for granted about how the world works must be reexamined in the light of current events. It's not just the latest pandemic, broken institutions, global instability, or the onslaught of new technologies that are causing radical change. The world is being transformed physically and politically. Technology is the handmaiden of much of this change. But since the sweep of global change is transforming the face of warfare, United States special operations forces (SOF) must adapt to these circumstances. Fortunately, adaptation is in the SOF DNA.

This book examined the global changes affecting SOF and offers possible solutions to the complexities challenging many long-held assumptions. The authors are a mix of leading experts in technology, business, policy, intelligence, and geopolitics, partnered with experienced special operators who either cowrote chapters or reviewed them to ensure accuracy and relevance for SOF. Our goal was to provide insights into the changes around us and generate ideas about how SOF can adapt and succeed in the emerging operational environment. In this wrap-up chapter, I try to pull together the strands to present a broad overview of what we have learned. We don't cover everything in this book, but there's a good chance we know the right people and can put you in touch with them.

Questioning Assumptions: Has *Everything* Changed?

Our challenge required us to distinguish between those things that are constant and those that are in a state of flux and require new thinking. For example, the laws of physics have not changed, although we are discovering new ways of using them to our advantage. The chapters on biology, material science, and cyber operations offer new insights from the sciences. But many fundamental characteristics of our surroundings remain unchanged, starting with human nature.

i The Bottle Rockets are an American alt-country band formed in 1992.

Not Everything Has Changed

Modern humans are driven by the same motivations that have inspired philosophy, creativity, discovery, and conquest for eons. This is important because so many things depend on human behavior, including the future of war, politics, and technology. The changes we see around us do not diminish the role of fear, insecurity, compassion, and creativity in defining the human condition. With the possible exception of artificially manipulated mass movements (which are addressed in the chapter by Herb Lin and Trisha Wyman), human nature remains the fundamental building block of global order. Therefore, protection from aggressive neighbors remains a primary motivation for humanity, and security is an enduring universal preoccupation.

Another constant is the way people organize for their security. Nation-states are undergoing many important changes, but they persist as the fundamental building blocks of international order and the primary providers of security to the vast majority of people on earth. This is true despite the limitations of sovereignty challenging the ability of nation-states to provide security for populations under their authority. The security dilemma that drives nations to defend themselves inevitably threatens other nations. Deterrence, therefore, will endure as a primary means for states to prevent aggression. The chapter by Brad Roberts shows how deterrence functions as a centerpiece of global order and outlines the role of SOF in reinforcing that order.

Another constant is civil conflict within states, as aggrieved groups challenge existing governments. Groups and individuals will inevitably resort to terrorism as a means of expressing displeasure with more powerful adversaries. New weapons and tactics may empower violent extremist organizations, complicating but not diminishing the SOF role in countering terrorism and supporting allies with foreign internal defense (FID) and other core mission capabilities.

Global competition for power, authority, territory, and resources is relentless, and war remains the final arbiter of unresolvable conflict, as it has throughout human history. The addition of new domains of conflict in outer space, cyber space, and the gray zone[ii] complicate this fundamental reality. With these underlying conditions firmly in place, long-standing practices of statecraft—diplomacy, alliances, and deterrence—remain essential to the maintenance of order. What is less certain is the future role of the international norms and multilateral institutions that have restrained the uses of force and imposed boundaries on violent conflict. Those appear to be changing.

Another global reality—one that is less rooted in antiquity but has gradually asserted itself as a defining aspect of global order—is globalization. The inevitable result of a global population approaching 8 billion people, globalization connects people and places in ways that are producing unprecedented physical and geopolitical conditions. We are more interconnected in more ways than ever before, making us more vulnerable, yet in some ways more powerful, in our interdependence. The

ii The *Cambridge English Dictionary* defines the gray zone as "activities by a state that are harmful to another state and are sometimes considered to be acts of war, but are not legally acts of war." (https://dictionary.cambridge.org/dictionary/english/gray-zone)

Covid-19 pandemic of 2020 demonstrated how interconnected the world has become, overwhelming governments, institutions, stock markets, and global health systems. Several chapters in the book examine the consequences of this interconnectedness, which affects everything from communications, supply chains, food security, migration flows, and disease transmission. Globalization must be considered as the backdrop for future military operations. Intense global connectedness affects many aspects of the special operations mission set directly.

Strategic Latency for SOF: Changes in Technology, the Balance of Power, and the Rules of Warfare

"If looks could kill, they probably will."
"Games without Frontiers," by Peter Gabriel (1980)

With these basic elements of the operating environment firmly in our sights, what are the new and unfamiliar factors of which we should be aware? Which of our assumptions should be adjusted to fit changing circumstances? These dependent variables reflect the changing balance of global power, measured in terms of military, economic, technological, cultural, and other elements of power. Prediction is hard, but forecasting can provide key insights, as shown in the chapter by Richard Lum and Ed Churchill. How will the convergence of known and unknown factors shape the operational environment and create risks and opportunities for SOF?

We define Strategic Latency as the potential for these dynamic factors to align in ways that shift the global balance of power. We use the word *strategic* to identify factors of power that have truly consequential significance for world affairs, as opposed to merely important or interesting developments. For example, nuclear fission held latent potential to shift the global balance of power, which was realized by the Manhattan Project and fully weaponized in 1945. Nuclear weapons changed the world. The military applications of aircraft, missiles, computers, the internet, and space technology might also qualify to be included in this category of strategic effects. Other candidates might include genetic engineering, artificial intelligence, quantum computing, and autonomous vehicles. Quite often, the convergence of technologies creates transformative effects, as in the combination of nukes and missiles, drones and artificial intelligence, and big data with social media. The strategic latency of many key emerging technologies was evaluated in these chapters, viewed through the lens of their potential relevance for SOF. Our hope is that the SOF community will find these insights to be relevant to its missions.

Technology is a dynamic function of human innovation, and, thus, one of the primary changing aspects of the operational landscape. Strategic latency focuses on the role of technology in world affairs. What other dynamic factors could define the operational environment for SOF? While the essence of human nature stays the same, cultures and organizations evolve. Nation-states follow their historic destiny,

experiencing periods of success and failure. Civilizations rise and fall. Individual and group identities are also changing, as described in the chapter by Jennifer Snow. New forms of identity and association beyond nationality complicate the role of nation-states and add complexity to the global landscape. What new groups will organize themselves to express shared interests, sometimes challenging national power and legitimacy? Will SOF be tasked to counter or support such nonstate actors?

The Shifting Landscape: A New Balance of Power

Other forces are also at work. Nationalist, authoritarian, and populist movements are reshaping political allegiances and changing the fate of nations. Nationalist leaders across the globe demonize minority groups and foment hatred based on religious and ethnic association. SOF is already navigating these troubled waters. At the same time, great-power competition has reemerged as revisionist powers seek to undermine the post–World War II international order. China is seizing this moment to redefine the Indo-Pacific balance of power and assert itself on the world stage. It is using massive investments in critical technologies to build its economic and military strength. The chapter on Chinese biotech advancements by James Giordano and L. R. Bremseth highlighted the challenge we face with Beijing's rapid transfer of strategic latency from basic science to military applications for use in nonkinetic warfare. Elsa Kania and Peter Wood examined Beijing's concept of operations for gray-zone warfare. Meanwhile, Vladimir Putin's Russia may not be as adept at channeling economic power into military might but competes by matching its strengths to US shortcomings, by picking political and technological sweet spots to exploit US and Western vulnerabilities. The chapter by Glenn Chafetz, Jonathan Fagins, and Michael Nacht highlighted some of the ways Russian SOF are innovating in modern unconventional warfare.

Russia and China are not alone in welcoming a sweeping realignment of global power. Iran, North Korea, and others are seizing the moment to diminish American influence and advance their own interests and ideas. Sometime allies such as Turkey, Saudi Arabia, and Pakistan appear less committed than previously to longstanding ties with the United States and actively seek new partners for a new era. Rising powers such as India and Brazil seek to increase their influence in the emerging multipolar jumble. Some trusted allies may question the United States' long-term reliability and seek new options. Old alliances are being reshuffled, and new ones are forming. Whatever new alliances are in store, SOF must be prepared to embrace the chaos and complexity of the new world order. This too plays to SOF strengths in working with and adapting to local conditions.

Expanding Our Concepts of the Operational Environment

Fundamental changes in weather and climate also pose important new challenges for SOF. Hurricanes, wildfires, environmental hazards, and rising sea levels all have direct consequences for military operations. Shortages of food, water, and energy increase political instability and may lead to conflict, and will certainly affect issues of access,

sustainability, and partnerships. How will SOF operate in these conditions? Our chapter on food security by Molly Jahn and her team described how food systems have become a contested domain for a wide range of subconventional warfare. These nontraditional security issues have become central features of the SOF operating environment.

One big takeaway from the events surrounding the COVID-19 outbreak is that soldiers and sailors can't fight as intended if they are sick.[1] The specter of whole battle groups being put out of commission because of sickness or deterred by pestilence-infested war zones raises troubling questions for force protection and human performance. In that vein, the chapter by Diane DiEullius and Peter Emanuel examined issues related to human enhancement and performance, including scientific and moral prospects for cyborg soldiers. Giordano and Bremseth speculated about the use of biological agents for hybrid warfare. SOF units may be better prepared to cope with such onerous environmental hazards and already possess specialized capabilities to enable them to operate under increasingly challenging circumstances. But there may be surprises ahead, and hidden costs associated with the technologies we use to cope with these adversities.

Technology always has at least two sides, divided between peaceful and military applications. In their chapter about new forensic techniques, Brad Hart and Brian Souza identified opportunities for detecting health threats that can also be used to track individuals. For SOF this translates into possible force protection applications and uses in tracking high-value targets. When combined with a variety of ubiquitous surveillance methods and big-data-driven artificial intelligence, as described in the chapter by Paul Scharre, might it be possible to know the health status and whereabouts of every person on earth? How might SOF deal with these trends? John Tullius outlined what a convergence of these developments could mean for intelligence collection, analysis, and operations. When we add to the picture the element of geospatial transparency—the all-seeing eye in the sky—as described in the chapter by George duMais, it is clear that many operational concepts will need to be modified, especially with respect to covert action.

Changing global and national demographics also have implications for SOF, as aging populations and youth bulges shape the destiny of nation-states and peoples, causing internal and regional instability across the globe. Migration and refugee flows are already affecting outcomes in the Middle East, Europe, across Africa, and spanning Asia. The fate of the Kurds, Rohingya, Huthis, Yazidis, and other ethnic minority groups have already figured prominently into SOF thinking. Planners and operators must increasingly find ways to maneuver in such challenging human terrain. Rita Konaev's chapter on megacities examined the challenges that massive concentrations of humanity pose for SOF. Not all these changes are new, nor are they necessarily all bad for SOF. Urban warfare is not new, and working with minority groups under difficult circumstances is part of the SOF playbook.

There are opportunities to be gleaned, and strategic latency to be exploited, from all these vectors. In his groundbreaking chapter, Marshall Monroe proposed a new way

of thinking about innovation that could accelerate SOF's ability to envision the future, be the first to adapt to emerging trends, train for over-the-horizon battlefields, and ride the wave of change to victory.

Declining Influence of Rules, Norms, and Treaties and the Future of WMD

Beyond the physical environment, changing norms of behavior increasingly define the political environment. On a global scale, the laws of warfare and prohibitions on the acquisition and use of weapons of mass destruction (WMD) may be losing influence. At the same time, access to WMD technology could make such weapons increasingly available to nations, groups, and individuals. The Treaty on the Nonproliferation of Nuclear Weapons, the Chemical Weapons Convention, and the Biological Weapons Convention all face significant challenges, especially with respect to verification and enforcement. Nuclear, chemical, and biological weapons are poised to break out of these restraints to make a dramatic comeback from being outlawed to being widely viewed as essential tools of national defense. The widespread use of chemical weapons in Syria, Russian and North Korean assassinations using WMD materials, and the continued growth of nuclear stockpiles in a number of countries all suggest WMD will feature prominently in future conflict. Whether naturally occurring or unleashed as weapons of war, biological pandemics greatly complicate the operational environment.

Now that SOCOM has expanded its role in countering these weapons, what is needed to ensure success? In his chapter, Brendan Melley assessed SOCOM's approach to the countering WMD mission and reviews preparations for a world where WMD shape the battlefield as never before. Michael Greene and I examined what it means for SOF to win and lose under such circumstances, where WMD are increasingly prevalent.

Beyond flagging controls and growing interest in WMD, established global standards governing trade, commerce, intellectual property, scientific research practices, corruption, building standards, and law enforcement could lose their influence in the emerging global disorder. Without a consensus among powerful states to promote and enforce norms of behavior, rules become voluntary, and rule breakers can be expected to seek advantage from lax standards of conduct. At the same time, disinformation campaigns further erode confidence in goods, services, governments, and national purpose. Cooperative international organizations depend on support from powerful nations for their legitimacy, and wither when they are neglected. Even the poster child for international cooperation, the United Nations (UN)—and its affiliated agencies—appears to be losing its former authoritative place in the world order. The UN Security Council, once a bastion of US and Western influence, has become a victim of competing worldviews. How will changes in attitudes toward multilateral cooperation and the rule of law affect SOF? Here too, there are risks and opportunities.

Moral and ethical codes of conduct shift naturally along with the balance of power, less reflecting the Western values that inspired the creation of international

treaties and multilateral organizations and increasingly challenged by rising powers and revisionist states eager to cast off the strictures of American influence. A new global outlook on longstanding ethics and norms is poised to shape the operational environment.

The Multi-Domain Battlefield

> *"Everything should be made as simple as possible, but not simpler."*
> ***—attributed to Albert Einstein***[2]

While war is a constant of international competition, the locations where and methods by which it is prosecuted are expanding. The battlefield now includes the deepest ocean trenches, vast subterranean lairs, drone-infested airspace, every nook and cranny of the electromagnetic spectrum, the polar regions, the gray zone, and outer space. Autonomous systems can fight in any of these domains, evoking science-fiction visions of robot armies. In his chapter, Michael Alexander illuminated what these trends mean for subterrain combat. DuMais extended the discussion to the space domain. A tsunami of information about the entire battlespace informs and misleads. What is the collective effect of multidomain conflict on SOF operations? What is the SOF role in these new domains?

The cyber domain has become a primary focus of global competition, as described in the chapters dedicated to illuminating the SOF role in cyber conflict. The chapter by Philip Reiner and Whitney Kassel outlined how SOF can integrate cyber training into its FID mission. David Bray and Vint Cerf showed how open societies fall prey to cyberwarfare. Further, Lin and Wyman illuminated the offensive and defensive challenges for SOF in the use of social media for influence operations. The chapter by Pablo Breuer, David Perlman, and Sara-Jayne Terp looked at the implications of weaponized information, and the chapter by Peter Singer examined the broader strategic implications of the weaponization of so many aspects of civil society. Offensive and defensive cyber tools have become indispensable additions to the SOF toolkit.

Many technologies that do not immediately appear to have relevance for SOF are revealing their latent military value. The introduction of 5G wireless opens a floodgate of information across domains, as described by Toby Redshaw in his chapter on the implications of 5G for SOF. Girish Nandakumar and Jon Cederquist reviewed how blockchain technology could affect SOF, and Scharre analyzed the effects of artificial intelligence on the SOF operational environment. Even things as seemingly basic as accurate timekeeping could have unanticipated operational consequences, as described by Robert G. Kennedy III in his chapter on quantum clocks.

Across all domains, an internet of military things links millions of sensors that feed massive amounts of data to warfighters, planners, analysts, and decision-makers. This data can help locate, track, and target people and objects. But the expansive concept of boundless warfare also further blurs the distinction between combatants and noncombatants, drawing civilian populations into a web of undeclared combat zones.

Equipping the Hyper-Enabled Operator

Which new technologies are best suited to help SOF succeed in this complex geopolitical and technological ecosphere? Leo Blanken and Phillip Swintek examined SOF's role as an innovation hub. As early adaptors, special operators are often on the cutting edge of strategic latency.

Lawrence Bronisz and Dominic Peterson showed how additive manufacturing (or 3D printing, as it is often called)—with its vast potential for using different materials and novel engineering designs, coupled with its portability—is a game changer for the SOF—and our adversaries. Nanotechnology is not the end-all, but as Randall Schunk related in his chapter, it is certainly a core enabler that has lived up to much of the hype of the early 2000s and is now ubiquitous in military systems, including advanced communications, novel sensors, new armor materials, and in situ medical treatments—with more to come! Energetic materials are, by definition, "disruptive."

Bryce Tappan and Patrick Bowden revealed how the future of advanced energetics is rich with new chemistry and designs to tailor the disruptive effects, to suit the needs and imagination of the SOF. Michael Valley reported in his chapter that although a Harry Potter invisibility cloak does not exist (yet), metamaterials—namely natural materials fashioned creatively to deliver unconventional properties—present unprecedented opportunities to manipulate energy, be it sound, light, radar, or shock. Thus, metamaterials offer radical possibilities in the SOF battlespace. Brian Holmes and Michael David showed flexible electronics are a new paradigm for the warfighter, with many applications in place or underway, such as antennas, sensors, and RF circuitry. The world is experiencing a revolution in compact, lightweight power sources, like lithium-ion batteries and advanced fuel cells. Karen Swider-Lyons, Joshua Lamb, and Yet-Ming Chiang clarified that this presents enormous potential for the SOF, but it is not without challenges, since key raw materials are not controlled by the United States. Finally, Robert Skaggs and Frank Gac showed the armor of the future is ripe with possibilities that build on not only new and advanced materials but also the entire suite of developments described in the "The Materials World" section of the book. This offers the potential to equip the soldier of the future with protection, power, communications, and incredible awareness of the environment. Thus, we truly are entering a new age of innovation and experimentation to identify mission-specific applications.

Big changes in the commercial world also have immediate impacts on SOF, especially for efforts to partner with companies to support critical mission requirements such as tailored technology needs for SOF teams. Snow, Brad Chedister, and Tamberin Bates reviewed the efforts of SOFWERX and other innovative platforms to find reliable commercial partners for SOF. The chapter by Sara Dudley showed how cryptocurrencies are being used to evade controls and support criminal enterprises. Success in identifying the right technologies for the mission, developing them into SOF capabilities, and fielding them effectively depends on understanding the private sector and finding the right partners.

We offer several big picture perspectives on the future role of SOF. Marveling at the massive complexity of this multi-domain "system of systems," Mark Maier and Churchill gave us ideas about how to conceptualize the SOF niche within the broader context of global military operations. The chapter by Lum and Churchill takes a future-studies approach to forecast major trends in irregular warfare and technology innovation that will shape the SOF mission. Dan Leaf tied it all together by orienting the future of modern-day commandos within the emerging global operational environment, including the many constraining political and economic factors that will limit SOF freedom of action. These strategic analyses of the SOF future integrate the geopolitical and technological trends projected throughout the volume. Understanding the chaos is a necessary first step to getting the right tools to train and fight effectively within it.

Changes in technology, geopolitics, and the commercial sector have important consequences for core SOF activities, including FID, civil affairs, military information support, counterproliferation, psychological operations, security forces assistance, counterinsurgency, and humanitarian assistance. To exploit the strategic latency of developments in these areas, SOF benefits from cultivating networks of trusted experts who can provide substantive knowledge that is directly tied to mission requirements. The chapters here represent such a network. We have endeavored to link expert knowledge and operational experience to SOF's core functions and tie them to emerging challenges and opportunities. Our goal is for the SOF community, along with the broader military and intelligence communities who work with them, to find this to be a useful resource for understanding tomorrow's challenges and stimulating discussion about ways to exploit strategic latency for US advantage.

Endnotes

1 Gilsinan, Kathy, "An Unhealthy Military Is Struggling to Fight COVID-19," April 3, 2020, Atlantic, https://www.theatlantic.com/politics/archive/2020/04/coronavirus-us-military-pandemic/609367; Cancian, Mark, "How Coronavirus Could Hurt U.S. Military Readiness," 11 March 2020, Forbes, https://www.forbes.com/sites/markcancian/2020/03/11/will-covid-19-devastate-military-readiness/#4b0efd7b1e10.

2 Quote Investigator, May 13, 2011, https://quoteinvestigator.com/2011/05/13/einstein-simple/.

Author Biographies

Michael Alexander

LTC Michael Alexander is a Special Forces Officer that serves as a strategic-and-operational-level planner within SOCOM. He is an alumnus of the Naval Postgraduate School's Defense Analysis Department, where he also served as a military faculty member supporting the emerging technology CP-WMD curriculum. He has 27 years of military experience and extensive depth in conducting special operations. He is an accomplished Green Beret and currently assigned to US Special Operations Command at Fort Bragg, North Carolina.

Tambrein Bates

Tambrein Bates served for 25 years in the US Army. During his military career, he served 20 years in special operations in various roles as an operator, operations staff member and in research and development (R&D) and combat development directorates (CDD) for classified programs. As an operator, he served in numerous locations around the globe, including Panama, Somalia, Central and South America, the Balkans, Afghanistan, and Iraq. In his R&D and CDD positions, he was responsible for the development, integration, testing, and acquisition of advanced operational technologies including EO/IR, information technology, communications, and weaponeering systems.

Upon military retirement, Tambrein worked for L3 Technologies in Greenville, Texas as a research fellow in the Special Programs Directorate, providing both tactical and technical expertise to SOF-focused programs and projects. As the SOFWERX director, he and his team are responsible for creating a platform for accelerating delivery of innovative capabilities to the United States Special Operations Command (USSOCOM) as well as refining capabilities through exploration, experimentation, and assessment of promising technology via a Partnership Intermediary Agreement with USSOCOM.

Leo Blanken

Leo Blanken is an associate professor in the Defense Analysis Department at the Naval Postgraduate School. He is the author of *Rational Empires: Institutional Incentives and Imperial Expansion* (University of Chicago Press, 2012) and coeditor of *Assessing War: The Challenge of Measuring Success and Failure* (Georgetown University Press, 2015). Leo collects and DJs rare soul and funk records from the 1960s.

Patrick Bowden

Patrick Bowden has 15 years of experience studying the chemistry and physics of high explosives and has well-known contributions to the scientific community,

specifically related to homemade explosives, insensitive high explosives, convergent shock geometries, fragment impact initiation, and detonation physics. He received his PhD in 2011 from the University of Rhode Island, with Professors Jimmie C. Oxley and James L. Smith as advisors. Following this, he performed postdoctoral research at Los Alamos National Laboratory (LANL), where he studied dynamic and static high-pressure measurements of inert and HE materials. Next, he held a staff scientist position in the High Explosives Science and Technology group (M-7) at LANL studying high explosives, thermites, and dynamic experimentation and diagnostics for over five years. He works at Dyno Nobel's research-and-development facility near Salt Lake City, Utah. Throughout his career, he has published more than 30 articles on explosives and their properties.

David A. Bray

Dr. David A. Bray has served in a variety of leadership roles in turbulent environments, including bioterrorism preparedness and response from 2000 to 2005, time on the ground in Afghanistan in 2009, as the nonpartisan executive director for a bipartisan national commission on research and development, and as a nonpartisan federal agency senior executive. He accepted a leadership role in 2019 to incubate a new global center with the Atlantic Council.

Dr. Bray also provides strategy to both boards and start-ups espousing human-centric principles to technology-enabled decision-making in complex environments. In 2018, he became a senior fellow with the Institute for Human and Machine Cognition. *Business Insider* named him one of the top "24 Americans Who Are Changing the World" under 40, and he was named a Young Global Leader by the World Economic Forum for 2016-2021. From 2017 to the start of 2020, David served as executive director for the People-Centered Internet coalition—chaired by Internet co-originator Vint Cerf—focused on providing support and expertise for community-focused projects that use the internet to measurably improve people's lives.

Loren R. (Rick) Bremseth

Loren R. (Rick) Bremseth is the senior special operations advisor for Cydecor, a disabled-veteran-owned small business that provides support services to Naval Special Warfare, special operations forces, Expeditionary Warfare components, and other military and government organizations.

Previously, Mr. Bremseth served as the deputy senior director of the Integration Support Directorate for the Department of the Navy, serving as a key advisor to the secretary, under secretary, and deputy under secretary of the Navy for sensitive activities. In 2006, he retired from the Navy after twenty-nine-and-half years of service within the Naval Special Warfare community. His assignments included command of SEAL Team Eight (1996-1998), and his major command tour was at Naval Special Warfare Group Three (2003-2005). He served as Deputy Commander, Special Operations Command, Pacific and Deputy Commander, Combined/Joint Special

Operations Task Force, Bosnia-Herzegovina, and he commanded the Joint Special Operations Task Force, Operation Enduring Freedom—Philippines.

Mr. Bremseth's military awards include the Defense Superior Service Medal, Legion of Merit (3), and associated joint, unit, and campaign awards and decorations by the Department of Defense and the Department of the Navy.

Pablo Breuer

Dr. Pablo Breuer is the chief information security officer (CISO) at Helm Services and is a 22-year veteran of the US Navy with tours including military director of US Special Operations Command Donovan Group and senior military advisor and innovation officer to SOFWERX, the National Security Agency, and US Cyber Command as well as being the director of C4 at US Naval Forces Central Command.

Pablo has been faculty at the Naval Postgraduate School, National University, and California State University, Monterey Bay, as well as a visiting scientist at Carnegie Mellon CERT/SEI. He is a founder and vice director of the Cognitive Security Collaborative and a primary author of the AMITT framework for countering misinformation. He is a cofounder and board member of the Diana Initiative and the CISO for Security BSides Las Vegas.

Larry Bronisz

Larry Bronisz is a senior research-and-development (R&D) mechanical engineer at Los Alamos National Laboratory (LANL) with four decades of broad and deep experience in creative mechanical/electromechanical design, analysis, fabrication, producibility, testing, and delivery of precision R&D hardware. He has worked in aircraft ejection systems (Air Force), robotics (industry and LANL), rocket engines (Aerojet), and global/national security hardware at LANL.

Since 1995, Bronisz has applied additive manufacturing (AM) to manufacture and prototype hardware for many global and national security programs. His AM technology familiarity includes PolyJet, Binder Jet, DLP, SLS, EOS Metal, FDM, SLA, RTM, and rapid casting. He has a strong applied-materials background and has demonstrated skill in miniaturization, ruggedized packaging, and field testing of complex systems delivered to the Department of Defense. He has designed and delivered assemblies ranging from 18 milligrams to 19 tons.

Bronisz has received five LANL team distinguished performance awards by leading a blast-wave guide-wall team and contributing to seismic sensing, a forensic sample-collection device, ARIES stockpile reduction weapons disassembly automation, and robotics for the Human Genome Project.

Bronisz is coinventor on 3 surgical robot patents and 11 others, including magnetic infrasound sensing, enhanced petroleum extraction, automated chemistry modules, and electropolishing of substrate materials for superconductors. He has pending patent applications for deployable space structures and megavolt insulators for x-ray applications. He holds a BS degree in mechanical engineering from the University of California, Davis.

Joseph Byrum

Joseph Byrum is currently chief data science at Principal Financial Group. He was recruited to build and manage a first-of-its-kind artificial intelligence tool for equity trading. Dr. Byrum left his previous position as global head of Product Development (Oilseeds) and head of quantitative sciences at Syngenta when it was acquired by ChemChina in 2017, at the time, the largest acquisition ever made by a Chinese company. At Syngenta, Dr. Byrum initiated and led the company's investments in data-centric R&D. As global head of product development (Oilseeds) and head of quantitative sciences, Dr. Byrum led operational, administrative, and financial oversight of R&D operations spanning the Americas. Dr. Byrum holds a PhD in genetics from Iowa State University, an MBA from the Stephen M. Ross School of Business at the University of Michigan, and an MS in genetics and a BS in science, crop and soil science from Michigan State University.

LTG (Ret.) Edward Cardon

Lieutenant General (Retired) Edward C. Cardon's service to the United States spans over 36 years. He honed his profession both domestically and internationally, including in Germany, Bosnia and Herzegovina, Iraq, and the Republic of Korea. Since retirement, General Cardon has created a wide portfolio focused on helping individuals and teams solve hard problems.

Jon Cederquist

Jon Cederquist is the strategic accounts director at Clearspeed, a San Francisco–based artificial-intelligence enhanced voice-analytics technology designed to assess human risk, identify fraud, and insider threat. He focuses mainly on the Latin America market, serving military, intelligence, government, and commercial organizations. Additionally, Jon is an associate at Vision Foresight Strategy, a foresight and strategic-analysis firm based in Honolulu, Hawaii. Jon holds a BS in civil engineering from the Virginia Military Institute and is a retired Navy SEAL with 24 years of service.

Vinton G. Cerf

Vinton G. Cerf is vice president and chief internet evangelist for Google. Cerf has held positions at MCI, the Corporation for National Research Initiatives, Stanford University, UCLA, and IBM. He served as chairman of the board of the Internet Corporation for Assigned Names and Numbers (ICANN) and was founding president of the Internet Society. He served on the US National Science Board from 2013 to 2018.

Widely known as one of the "Fathers of the Internet," Cerf received the US National Medal of Technology in 1997, the Marconi Fellowship in 1998, and the ACM Alan M. Turing Award in 2004. He has been awarded the Presidential Medal of Freedom (2005), the Japan Prize (2008), and the Queen Elizabeth II Prize for Engineering (2013). He is a fellow of the Institute of Electrical and Electronics Engineers, Association for Computing Machinery, the American Association for the

Advancement of Science, the American Academy of Arts and Sciences, the American Philosophical Society, the Computer History Museum, and the National Academies of Engineering and Science.

Cerf holds a bachelor of science degree in mathematics from Stanford University and master of science and PhD degrees in computer science from UCLA and holds 29 honorary degrees from universities around the world.

Brad Chedister

Brad Chedister is the chief technology officer of DEFENSEWERX—in partnership with the Department of Defense (DOD)—leading multiple innovation facility locations and teams across the United States and serving as a special advisor for bio-tech/med-tech/human-performance-optimization technologies for SOFWERX, Special Operations Command's partner. Chedister serves as a cochairman for the Warfighter Sustainment and Performance Working Group (NDIA/DOD entity), a cochairman of the automobile industry's Exoskeleton Working Group (current and future technologies subgroup), an advisory member of the Cognitive Performer Working Group, a member of Northwestern University's Kellogg Institute TWIN, and a member of ERGO Global Futures.

From 2013 to 2016, Brad Chedister was the lead engineer and subject matter expert (SME) supporting USSOCOM HQ Commander's Science and Technology Initiative, the Tactical Assault Light Operator Suit (TALOS) joint task force. He spent 2004-2016 as a technology scout and SME supporting multiple SOCOM priorities. From 2005 to 2017, he served as the research-and-development (R&D) lead for several SOCOM programs. Additionally, Chedister was selected to lead a brainstorming group for the Ebola crisis dealing with key technologies in collaboration with the World Health Organization and White House R&D leadership. Chedister held the position of Warfighter Systems Architect director at MIT-affiliated Draper Laboratory from 2016 to 2018. Before joining USSOCOM in 2005, he played professional baseball for the Houston Astros organization. Chedister is a biomedical engineer by training and holds a double master's degree in engineering management and technology management.

Yet-Ming Chiang

Dr. Yet-Ming Chiang is a Kyocera Professor in the Department of Materials Science and Engineering at Massachusetts Institute of Technology (MIT), where he researches advanced materials, electrochemical energy storage, and clean-energy technologies. Current research topics in his group include solid-state batteries, high-energy-density rechargeable batteries for electric vehicles and electric aviation, and large-scale energy storage for stationary applications. He received his PhD in ceramics in 1984 and his BS in materials science and engineering in 1980, both from MIT. He has cofounded several companies based on his MIT research, including the energy-storage companies A123 Systems, 24M Technologies, and Form Energy. He is an elected member of the United States National Academy of Engineering.

Edwin A. Churchill II

LTC Edwin A. Churchill II is the former director of Joint Special Operations Command's innovation cell, named JSOC-X. He led a team dedicated to implementing emerging technologies and advanced research and development projects into the current and future needs of special operations forces across the full spectrum of operations. The efforts focused on bridging the gap between current operational capabilities and the future state the Department of Defense (DOD), interagency, and allied partners will be operating in to create a strategic advantage over US adversaries.

Prior to his assignment with JSOC, LTC Churchill worked in the research and development of cannon caliber munitions in Picatinny Arsenal, as well as a scientist/engineer working on unmanned aerial systems and Future Vertical Lift transmission research and development at NASA Glenn Research Center. His work has resulted in several patents, publications, and awards in innovation. LTC Churchill has presented his work to leaders at all levels of government, including the DOD intelligence community, congressional members and staff, and senior members of military agencies, highlighting the importance of DOD partnering with nontraditional industry partners to maintain US strategic advantage in an environment of rapidly emerging advanced technologies.

Thomas E. Creely

Dr. Tom Creely is creator and director of the Ethics and Emerging Military Technology Graduate Certificate Program and associate professor at the United States Naval War College. He works with the Department of Defense Joint Artificial Intelligence Center, Defense Innovation Board, and National Security Commission on Artificial Intelligence. In the Brown University Executive Master of Cybersecurity Program, he is the lead for cyber-simulation curriculum. Tom serves on the board of directors of the Association for Practical and Professional Ethics and the Boston Global Forum AI World Society Standards and Practice Committee and editorial board of *Shaping Futures* magazine. He served on the NATO Science and Technology Organization technical team. A retired Navy chaplain, his Navy career included sea, ashore, overseas, and the Marine Corps, as well as having served as an enlisted sailor. His earlier work experience included banking and restaurant industries and as a principal of a consulting business.

Michael W. David

Dr. David has served on the faculty of the Oettinger School of Science and Technology Intelligence at the National Intelligence University (NIU) since 2014. He teaches courses on cyber and data-analytics issues. Prior to joining NIU, he worked as a subject-matter expert in the Washington, DC area. He focuses on cyber, supply-chain, and energy-infrastructure security issues. Previously, Dr. David worked for the Cubic Corporation of San Diego and served as vice president for international operations in Tokyo, New York City, Singapore, and Brussels. He has traveled extensively throughout Asia, the European Union, the Middle East, and North Africa.

Dr. David served on active duty in the US Army from 1971 to 1981 and in the Army Reserve from 1981 to 1999. While on active duty, he served in reconnaissance, special forces, and Army Security Agency (ASA) units, including the 400th ASASOD, 1st SF Group. His last reserve-duty service was with the US mission to the United Nations in New York at the rank of lieutenant colonel. He is fluent in Japanese and possess basic French-language skills.

Zachary S. Davis

Dr. Zachary S. Davis is a senior fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory and a research professor at the Naval Postgraduate School in Monterey, California, where he teaches courses on counterproliferation. He has broad experience in intelligence and national security policy and has held senior positions in the executive and legislative branches of the US government. His regional focus is South Asia.

Davis began his career at the Congressional Research Service at the Library of Congress and has served with the State Department, congressional committees, and the National Security Council. Davis was group leader for proliferation networks in LLNL's Z Program and in 2007 was senior advisor at the National Counterproliferation Center in the Office of the Director of National Intelligence. He is the author of numerous government studies and reports on technical and regional proliferation issues. He leads a project on the national security implications of advanced technologies, focusing on special operations forces.

Davis's scholarly publications include articles in *Orbis*, *Asian Survey*, *Arms Control Today*, *Security Studies*, and the *American Interest* and chapters in numerous edited volumes. He was editor of the widely read 1993 book *The Proliferation Puzzle: Why States Proliferate and What Results*. His edited book on the 2002 South Asia crisis was published by Palgrave Macmillan. He is the editor of two recent books on emerging technology: *Strategic Latency and World Power: How Technology Is Changing Our Concepts of Security* (2014) and *Strategic Latency Red, White and Blue: Managing the National and International Security Consequences of Disruptive Technologies* (2018). Davis holds a doctorate and masters in international relations from the University of Virginia.

Diane DiEuliis

Dr. Diane DiEuliis is a senior research fellow at National Defense University (NDU). Her research areas focus on emerging biological technologies, biodefense, and preparedness for biothreats. Specific topic areas under this broad research portfolio include synthetic biology, the US bioeconomy, dual-use life sciences research, disaster recovery, and behavioral, cognitive, and social science as it relates to important aspects of deterrence and preparedness.

Prior to joining NDU, Dr. DiEuliis was the deputy director for policy and served as acting deputy assistant secretary for policy and planning in the Office of the Assistant

Secretary for Preparedness and Response (ASPR), US Department of Health and Human Services. While there, she coordinated policy in support of domestic and international health emergency preparedness and response activities, including implementation of the Pandemic All-Hazards Preparedness Act, the National Health Security Strategy, and the Public Health Emergency Medical Countermeasures Enterprise (PHEMCE).

From to 2007 to 2011, Dr. DiEuliis was the assistant director for life sciences and behavioral and social sciences in the Office of Science and Technology Policy (OSTP) in the Executive Office of the President. During her tenure at the White House, she was responsible for developing policy in areas such as biosecurity, synthetic biology, biotechnology, social and behavioral science, scientific collections, human subjects' research, and STEM education. Dr. DiEuliis also worked to help coordinate the interagency response to public health issues such as the H1N1 flu pandemic.

Prior to working at OSTP, Dr. DiEuliis was a program director at the National Institutes of Health (NIH), where she managed a diverse portfolio of neuroscience research in neurodegenerative diseases. She completed a fellowship at the University of Pennsylvania in the Center for Neurodegenerative Disease Research and her postdoctoral research in the NIH Intramural Research Program, where she focused on cellular and molecular neuroscience. Dr. DiEuliis has a PhD in biology from the University of Delaware.

Sara Dudley

Col. Sara Dudley graduated with a bachelor of science degree in economics from the United States Military Academy. She also holds a master's degree in business administration from Harvard University and a master's of arts degree in financial integrity from Case Western Reserve Law School and was an Army War College fellow at Yale University in the Jackson Institute for Global Affairs. She currently serves as the United States Army Special Operations Command comptroller. Sara was commissioned in 1998 as a second lieutenant and has served 22 years in the Army Finance and Comptroller Corps.

George duMais

Dr. George duMais recently retired from the Central Intelligence Agency after thirty-three years of service. For the final six years he was assigned to the National Reconnaissance Office, where he worked on the development of clusters of small satellites from national security missions. He is currently a consultant at FTS International, where he continues to support the development of space technology for intelligence and defense applications. He holds a BS in physics and a PhD in philosophy, both from the University of Maryland.

Peter Emanuel

Dr. Peter Emanuel is the senior research scientist for bioengineering at the US Army's Combat Capabilities Development Command Chemical Biological Center (formerly US Army Research, Development and Engineering Command Edgewood Chemical Biological Center [ECBC]). In this role, he advises Army leadership on emerging technologies in synthetic biology and bioengineering and exploitation of these new fields for applications that support national defense. He maintains active research programs focusing on developing a fundamental understanding of the synthesis, directed self-assembly, and hierarchical organization of naturally occurring materials. This understanding is used to engineer new biologically enabled artificial materials for applications in chemical and biological agent detection, protection, and remediation.

Emanuel previously served six years as the chief of ECBC's BioSciences division, where he led the biological research program for the nation's premier nonmedical research institute for chemical and biological defense. Prior to assuming this role, he served three years in the Bush and Obama administrations as the assistant director for chemical and biological countermeasures within the Office of Science and Technology Policy in the Executive Office of the President. In this position, Dr. Emanuel advocated for the role of science and technology at policy coordinating bodies within the White House and throughout the interagency community.

Dr. Emanuel received a BS in microbiology from the University of Maryland at College Park in 1988 and a PhD in molecular and cellular biology from Penn State University in 1994.

Jonathan Fagins

Major Jonathan Fagins is a visiting scientist at the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory. His CGSR research interests include pathway-to-defeat methods, countering weapons of mass destruction, nonproliferation, defense policy, and nuclear deterrence projects. Jonathan authored "Maintaining Presence: How Do Special Operations Forces Contribute to the Deterrence and Assurance Mission in Europe?" His research highlights how the core activities of special operations forces may complement traditional deterrence and assurance in Europe.

Jonathan is a US Army Special Forces officer with 19 years of service. His deployments include Afghanistan, Iraq, Syria, Niger, and Burkina Faso. He holds a bachelor of science degree in general science from the United States Naval Academy. Additionally, Jonathan received a master of science degree in defense analysis (irregular warfare) from the Naval Postgraduate School in 2019 and a master of science degree in international relations (national security affairs) from Troy University in 2020.

He is married to Teah Fagins, and together they have three children. Jonathan enjoys myriad activities, including hiking, CrossFit, surfing, and camping with his family. He also enjoys coaching youth sports.

Frank D. Gac

Dr. Frank D. Gac retired in 2014, after an exciting and productive 38-year career with the Los Alamos National Laboratory (LANL). During that time, he served as an executive advisor to the principal associate director for Global Security; led the Ceramic Science and Technology and International Research, Analysis, and Technology Groups; and was on intergovernmental personal assignments with various components of the US government. He devoted the majority of his materials research to ceramic processing, the development of advanced ceramic matrix composites, armor system design and analysis, in situ corrosion research under extreme environments, and nanoscience and technology. He is a guest scientist with LANL and a consultant to the Lawrence Livermore National Laboratory Center for Global Security Research. Dr. Gac has been involved with the Strategic Latency project since its inception in 2009.

Dr. Gac has BS and MS degrees in ceramic engineering from the University of Illinois and University of Missouri–Rolla (now known as the Missouri University of Science and Technology), respectively, and he holds a PhD in materials science and engineering from the University of Washington.

James Giordano

James Giordano, PhD, is professor in the Departments of Neurology and Biochemistry, chief of the Neuroethics Studies Program, and codirector of the Program in Brain Science and Global Health Law and Policy of the Pellegrino Center for Clinical Bioethics at Georgetown University Medical Center. He is senior fellow of the Project on Biosecurity, Technology, and Ethics at the US Naval War College, consulting bioethicist to the US Defense Medical Ethics Center, and distinguished visiting professor at the Coburg University of Applied Sciences in Coburg, Germany. He chairs the Neuroethics Subprogram of the IEEE Brain Initiative; is a fellow of the Defense Operations Cognitive Science section, SMA Branch, Joint Staff, Pentagon; and is an appointed member of the Neuroethics, Legal, and Social Issues Advisory Panel of the Defense Advanced Research Projects Agency (DARPA).

Professor Giordano has previously served as Donovan Senior Fellow for Biosecurity at US Special Operations Command (USSOCOM) and task leader of the EU-Human Brain Project Sub-Program on Dual-Use Brain Science. He was JW Fulbright Visiting Professor of Neuroscience and Neuroethics at the Ludwig-Maximilians University, in Munich, Germany, and an International Fellow of the Center for Neuroethics at the University of Oxford.

Professor Giordano is a former US naval officer, holding designations as an aerospace physiologist, research physiologist, and research psychologist, and he served with the US Navy and Marine Corps. In recognition of his achievements, he was elected to the European Academy of Science and Arts and named an Overseas Fellow of the Royal Society of Medicine (UK).

Mike Greene

A recognized subject matter expert on counter proliferation (CP) and counter weapons of mass destruction (CWMD), Mike Greene brings deep technical knowledge and more than 25 years of real-world military experience to his work with CEOs, academic institutions, and senior government officials. While on active duty Mike deployed to combat in the Middle East on numerous occasions, earning four bronze stars (one "V" for valorous actions). He graduated from Explosive Ordnance Disposal School, Dive School, Defense Language Institute (Arabic), National Intelligence University (BSI), and UNC Kenan-Flagler Business School (MBA).

Mike served seven years at Naval Special Warfare Development Group (DEVGRU)—considered to be the most elite unit in the US Navy and Department of Defense. While at DEVGRU, Mike managed Special Programs that targeted adversarial WMD programs, developing and deploying technology to disrupt WMD development, respond to and neutralize WMDs during crisis events, and protect and decontaminate US personnel and equipment when required.

Mike coordinated efforts up the chain of command to the Office of the Secretary of Defense and across the US government with the Departments of Justice, Energy, and Homeland Security. In addition to collaborating across the US government, academia, and industry, Mike has significant experience coordinating efforts with various coalition partners to develop and deploy technology against programs that posed significant threats. Mike possesses conversational fluency in Arabic and Spanish.

Michael S. Gremillion

Colonel Michael S. Gremillion is the deputy director of Weather, Headquarters US Air Force, Washington, DC. He is responsible for assisting the director in developing and implementing weather and geoscience doctrine, policies, plans, programs, and standards. He plans, programs, and budgets for Air Force Weather resources and manages the execution of the $300-million-per-year weather program. He interfaces with the Air Force and Army regarding full exploitation of weather resources and technology. He also directs interagency activities with agencies such as the Department of Commerce, National Aeronautics and Space Administration, and the Federal Aviation Administration. Colonel Gremillion also has served as a field-agency staff officer, fighter-wing weather officer, a Pentagon staff weather officer, space-launch staff meteorologist, a flight commander, and intelligence operations officer. He holds a BS in atmospheric science from the University of Kansas, an MS in meteorology from Texas A&M University, and an MBA from Regis University.

Brad Hart

Since 2018, Brad Hart has been the program manager for Global Security Principal Directorate's Z Program at LLNL. The role of Z Program is to apply the complete set of LLNL's science and technology capabilities to support the intelligence community in overcoming its most difficult challenges. Brad leads a diverse, multidisciplinary

team of intelligence professionals to deliver comprehensive analysis, policy, and operational support in areas where technology research and development are critical to national strategic priorities. These priorities range from combating weapons of mass destruction and cyber security to space and other emerging and disruptive technologies and include detection and analysis that anticipates consequences and contributes to US government actions to preserve and enhance national security.

Brad began his career in 2001 as a postdoc at LLNL in the Chemistry and Materials Science Directorate. He served as a staff scientist in the Forensic Science Center (FSC) from 2003 to 2008, at which point he left the laboratory to serve as a branch chief within the Defense Intelligence Agency. While there, he oversaw many global technical collection activities, as well as the operation of multiple forensic laboratories in active theaters of operation. Brad returned to LLNL in 2011 to serve as the director of the FSC. He holds a BS in chemistry from the University of Kansas and a PhD from the University of California, Irvine.

Brian T. Holmes

Dr. Holmes is the dean of the Oettinger School of Science and Technology Intelligence at the National Intelligence University (NIU) in Bethesda, Maryland. The school is the focus for science and technical analytic education, research, and external engagement across the intelligence and national security communities.

Dr. Holmes holds two patents with the US Navy, has published numerous peer-reviewed scientific papers, and received the Deputy Director of National Intelligence for Analysis Distinguished Analysis Award, a National Intelligence Meritorious Unit Citation, and the 2018 NIU Faculty Research Award. His career includes stints as a scientific researcher at the US Naval Research Laboratory, an intelligence analyst for the Defense Intelligence Agency, an intelligence officer in the US Navy Reserves, and a professor at NIU.

Molly M. Jahn

Dr. Molly Jahn is the founding principal of the Jahn Research Group and professor of Agronomy at the University of Wisconsin–Madison, where she teaches Systems Thinking (on leave 2019-2020 for government service). She is adjunct senior research scientist at Columbia University's Earth Institute and a Special Government Employee at NASA. From 2006 to 2011, she was the 12th dean of the University of Wisconsin's College of Agricultural and Life Sciences and director of the Wisconsin Agricultural Experiment Station, and from 2009 to 2010, deputy and acting USDA Under Secretary of Research, Education and Economics. Crop varieties from her vegetable breeding programs at UW–Madison and Cornell University are grown commercially and for subsistence on six continents under more than 60 commercial licenses. She has authored more than 100 peer-reviewed scientific publications and a series of high-impact reports with government and private-sector collaborators, including Lloyd's of London, Thomson Reuters, and Cargill. Dr. Jahn has trained dozens of students now working all over

the world and has been awarded honorary doctor of science degrees in both the United States and United Kingdom. She consults globally for business, universities, governments, philanthropic organizations, and international multilateral institutions in agriculture, food security, risk in food systems, life sciences, and environment.

Budhikka "Jay" Jayamaha

A faculty member at the United States Air Force Academy in Colorado Springs, Jay brings his political science and security studies background to the study of human and food-system security. At the Jahn Research Group, he examines how internal conflict dynamics in countries with weak institutions influence the food system and shape multistate food crises. He also brings his experience and interests in the use of geospatial data in complex humanitarian emergencies from international crisis mappers. Jay holds a PhD in political science from Northwestern University, where he researched how combatant-state relations shape wartime authority structures, with case studies in Iraq, Iraqi Kurdistan, Turkey, and Nepal. Prior to his studies at Northwestern, Jay served in the US Army as an airborne infantryman in the 82nd Airborne Division during the Iraq War and the war on terror.

Elsa B. Kania

Elsa B. Kania is an adjunct senior fellow with the Technology and National Security Program at the Center for a New American Security. Her research focuses on Chinese military strategy, military innovation, and emerging technologies. Ms. Kania also serves as an officer in the US Navy Reserve and works in support of the US Air Force's China Aerospace Studies Institute through its associates program. She is a nonresident fellow in Indo-Pacific Security with the Institute for the Study of War and is a nonresident fellow with the Australian Strategic Policy Institute's International Cyber Policy Center. She serves as an adjunct policy advisor for the nonprofit Institute for Security and Technology, contributes to the Party Watch Initiative at the Center for Advanced China Research, and cofounded the China Cyber and Intelligence Studies Institute, a nonprofit research collaboration.

Ms. Kania was named an official "Mad Scientist" by the US Army's Training and Doctrine Command and was a 2018 Fulbright Specialist in Australia with the Australian Strategic Policy Institute. Her writings and commentary have appeared in *Foreign Affairs*, *Foreign Policy*, *Lawfare*, *Politico*, and *Defense One*. Ms. Kania is a PhD candidate in Harvard University's Department of Government and a graduate of Harvard College (summa cum laude, Phi Beta Kappa). Her book *Fighting to Innovate* is forthcoming.

Whitney Kassel

Whitney Kassel is vice president and head of cyber event management for North America at Morgan Stanley. As part of the firm's Fusion Resilience Center, the cyber event management team orchestrates responses to major cyber events that threaten the firm's clients, assets, and reputation. Prior to joining Morgan Stanley in 2018,

Whitney led engagement efforts with key government clients at Palantir Technologies, a data analytics and integration company. From 2011 to 2015, Whitney was a senior director at the Arkin Group, a business intelligence and private-investigations firm, and she wrote a regular column for *Foreign Policy* magazine. She has also written for *Foreign Affairs*, *Just Security*, *Defense One*, the *Atlantic*, the *Baltimore Sun*, *Huffington Post*, and others. From 2007 to 2011, she served in the Office of the Under Secretary of Defense for Policy, where she focused on Pakistan, Afghanistan, special operations, and counterterrorism. During this time, she served in Afghanistan and Pakistan. Whitney holds a master's degree in international relations and international economics from the Johns Hopkins School of Advanced International Studies and a bachelor of arts from Barnard College. She speaks French and Russian and lives in Brooklyn.

Aaron M. Kelly

Aaron is a research specialist at the Jahn Research Group. He is currently earning a BS in applied mathematics, with an emphasis in computer science, at the University of Wisconsin–Madison.

Robert G. Kennedy III

Robert G. Kennedy III PE is a polyglot systems engineer with Tetra Tech and general chairman of the Asilomar Microcomputer Workshop. Trained as a mechanical engineer specializing in robotics and Soviet studies, he worked in artificial intelligence for the Oak Ridge National Laboratory and manufacturing for the Douglas Aircraft Company.

In 1994-95, he served as an American Society of Mechanical Engineers congressional fellow, spending his year in the House Subcommittee on Space, focusing on commercial remote sensing and Russian space matters. He was instrumental in the formulation and evolution of Presidential Decision Directive/ NSC 23, the Commercial Remote Sensing Policy. He has participated in the Hackers Conference and was a web security analyst doing counter-cracking with other white-hat hackers just prior to 9/11. In 2011, his published research in geoengineering resulted in a personal invitation by academician Yuri Antonovich Izrael to come to Moscow as a guest of the Russian Academy of Sciences and Roshydromet (Russian weather service) to participate in an international scientific conference on the problems of adaptation to climate change.

Kennedy is president of the American branch of the Institute for Interstellar Studies. He has worked for the Navajo Nation helping it develop big solar. He has also worked in Ethiopia, Tanzania, Uganda, and Rwanda on behalf of USAID and the British Foreign Office to build resilient interdisciplinary teams of young African geoscientists and engineers to develop their vast and indigenous renewable energy resources. He takes pride in speaking enough foreign languages to start a bar fight just about anywhere in the world.

Margarita Konaev

Dr. Margarita Konaev is a research fellow at Georgetown's Center for Security and Emerging Technology (CSET) interested in military applications of artificial intelligence, urban warfare, and Russian military innovation. Previously, she was a nonresident fellow with the Modern War Institute at West Point, a postdoctoral fellow at the Fletcher School of Law and Diplomacy, and a postdoctoral fellow at the University of Pennsylvania's Perry World House. Before joining CSET, she worked as a senior principal in the marketing and communications practice at Gartner.

Margarita's research on international security, armed conflict, nonstate actors, and urban warfare in the Middle East, Russia, and Eurasia has been published by the *Journal of Strategic Studies*, the *Journal of Global Security Studies, Conflict Management and Peace Science*, the French Institute of International Relations, the *Bulletin of the Atomic Scientists*, *Lawfare*, *War on the Rocks*, Modern War Institute, Foreign Policy Research Institute, and a range of other outlets. She holds a PhD in political science from the University of Notre Dame, an MA in conflict resolution from Georgetown University, and a BA from Brandeis University.

Megan Konar

Megan Konar is an assistant professor in the Department of Civil and Environmental Engineering at the University of Illinois at Urbana-Champaign. Professor Konar's interdisciplinary research focuses on the intersection of water resources and food supply chains, drawing from hydrology, environmental science, and economics. Dr. Konar received a PhD in civil and environmental engineering from Princeton University in 2012; an MS in water science, policy, and management from Oxford University in 2005; and a BS in conservation and resource studies from the University of California, Berkeley in 2002. She was awarded the NSF CAREER award and early-career award from American Geophysical Union Hydrologic Sciences.

Joshua Lamb

Dr. Joshua Lamb is a principal member of the technical staff with the Advanced Power Sources R&D organization at Sandia National Laboratories. He primarily oversees the Battery Abuse Testing Laboratory (BATLab) team, which focuses on the development of inherently safe lithium-ion batteries by understanding the consequences and mechanisms of failure, developing cradle-to-grave battery testing, and developing new materials for use in battery systems. Joshua earned his PhD in metallurgical engineering in 2008 and his BS in chemical engineering in 2002 from the University of Nevada. Since joining Sandia in 2011, Joshua has researched advanced techniques for determining the stability of lithium-ion batteries and the development of advanced battery abuse and safety tests.

Herbert Lin

Herbert Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University. His research interests relate broadly to policy dimensions of cybersecurity and cyberspace, and he is particularly interested in the use of offensive operations in cyberspace as instruments of national policy and in the security dimensions of information warfare and influence operations on national security.

In addition to his positions at Stanford University, Lin is chief scientist, emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, where he served from 1990 through 2014 as study director of public policy and information technology projects; adjunct senior research scholar and senior fellow in cybersecurity (not in residence) at the Saltzman Institute for War and Peace Studies in the School for International and Public Affairs, Columbia University; and a member of the Science and Security Board of the Bulletin of Atomic Scientists. In 2016, he served on President Barack Obama's Commission on Enhancing National Cybersecurity. In 2019, he was elected a fellow of the American Association for the Advancement of Science. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT.

Richard A. K. Lum

Richard is an academically trained futurist and chief executive of Vision Foresight Strategy LLC (VFS), a foresight and strategic analysis firm based in Honolulu. He has conducted foresight and strategy work on projects for organizations such as US Indo-Pacific Command, US Special Operations Command, the Office of Naval Research, the European Commission, the UK government, NASA, and PepsiCo. Richard is the author of *4 Steps to the Future: A Quick and Clean Guide to Creating Foresight* (2016) and his contributions were featured in the book *Thinking about the Future: Guidelines for Strategic Foresight* (2006) and *A Careful Revolution* (2019; coauthored with Anne Gibbon). His work has been published in the *Journal of Futures Studies*, the journal *Futures*, *International Journal of System of Systems Engineering*, *World Future Review*, and *Small Wars Journal*. Richard is a nonresident senior fellow at the Atlantic Council. He holds a PhD in political science from the futures studies program at the University of Hawai'i. His dissertation research focused on developing a conceptual framework for designing future governance systems.

Mark W. Maier

Dr. Mark W. Maier is a technical fellow at the Aerospace Corporation and an author and a practitioner of systems architecting (the art and science of creating complex systems). He is coauthor, with Dr. Eberhardt Rechtin, of *The Art of Systems Architecting*

(3rd ed.), the mostly widely used textbook on systems architecting, as well more than 50 papers on systems engineering, architecting, and sensor analysis. Since 1998, he has been employed by the Aerospace Corporation, a nonprofit corporation that operates a Federally Funded Research and Development Center with oversight responsibility for the US National Security Space Program. His position of technical fellow is the highest technical rank in the company.

At the Aerospace Corporation, Maier founded the systems architecting training program (an internal and external training program) and applies architecting methods to government and commercial clients, particularly in portfolios-of-systems and research-and-development problems. He received BS and MS degrees from the California Institute of Technology and engineer and PhD degrees in electrical engineering from the University of Southern California (USC). While at USC, he held a Hughes Aircraft Company Doctoral Fellowship, where he was also employed as a section head. Prior to coming to the Aerospace Corporation, he was an associate professor of electrical and computer engineering at the University of Alabama at Huntsville.

Brendan G. Melley

Mr. Melley is the director of the Center for the Study of Weapons of Mass Destruction (CSWMD), National Defense University. He joined CSWMD in 2011 as a senior research fellow and led the center's support to USSOCOM and the intelligence community for countering WMD and counterproliferation and was CSWMD's coordinator for countering WMD policy support. Prior to joining the center, he was vice president of the Cohen Group, an international business consulting firm.

Mr. Melley served as a director on the National Security Council staff from 2001 to 2005 in both the intelligence programs and proliferation strategy offices and managed the development and implementation of the Proliferation Security Initiative.

Previously, Mr. Melley had senior staff assignments at the President's Foreign Intelligence Advisory Board and the Defense Intelligence Agency (DIA) and was a professional staff member on the Commission on the Roles and Capabilities of the US Intelligence Community. Mr. Melley served on active duty as an infantry officer in the US Army's 25th Infantry Division (Light) and as a military intelligence officer at the DIA. He graduated from both Providence College, Rhode Island and the Postgraduate Intelligence Program at DIA and has an MS in WMD studies from Missouri State University.

Marshall Monroe

Marshall Monroe is founder and chairman of Marshall Monroe MAGIC, a creative technology incubator and strategic design studio headquartered in New Mexico. The firm leverages its ongoing research in the fields of innovation excellence and global markets to formulate new transformation plans and advise select clients in areas of visioning, advanced concepts, mission transformation, business development, and the meeting of grand strategic challenges. MMMagic's clients include Cirque du Soleil, the Michael Jackson estate, Legendary Entertainment, HBO, DIRECTV, NASA, USSOCOM,

multiple national laboratories, Paul Allen's Vulcan Ventures, the Defense Threat Reduction Agency, and MITRE Corporation. Monroe is founder of the Magic Canyon Institute and has briefed white papers from that research arm to multiple US national labs, the Pentagon, UK special forces groups, and the State Department.

Monroe spent 14 years as a creative executive with the Walt Disney Company and was a founding member of the Disney research-and-development division. He holds 15 patents for entertainment technologies. He is well known for designing Blizzard Beach, the wildly successful $100 million water park in Walt Disney World, Florida. Monroe is a former member of the US Director of National Intelligence's Intelligence Science Board and was the founding chairman of the New Mexico Governor's Council on Film and Media Industries. Monroe has a degree in mechanical engineering and fine art from Stanford University.

Seth C. Murray

Dr. Seth C. Murray, professor and Eugene Butler Endowed Chair in Agricultural Biotechnology, Department of Soil and Crop Sciences, Texas A&M University. Dr. Murray received his PhD from Cornell University and a BS from Michigan State University. His research program focuses on new approaches in high throughput field phenotyping (including unoccupied aerial vehicles, [i.e. drones]), quantitative genetic discovery, gene to phene data analytics and applied maize (corn) breeding in Texas. He has released nine maize lines, some having been licensed and being grown by Texas farmers, including proprietary hybrids for whiskey. He has coauthored 64 peer-reviewed articles and served in leadership roles for the American Seed Trade Association (ASTA), the Crop Science Society of America (CSSA), the National Association of Plant Breeders (NAPB), and the North American Plant Phenotyping Network (NAPPN). He is a fellow of CSSA and was named a Blavatnik Young Life Sciences finalist. In 2016-2017, he served as the senior advisor of agricultural systems in the Office of the Chief Scientist at the USDA. He also founded and serves as editor of the *Plant Phenome Journal*.

Michael Nacht

Michael Nacht is the Thomas and Alison Schneider Professor of Public Policy in the Goldman School of Public Policy at the University of California, Berkeley. He was dean of the Goldman School from 1998 to 2008 when *US News and World Report* ranked it the nation's number one graduate school in public policy analysis. From 2009 to 2010, he was Assistant Secretary of Defense for Global Strategic Affairs when he chaired the NATO High-Level Group that advises the NATO alliance on nuclear posture and policy issues. He is the author, coauthor, and editor of numerous publications, including two volumes on latent technologies and national security coedited with Zachary Davis of Lawrence Livermore National Laboratory.

Girish Sreevatsan Nandakumar

Girish Sreevatsan Nandakumar is a PhD candidate in international studies at Old Dominion University in Norfolk, Virginia. He majors in international political economy and development and minors in modeling and simulation. His dissertation explores the political economy of global private currencies. He was a fellow at USSOCOM's Donovan Group and currently works at the Virginia Modeling, Analysis, and Simulation Center (VMASC).

Tony Nguy-Robertson

Dr. Nguy-Robertson is the Water Security program manager and a project lead in the Geospatial Epidemiology Program in the Predictive Analytics Pod within NGA Research. The Water Security program seeks to fill operational gaps in hydrology for the intelligence community and Department of Defense by leveraging academia and industry. Projects have included topics in groundwater, crop irrigation, surface water dynamics, and water quality. His work in the area while at NGA has included publications by the National Academies of Science, peer-reviewed literature, and operational tools. Dr. Nguy-Robertson's efforts in the Geospatial Epidemiology program seek to leverage environmental data to understand and predict future disease outbreaks that threaten national security. Prior to joining NGA Research, Dr. Nguy-Robertson worked in the Office of Geomatics supporting natural hazard and environmental models used in operations. His work has included the examination of the environmental causal factors of the Arab Spring and Ebola outbreaks. These results have been shared at international conferences. He has also convened sessions on the topic of environmental influences on food, water, and health security. He collaborates across the US government, academia, and industry.

Dr. Nguy-Robertson received his PhD from the University of Nebraska–Lincoln in natural resources, MS from Indiana University in geology, and BS from Purdue University in biochemistry. His graduate work has focused on hyperspectral remote sensing of harmful algal blooms and crops with the goal of taking close-range sensors and applying them to airborne and satellite sensors. His postdoctoral research at the University of Nebraska–Lincoln involved relating eddy-covariance flux data to remote sensing models and developing crop-disease risk models. He has more than 25 peer-reviewed publications.

William L. Oemichen

William L. (Bill) Oemichen is a principal in the Jahn Research Group and a senior research fellow in Food Systems Security and Preparedness at the University of Wisconsin–Madison Law School and College of Agricultural and Life Sciences. Oemichen previously served as Wisconsin Health Emergency Preparedness and Response director, as Wisconsin Trade and Consumer Protection administrator, as deputy Minnesota Agriculture commissioner, as CEO of the largest all-cooperative business trade association in the United States, and as a staff member of the US House

of Representatives, Minnesota Senate, and Minnesota House of Representatives. Oemichen earned a JD from the University of Wisconsin Law School and a BA in economics from Carleton College with a concentration in science, technology, and public policy and served as a policy fellow at the University of Minnesota's Hubert H. Humphrey School of Public Policy. Oemichen taught as an adjunct professor at the University of Minnesota School of Population and Clinical Sciences and served on the chancellor's Board of Visitors for UW-Madison. Oemichen currently serves on a number of corporate and federal, state, and local governmental boards, including the board of the education and insurance arm of the $340 billion American Farm Credit System.

David M. Perlman

David M. Perlman, PhD, formerly of Twitter, has worked on fighting back against disinformation, market manipulation, and digital deception since 2016. He has presented to defense officials and business leaders on social networks and psychological influence, led a workshop for NATO officials in London, and presented on corporate risks of misinformation security at the Black Hat cybersecurity conference. In his previous career, he studied physics, electrical engineering, information technology, and game theory. For his doctorate in cognitive science, he used functional MRI brain imaging, biometrics, and methods from behavioral economics to study attention, emotion, and identity. His personal career highlight was presenting his research one-one-one to His Holiness the Dalai Lama at a monastery in India. He is a data scientist and security researcher at Leviathan Security Group.

Dominic Peterson

Dominic Peterson earned his PhD in chemistry from the New Mexico Institute of Mining and Technology. After completing a postdoctoral fellowship at Lawerence Berkeley National Laboratory, he joined Los Alamos National Laboratory as a staff scientist in the chemistry division. His early career focused on the development of separation and detection methods for radioactive analytes in a variety of environments and on techniques for nuclear forensics. He then became a team leader in the materials sciences and technology division for a team that focused on developing and understanding soft materials used in nuclear weapons. Next, he became the group leader for the engineered materials group, where he focused partly on how to increase the capabilities of the group in polymer additive manufacturing. Dr. Peterson returned to science and is focusing on nuclear nonproliferation. His research interests include plutonium materials, additive manufacturing, separations science, and applications of science to solve national problems.

Michael J. Puma

Dr. Puma is director of the Center for Climate Systems Research, part of Columbia University's Earth Institute and colocated with the NASA Goddard Institute for Space Studies. The center has over 30 scientists and staff working closely with NASA on earth science and climate impacts research. Dr. Puma's research focuses on global food security, hydroclimatology, and human migration. He is especially interested in understanding the sensitivity of complex, socioeconomic systems to nonpredictable extremes, including megadroughts, volcanic eruptions, wars, and trade restrictions. Dr. Puma's research has been funded by a variety of institutions including the National Science Foundation, NASA, the US Department of Defense, the United Nations Development Programme, and the Columbia World Project "Adapting Agriculture to Climate Today for Tomorrow" (ACToday). His efforts on global food security also have been supported through a fellowship from Columbia's Center for Climate and Life.

Toby Eduardo Redshaw

Toby Redshaw is responsible for Verizon's Enterprise Innovation and 5G Solutions area. He previously ran 5G Ecosystems, Innovation, and Product Development, AR/VR, and Location Services/Geo Intelligence Business. Prior to joining Verizon, Toby was chief executive officer of Kevington Advisors, a leading-edge consultancy offering services in enterprise-technology strategy and transformation, coaching start-ups and various government and military engagements.Toby previously held global chief information officer positions at American Express and Aviva PLC. He had simultaneous product, marketing, strategy, venture, diversity, and technology responsibilities during his six years at Motorola, while also working as executive chairman of a start-up portfolio company.

Toby is the founding chairman (emeritus) of the Kellogg Innovation Network (originally at Kellogg Graduate School of Management at Northwestern University, now TWIN Global). He cochairs the working group on scale disruptive technologies at the Council on Competitiveness and sits on the Dell IT and the Lake Nona Impact Forum advisory boards. He was born and raised in Mexico City and is proud to have become a US citizen in 2014. Among Toby's recognitions, InfoWorld named him a Top CTO 25—Most Influential IT Leader and *InformationWeek* a Top 50 Global CIOs.

Philip Reiner

Philip Reiner is the CEO and founder of the Institute for Security and Technology, a San Francisco Bay Area–based nonpartisan nonprofit that works to outpace emerging security threats posed by advanced technologies by bridging technical experts and national security policymakers. He previously served in the Obama White House as Senior Director for South Asia on the National Security Council (NSC) staff, the senior advisor for Afghanistan and Pakistan, and a director for Pakistan on the NSC staff. He was a civil servant in the Office of the Under

Secretary of Defense for Policy at the Pentagon—where he received the Office of the Secretary of Defense Medal for Exceptional Civilian Service—and for a number of years at Raytheon Space and Airborne Systems, working in their electronic warfare, remote sensing, and vision systems business units.

Philip is as a member of the advisory board for the AI Security Initiative at the UC Berkeley Center for Long-Term Cybersecurity, an affiliate with Stanford's Center for International Security and Cooperation, the director for advisory at AETOS Strategy and Advisory, and the owner of a personal consulting business, where he advises both public and private clients on business, tech, and international security with a predominant focus on India, China, and Japan. His writing has appeared in *Foreign Affairs*, the *Cypher Brief*, *War on the Rocks*, and *C4ISRNet*. He obtained his master's degree in international relations and international economics from the Johns Hopkins School of Advanced International Studies and a bachelor of arts in comparative religions with a minor in history from the University of California, Santa Barbara, focusing on both East and South Asian history. He routinely guest lectures on emerging international security risks at UC Berkeley and Stanford University and lives in Oakland with his wife and two daughters.

Brad Roberts

Brad Roberts is director of the Center for Global Security Research at Lawrence Livermore National Laboratory in California. From April 2009 to March 2013, he served as Deputy Assistant Secretary of Defense for Nuclear and Missile Defense Policy. In this role, he served as policy director of the Obama administration's Nuclear Posture Review and Ballistic Missile Defense Review. From September 2013 through December 2014, Dr. Roberts was a consulting professor and William Perry Fellow at the Center for International Security and Cooperation at Stanford University. Prior to joining the Obama administration, Dr. Roberts was a member of the research staff at the Institute for Defense Analyses and an adjunct professor at George Washington University.

Jean-Paul Rodrigue

Jean-Paul Rodrigue received a PhD in transport geography from the Université de Montréal (1994) and has been at Hofstra University since 1999, initially at the Department of Economics and Geography and then at the Department of Global Studies and Geography. Dr. Rodrigue sits on the international editorial board of the *Journal of Transport Geography*, the *Journal of Shipping and Trade*, the *Asian Journal of Shipping and Logistics*, and the Cahiers Scientifiques du Transport. He is a board member of the University Transportation Research Center, Region II of the City University of New York and is a lead member of both the PortEconomics.eu initiative and the International Association of Maritime Economists. Dr. Rodrigue was a member of the World Economic Forum Global Agenda Council on the Future of Manufacturing (2011-2016). In 2013, the US secretary of transportation appointed Dr. Rodrigue to sit on the advisory board of the US Merchant Marine Academy, a position he held until 2018. He is also the New

York team leader for the MetroFreight project about city logistics. He regularly performs advisory and consulting assignments for international organizations and corporations and is interviewed by the media about transportation-related matters.

Matthew A. Rose

Matthew A. Rose is a cleared technologist and national security expert currently working for the US federal government as a civilian. He is assigned to the leadership team at the General Services Administration's Centers of Excellence, a White House effort to accelerate enterprise technology modernization across government. His current assignment requires that he lead and oversee cloud optimization, customer experience, data and analytics, development of a functional contact center, program management, and the artificial intelligence work units. Mr. Rose is also a commissioned officer in the US Army Reserve, where he serves as the National Capital Region innovation officer, assisting the Army Futures Command, bridging the gap between DOD innovation requirements and the private sector. In past assignments, Mr. Rose incorporated advanced analysis and visualization tools to improve legacy systems and processes, saving the Joint Force and the government time and money, while improving the user experience enterprise wide. Mr. Rose maintains DOD and USAID Planner Certifications and several DOD all-source intelligence certifications. He has also completed the IC Advanced Analysis Career Program and teaches executive leadership to industry and nonprofit C-suite leaders.

Paul Scharre

Paul Scharre is a senior fellow and director of the Technology and National Security program at the Center for a New American Security. He is the award-winning author of *Army of None: Autonomous Weapons and the Future of War*, which won the 2019 Colby Award and was one of Bill Gates's top five books of 2018. Dr. Scharre worked in the Office of the Secretary of Defense in the George W. Bush and Barack Obama administrations, where he played a leading role in establishing policies on unmanned and autonomous systems and emerging weapons technologies. He led the Department of Defense (DOD) working group that drafted DOD Directive 3000.09, establishing the department's policies on autonomy in weapon systems. He holds a PhD in war studies from King's College London and an MA in political economy and public policy and a BS in physics, cum laude, from Washington University in St. Louis. Prior to working in the Office of the Secretary of Defense, Scharre served as an infantryman, sniper, and reconnaissance team leader in the Army's Third Ranger Battalion and completed multiple tours to Iraq and Afghanistan. He is a graduate of the Army's Airborne, Ranger, and Sniper Schools and Honor Graduate of the 75th Ranger Regiment's Ranger Indoctrination Program.

P. Randall Schunk

P. Randall (Randy) Schunk received his PhD in chemical engineering and materials science in 1989 from the University of Minnesota. He has worked at Sandia National Laboratories for more than 30 years and was most recently promoted to the position of senior scientist. His technical work has focused on manufacturing-process science and engineering, including metallurgy and ceramics, nanomanufacturing, roll-to-roll printing and coating, and polymer processing. Since 2008, he has also served as a national laboratory professor in the Chemical and Biological Engineering Department at the University of New Mexico (UNM). His research group at UNM specializes in developing advanced models for materials-manufacturing processes.

Peter Warren Singer

Peter Warren Singer is strategist and senior fellow at New America. He has been named by the Smithsonian as one of the nation's 100 leading innovators, by *Defense News* as one of the 100 most influential people in defense issues, by *Foreign Policy* to its Top 100 Global Thinkers List, and as an official "Mad Scientist" for the US Army's Training and Doctrine Command. Peter is the author of multiple best-selling, award-winning books. His nonfiction books include *Corporate Warriors: The Rise of the Privatized Military Industry* (2007), *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know* (2014), *Children at War* (2015), and *LikeWar: The Weaponization of Social Media* (2018), which explores how social media has changed war and politics. Both Amazon and *Foreign Affairs* named it book of the year.

Peter is also the coauthor of a novel type of novel, using the format of a technothriller to communicate nonfiction research. His first, *Ghost Fleet: A Novel of the Next World War* (2015), was both a top summer read and joined the professional reading list of every branch of the US military, leading to briefings everywhere from the White House to the Pentagon. His latest such novel is *Burn-In: A Novel of the Real Robotic Revolution* (2020).

S. Robert (Bob) Skaggs

S. Robert (Bob) Skaggs attended the International School of Nuclear Science and Engineering at Argonne National Laboratory after receiving his BS in mechanical engineering with honors from the New Mexico College of Agriculture and Mechanic Arts (now New Mexico State University) in 1958. Commissioned as a 2nd Lt US Army reserve as a distinguished military graduate, he was assigned to further his education at the Defense Atomic Support Agency at the Nevada Test Site. Upon completion of this school, Bob moved to Los Alamos Scientific Laboratory (now Los Alamos National Laboratory; LANL) where he worked on plasma diodes and simultaneously pursued an MS in nuclear engineering at University of New Mexico–Los Alamos, graduating in 1967. He then resigned from Los Alamos and went to graduate school full time at the

University of New Mexico main campus in Albuquerque, earning his doctorate in 1971 from the Department of Chemical Engineering with an emphasis in materials science. In 1972, Dr. Skaggs returned to LANL, where he evaluated the vulnerability of atomic weapon components to nuclear radiation, led research on advanced ceramic matrix composites for high-temperature applications, and served as the program manager for armor in the National Armor/Anti-Armor Program.

Dr. Skaggs retired from LANL in 1993 and pursued private consulting for the following 20 years, retiring from active work in 2013. His final technical contribution was coauthoring the chapter entitled "Armor of the Future: Spider Webs, Buckyballs, Nanotubes, and Beyond," for this book. He passed away on February 20, 2020.

Jennifer Snow

Lt. Col. Jennifer "JJ" Snow is the AFWERX innovation officer for the US Air Force, Air Force Materials Command. She serves as the military representative for technology outreach and engagement, bridging the gap between government and various technology communities to improve collaboration and communications, identify smart solutions to wicked problems, and guide the development of future technology policy to benefit the US Air Force, Department of Defense (DOD), interagency, and allied partners.

Prior to her current assignment, Lt. Col. Snow was the Donovan Group innovation officer for US Special Operations Command and the SOFWERX innovation team. She is a distinguished graduate of the Naval Postgraduate School. Her work has been presented to members of the National Security Council, the White House, and key seniors across the DOD, intelligence community, and interagency to highlight emergent risks and opportunities involving technology and technology-influenced environments.

Brian Souza

Since 2017, Brian Souza has served as the group leader for Biosecurity and Bioforensics in LLNL's Physical and Life Sciences Directorate, where he leads multidisciplinary teams that develop and deploy world-class science and technology to help intelligence and warfighter communities counter vulnerabilities to biological threats. Additionally, he has served as the deputy director for the Center for Biosecurity within the Global Security Directorate and was responsible for program development, including support to the warfighter and USSOCOM for almost twenty years.

During his 20 years at LLNL, Souza has held senior research positions in the Biology and Biotechnology Division, the Forensics Science Center, and International Assessments as a counterterrorism analyst. He currently develops programmatic work within the Global Security Directorate that uses intelligence to inform science-based discovery to provide support to the operations community.

"20 years after starting at LLNL as a research biologist, I continue to be amazed at the contributions of my fellow scientists and the opportunities we all have to serve our nation. I remain grateful for all that LLNL continues to offer—mission, resources, interdisciplinary science, and great friendships."

Karen Swider-Lyons

Dr. Karen Swider-Lyons holds a joint appointment as the director of US Naval Research Laboratory's Laboratory for Autonomous Systems Research (LASR) and the head of the alternative energy section in the chemistry division. Her career has focused on energy materials for batteries and fuel cells and how to integrate them into autonomous systems. Her work on fuel-cell-powered autonomous systems started in 2003 with the Spider Lion unmanned aerial vehicle, and later the Ion Tiger UAV and the Hydranox unmanned undersea vehicle. She earned her PhD in 1992 in materials science and engineering at the University of Pennsylvania and holds a BS in chemistry from Haverford College (1987).

Philip Swintek

Philip Swintek is a special forces officer in the United States Army. He graduated from the Naval Postgraduate School, holding a master's of science in space systems operations and a master's of science in defense analysis.

Bryce C. Tappan

Dr. Bryce C. Tappan is a staff scientist in the High Explosives Science and Technology group (M-7) at the Los Alamos National Laboratory (LANL). He was a recipient of the LANL Agnew National Security Postdoctoral Fellowship and is associate editor of the *International Journal of Energetic Materials and Chemical Propulsion* and editorial board member of the *Journal of Energetic Materials*. His research interests include production of new energetic materials and the study of the decomposition of energetic materials, including the combustion synthesis of nanostructured metal foams and the development of a new solid rocket propulsion system. He is the principle investigator for the development of propulsion systems for small satellites, funded by the LANL-LDRD program. He has a patent related to that subject and has published extensively and received numerous awards, including the *R&D Magazine*'s prestigious R&D100 Award.

In the fields of high explosives science and combustion synthesis, Dr. Tappan has given numerous presentations nationally and internationally and authored or coauthored over 60 articles, reviews, and conference proceedings. While completing his PhD at the University of Delaware, under the supervision of advisor Dr. Thomas B. Brill, Dr. Tappan did pioneering work in the development of nanostructured energetic materials through a novel process involving a sol-gel to cryo-gel synthesis. Other research specialties include the investigation of thermal decomposition of energetic materials by various methods, including in situ gas-phase FT-IR spectroscopy. As an undergraduate student, he performed research at the Sandia National Laboratories Explosive Components Facility. He also had an undergraduate student appointment at LANL in the High Explosives Science and Technology group. He studied chemistry as an undergraduate at the New Mexico Institute of Mining and Technology and worked at the Energetic Materials Research and Testing Center (EMRTC).

Sara-Jayne Terp

Sara-Jayne Terp builds frameworks to improve how autonomous systems and human communities work together. Fusing her work as a data scientist and information-security expert, she examines the light and dark sides of the human-artificial intelligence (AI) interface, building algorithms that enable autonomous systems to accelerate the creation of shared situational awareness in crises and applying information-security principles to counter the impact of misinformation and disinformation campaigns on human systems. She runs Bodacea Light Industries, is a senior advisor at the Atlantic Council, and chairs the Cognitive Security CoLab. Previously, she taught data science at Columbia University, served as chief technology officer of UN Global Pulse (the United Nation's big-data initiative), and designed machine-learning algorithms and unmanned vehicle systems at the UK Ministry of Defense. Sara holds degrees in AI and neural networks.

Gregory F. Treverton

Gregory F. Treverton stepped down as chairman of the National Intelligence Council in 2017. He is a senior adviser with the Transnational Threats Project at the Center for Strategic and International Studies (CSIS) and a professor of the Practice of International Relations at the University of Southern California. Earlier, he directed the RAND Corporation's Center for Global Risk and Security and, before that, the Intelligence Policy Center and the International Security and Defense Policy Center. Also, he was associate dean of the Pardee RAND Graduate School. He served in government for the first Senate Select Committee on Intelligence. He has taught at Harvard and Columbia Universities and has been a senior fellow at the Council on Foreign Relations and deputy director of the International Institute for Strategic Studies in London. He holds an AB summa cum laude from Princeton University and an MPP and PhD in economics and politics from Harvard.

John D. Tullius

John serves as a vice president for open-source intelligence programs at Orbis Operations. He retired from the CIA after serving as the National Intelligence Chair at the Naval Postgraduate School (NPS; 2016-2019), where he taught a variety of intel-related courses and worked with student teams on technology initiatives to address Department of Defense operational requirements.

Prior to NPS, John managed the Open Source Enterprise's bureaus in the Middle East (2014-2016) and Europe (2010-2014), overseeing regional collection efforts and working with liaison partners to develop capabilities. From 2007 to 2010, he managed a group of analytic methodologists that used social network, geospatial, and temporal analysis to address complex problems. John also served as a nuclear expert working on the top U.S. priority issue for a U.S. mission in Europe (2005-2007) and managed a team of analysts (1997-2005) that covered East Asia proliferation and science-and-technology issues.

John served as an Army infantry officer in the Oregon National Guard from 1990 to 1997. He has a PhD in political science (University of Oregon, 1997) and an executive MBA from Georgetown University (2001).

Michael Valley

Dr. Michael Valley is senior manager for the materials science research and development group, part of Sandia National Laboratories' Material, Physical, and Chemical Sciences Center. He leads broad research programs that seek knowledge of materials structure, properties, and performance and the processes to produce, transform, and analyze materials. He is also deputy director for Sandia's Science and Technology Products program area, which bridges science and technology with national security applications. Prior to joining Sandia Labs, he was an assistant professor in the Mechanical Engineering Department at New Mexico State University and an officer in the US Air Force. He has chaired more than two dozen international conferences and has over 100 publications. Dr. Valley received a BS from the United States Air Force Academy and his MS and PhD from New Mexico State University.

Peter Wood

Peter Wood is a defense analyst at BluePath Labs. He has published over 100 articles and studies on Chinese military and foreign affairs, including *China's Military Civil Fusion Strategy: A View from Chinese Strategists* (2020), with Alex Stone; *China's Aeroengine Industry* (2020), with Alden Wahlstrom and Roger Cliff; and *China's Aviation Industry: Lumbering Forward* (2019). Mr. Wood received an MA in international studies from the Hopkins-Nanjing Center for Chinese and American Studies and a BA in political science from Texas Tech University. He spent four years studying in China and is proficient in Mandarin Chinese.

Trisha E. Wyman

Major Trisha E. Wyman is a visiting scientist at the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory (LLNL) and a leader in psychological and special operations for the US Army Special Operations Command. She also trained and is educated in intelligence and chemical, biological, radiological, and nuclear fields. She has nearly two decades of military service with deployments and assignments around the world. Trish is a Distinguished Honor Graduate of the US Army's Psychological Operations qualification course and holds the Meritorious Service Medal, NATO Medal, and other awards and decorations.

Major Wyman holds a bachelor's degree in global studies with a concentration in political science from Methodist University and a master's degree from the George Washington University in security and safety leadership. She earned a master of science in information strategy and political warfare from the Naval Postgraduate School. In addition, Trish also graduated from the Naval War College, Joint Professional Military Education with distinction.

Major Wyman's recent CGSR research focuses on Russian disinformation and includes a thesis titled "Social Media and Strategic Nuclear Weapons: The Russian Case." Trish also explores media tactics and methodologies in support of security strategy, including deterrence and coercion. She has also coauthored a chapter titled "Special Operations Forces and Cyber-Enabled Influence Operations" in a book for the US Special Operations Command.

"This compendium of valuable concepts from some of the brightest minds in national security offers current and future SOF leaders and operators solutions for a complex, uncertain, and dangerous special operations battlefield. This book will stimulate discussions from the team room to the board room and serve as a valuable resource for SOF imagineers, policy makers, planners, and operators for years to come."

Douglas H. Wise

Former Deputy Director of the Defense Intelligence Agency and retired clandestine operator from CIA's Senior Intelligence Service

"SOF has always been an accelerator—propelling the Defense Department forward in tactics, strategic approaches, people selection, and in dozens of other ways. The coming technology revolution will be no different. This excellent book draws on world-class expertise to highlight the many ways SOF can do this. Must reading for not only future SOF leadership but indeed all security leaders and policy makers."

General Joseph L. Votel

Former commander, United States Central Command and president and CEO, Business Executives for National Security

Lawrence Livermore National Laboratory

To learn more please visit our website: cgsr.llnl.gov

ISBN-978-1-952565-07-6