LATENCY UNLEASHED: THE MILITARY IMPLICATIONS OF EMERGING TECHNOLOGIES

Workshop Summary

July 20-22, 2021

Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

Workshop Summary

LATENCY UNLEASHED: THE MILITARY IMPLICATIONS OF EMERGING TECHNOLOGIES

Center for Global Security Research
Livermore, California, July 20-22, 2021

Prepared by Brandon Kirk Williams with contributions from Spencer Erjavic, Evan Lisman, Nina Miller, Hilary Reininger, Lois Rosson[1]

On July 20-22, 2021, the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory (LLNL) hosted a workshop titled "Latency Unleashed: The Military Implications of Emerging Technologies." This session brought together participants drawn from across the policy, military, and private sector communities in the United States. The workshop evaluated the progress made in analyzing the latent strategic potential of key technologies, determining near peer competitors' technological advances, as well as opportunities and challenges facing the United States' innovation ecosystem. Panels approached the question of strategic latency through a Red, White, and Blue framework to understand how adversaries, private sector, and the United States and its allies address the challenge of technological innovation. The workshop covered the specific military applications of strategically latent technologies ranging from the operational level to strategic planning. The workshop advocated for 1) acknowledging the precarity of the United States' lead by urging action on the part of the policy and defense community, 2) improving government relations with the private sector, where the bulk of innovation occurs, to speedily integrate technology, and 3) embracing new mental models that anticipate the accelerating pace of innovation where technological convergence will challenge traditional modes of warfare, analysis, and decision-making.

Discussion was guided by the following key questions:

- How is the strategic latency challenge changing?
- How might emerging technologies affect the nature and dynamics of future conflicts?
- What implications follow for U.S. military planners, especially in the special operations forces (SOF) community?

Key take-aways:

1. Over the past decade, strategic latency has evolved from an over-the-horizon problem to a here-and-now problem. That is, states have gone beyond just hedging against new dangers with advanced S&T programs to deploying new capabilities and competing for advantage

[1] The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

using technological means. The strategic potential of many nations is being "unleashed" in the sense that they are finding military applications for new technologies.

2. The disruptive new technologies are numerous and their number is increasing as S&T innovation accelerates. But a few stand out as especially consequential in terms of their impact on stable strategic relations among major power rivals. Among these, artificial intelligence stands out as especially likely to be a major driver of military change.

3. The innovators are numerous and they compete vigorously. Major powers are the most capable of exploiting a broad array of technologies for military gain. But they are not alone in securing military benefits. Numerous medium and smaller-sized powers compete selectively for technical advantages including, for example, Israel, Iran, and Turkey. Non-state actors have also shown themselves to be adept at utilizing state-developed capabilities and tactics for exploiting disruptive technologies.

4. China has an ambitious, comprehensive, and well-resourced plan to build world-class science and technology institutions, to rapidly innovate, and to identify, develop, and field military applications. With its long-standing focus on "informatized" warfare, it has invested heavily in military applications of cyber and now artificial intelligence. It is fielding significant new capabilities while also applying emerging tech to existing design and production infrastructure. But China is not ten feet tall. It struggles with an underdeveloped work force and a stifling bureaucracy. It also remains heavily dependent on information and technology from outside its borders.

5. Russia also has a plan that is comprehensive and ambitious, though less well-resourced than China's. It too has made significant headway in fielding new capabilities. It too has prioritized cyber and AI. But its challenges are even more significant, not least because sanctions have greatly constrained its needed access to Western information and technology. And it lacks the vibrant private tech sector required to generate technology innovation.

6. The impact of emerging technologies on the nature and dynamics of future conflicts is likely to be well beyond what we have so far envisioned. So far at least, that vision has centered on impacts at the operational and strategic levels of war. At the operational level, the expert community expects the application of emerging and disruptive technologies to improve standard military operational art in various ways. At the strategic level, it expects potentially destabilizing implications as deterrence is simultaneously weakened and strengthened. A broader view is needed. Red's ambition isn't, after all, simple preparedness for direct combat with the US; rather, it is to re-make the international order, suppress the functioning of Western societies and governance, and win without fighting. Red is already attacking many elements of the "system of systems" that constitute the way of life of the Western democracies. Blue must learn to think about this system of systems holistically to be better at both defense and offense. "System thinking," defined as "an approach that collects interior, exterior, and collective adversary views," can help us to imagine future forms of conflict consistent with Red's worldview and to anticipate the associated non-linear breakthroughs in capabilities and concepts they may seek. Innovative gaming and red-teaming can help envision alternative outcomes.

7. Given the hard to predict nature of many emerging and disruptive technologies, and the success of major power rivals in pursuing military applications, the US response to strategic latency has evolved over the last decade—and must evolve further. A decade or so ago, the US was focused primarily on trying to anticipate future developments of a kind and scale capable of dangerously altering the balance of power and ensuring the ability to provide strategic warning. Today, improved anticipation and warning remain important. But there is a new focus on competing successfully with major power rivals to ensure strategic stability and gain the disruptive advantages of emerging technologies for ourselves. Looking to the future, there is rising interest in overcoming political, bureaucratic, and social obstacles to a more agile national S&T strategy.

8. Greater US agility requires continued efforts to improve public-private sector partnerships. S&T innovation is mostly driven by the US private sector and not, as in the Cold War, by the US Government, given its ability to efficiently mobilize a skilled work force and significant capital. The space sector provides powerful examples of how such partnerships can be made to be mutually beneficial even when interests do not fully converge. The development in recent years of specialized institutions to build bridges connecting the public and private sectors, such as Defense Innovation Unit, In-Q-Tel, and SOFWERX, has been helpful in fostering partnerships. But more can and should be done, including reform of DOD procurement and regulatory frameworks that stifle innovation.

9. Greater US S&T agility also requires continued efforts by the U.S. national security community to understand the implications, military and otherwise, of emerging technologies. Ongoing National Defense Strategy reviews provide opportunity to understand the implications of emerging tech for US strategies in peacetime, crisis, and war. In recent years, considerable effort has gone into understanding Red's approach to emerging tech; now is the time to put more focus on Blue's approach.

10. Improving whole of nation agility in S&T also requires a more proactive governmental effort to build the workforce of the future. That workforce should blend the expertise and experience of its more "seasoned" members with the skills and mindset of a younger generation that is steeped in new technologies and shaped by neither the Cold War nor 9/11. The declining social value of public service must be addressed, in part by fixing sclerotic government bureaucracies to make public service an attractive and rewarding career option.

Panel 1: Re-thinking Strategic Latency

- Over 7 years of work, what have we learned?
- How has the problem evolved?
- How might it yet evolve over the 7 years ahead?

Looking back on seven years' publications and workshops, Panel 1 assessed the progress of the Center for Global Security Research's multi-volume strategic latency project and looked to the future of how the subject will evolve. Since 2014, a total of 108 authors contributed to 73 chapters analyzing disparate technologies that carry the latent potential to upset the geopolitical balance of power. One of the project's signal accomplishments was to realize an intellectual agenda where representatives from policy, academia, the intelligence community, the private sector, Special Operations Forces (SOF), and futurists collaborated to understand the tectonic technological changes shaping and reshaping power in the international system. Technologies first identified in 2014 are rapidly reordering society, military affairs, policy, and life where humans are inventing tools that have myriad, converging purposes. Some of the effects are speculative. Others manifest daily in a 4th Industrial Revolution that touches every aspect of life, and poses twin problems for the United States.

First, converging technologies, many orbiting the general field of artificial intelligence (AI), will create strategic effects of the magnitude to remold geopolitics in a rapidly accelerating timeline. Unlike during the Cold War, private companies drive innovation in frontier technologies. Adopting technologies occurs rapidly in the private sector, but the U.S. government faces bureaucratic inertia, an affinity for legacy platforms, and a byzantine acquisition process that hamstrings its ability to integrate technologies at a necessary pace. Many other nation states confront the same hurdle. Nevertheless, the pace of innovation is unfolding at historically unseen speeds where mastering technologies will grant potentially insurmountable first-mover advantages to the nation-state that deploys technology synergistically. Preexisting assumptions of the United States' technological superiority can be shattered unless change is embraced. Quasi-governmental institutions such as AFWERX, SOFWERX, In-Q-Tel, and DIU facilitate targeted innovation for specific DOD and IC users. They may be insufficient, however, to streamline the needed flow of technology and talent into the entire national security community when and where they are most needed.

Second, panelists agreed that cultivating the next generation of public servants presents a key challenge for the United States' national security. Millennials and Gen Z matured in a cocoon of technology that is inseparable from their lived experience, and members of both generations are not steeped in the Cold War or 9/11's historical memory. Technological adaptability and fluency will be the future's coin of the realm, and younger generations intuitively grasp technology's dynamism or chaos. Experienced professionals in the national security ecosystem must strive to create an inclusive community of future leaders—adapting to embrace them rather than fitting them into traditional service identities. Nurturing a service mentality is vital for incorporating the perspectives of a generation that will evolve with the technological security dilemmas in the next 7 years and beyond. The quickening pace of innovation calls for policy makers to develop new mental models and open pathways to welcome talent from the private sector and that prevents brain drain from government to lucrative private sector careers. Fostering a service identity in future generations is of the utmost importance, because technology is only useful in

the hands of those who can instinctually know it and apply it to the vexing security dilemmas in the not so distant future.

Panel 2: The New Disruptors: Cyber and AI

- How might these technologies be applied by Red for military gain?
- How should they be applied by Blue?

Turning to the disruptive potential of cybersecurity and AI, the workshop's second panel analyzed Red and Blue's progress in applying frontier technologies for military gain. For cyber, the threats are urgent, whereas AI carries still greater latent potential. Time horizons distinguish the two technologies, but preparation for global strategic competition demands urgent attention on cyber and AI. Red possesses certain global advantages over Blue. China in particular leveraged the Belt and Road Initiative to distribute its commercial communications and cybersecurity technology throughout Africa, Asia, and Latin America. The Chinese government and its proxies likely monitor communications passing through Chinese-owned or technology-dependent networks, and there is a high likelihood that China will capitalize on converging cyber and AI technologies to conduct surveillance and espionage. Future operating environments may tilt against Blue when converging technologies reduce Red's operational friction to employ cyber and AI against Blue.

Cyber's disruptive potential presents Blue with a number of obstacles and opportunities to compete against Red. The United States' ability to assist its allies must start with a frank appraisal that assumes allied breach by Red. Starting from a defense-oriented perspective encourages strategic planners to chart how Blue can tailor cyber solutions to protect networks from infiltration. Many operators from SOF and the U.S. military are trained for traditional missions and do not have the training and experience needed for cyber partner capacity building. Modernizing security assistance to assist allies in hardening networks and encrypting communications could be a vital first step for Blue to apply cyber for military gain. Regarding offensive cyber weapons, the time may have come for an honest conversation of how the United States can share tools with allies. The United States' long history of security cooperation entrusted allies with weapons, and senior leaders in the Pentagon and at the White House may need to overcome the apprehension of sharing with allies offensive tactics, techniques, and procedures that are available in the public domain.

The race for AI does not mirror other military technologies in the twentieth century and the competition between Blue and Red for military gain is increasingly on a level playing field, especially regarding China. The United States does not have a multi-decade lead on competitors and some of the best innovation is occurring outside the United States. AI is not analogous to stealth technologies, for instance. Battlefield and non-battlefield applications of AI will improve Blue's ability to sift through reams of data for use cases in a range of tasks from predictive capabilities to document management. Like Blue, Red seeks to import the best technologies from the private sector to achieve efficiencies of scale for combat readiness. Decision makers in adversary capitals are betting heavily on AI to compete against Blue, but all countries face bureaucratic impediments. Red's bureaucracies are also slow and cumbersome, reluctant to challenge entrenched political and military relationships. The specter of China's Military-Civil Fusion should not be exaggerated—not every company dutifully delivers its data and tools to the

People's Liberation Army (PLA), and the PLA itself is a massive bureaucracy. Blue is making progress importing AI from commercial partners, and the Department of Defense is adopting nimble, creative approaches to apply IT technologies to the battlefield. Blue's ability to integrate a convergence of AI, robotics, and autonomous systems in a strategy of Mosaic Warfare may alter the strategic calculus that prevents Red from applying those technologies to shift the balance of power.

Panel 3: The New Disruptors: Bio and Advanced Energetics

- How might these technologies be applied by Red for military gain?
- How should they be applied by Blue?

The workshop's third panel zoomed out to consider the epistemologies surrounding the disruptive potential of bio and advanced energetics. Panelists explored how to step beyond an inventory of threats and instead to ask how systems thinking can prepare for a convergence of technologies that could upset geopolitics. Drawing philosophical insights from Thomas Kuhn and Michel Foucault, the panelists defined technology broadly to study the role of systems thinking for Red and Blue. China, for example, possesses advantages in this intellectual and cultural terrain that grants it advantages in socializing disruptive technologies. The PRC's authoritarian system is often better suited to integrate technology into aspects of life ranging from governance to the kill chain. Panelists argued for retrofitting Blue's strategic vision to articulate how bio and advanced energetic technologies are converging with AI, autonomous systems, and information tools to challenge the order of things. Blue's ability to look down range and define goals will be a persistent challenge for integrating bio and energetics in a near-term future when technologies overlap with unforeseen effects. In essence, shedding reductive analyses helps us see that one system will not be siloed off from another. Systems will be embedded in systems, and old thinking is an albatross that constrains our ability to adapt to the future. Urgency lies in defining goals and shifting Blue's epistemologies to institutionalize systems thinking to prepare for the next thirty or more years of geopolitical contest.

For Blue, focusing on the United States, the galloping pace of technological innovation demands strategic planners shed Cold War-era conceptions of time. Transformations surrounding genome editing revolutionized humanity's relationship to every species, and what were once considered immutable laws have been abandoned. Instead of a development cycle where a product was invented in 10 to 15 years, the vista has shrunk to 5 years or less. Moore's Law has been proven to be far too conservative. Science and strategy must coordinate to align goals in order for systems to work harmoniously with this new time scale in mind. The United States possesses historical exemplars and institutional models that can replicated to remain competitive while also unlocking systemic advantages for Blue. The Manhattan Project's defined goals illustrate a past ability to deploy systems thinking for overwhelming strategic gain. Similarly, one panelist advocated for the Defense Advanced Research Projects Agency (DARPA) and Intelligence Advanced Research Project Agency (IARPA) models to foster opportunities for innovation at a smaller scale with outsized effects.

Red, primarily China, approaches the future by adopting systems thinking to overturn historic hegemonies by envisioning a future of a Sino-centric world order. China aspires to foster new hegemonies that alter the balance of power by creating webs of dependencies by manipulating

trade and aid advantages, evident in its Belt Road Initiative. Senior members of the Politburo in Beijing adopt a longitudinal perspective to select which intellectual and material systems are necessary in 2030 to propel China to the apex of its power by 2049. All of this fuses to produce asymmetric advantages for China, especially when novel natural or human-made emergencies demand system-wide remedies. Red's ability to deploy systems thinking for military gain will be apparent when ecological and biological disruptions necessitate intersecting technological solutions. China's rollout of a systems thinking playbook in the Uyghurs' mass detention provides an early test case at scale for how China will use bio and advanced energetic technologies to overturn power hierarchies in the international system. However, the global COVID pandemic highlights shortcomings in the PRC approach.

Panel 4: Military Competition in a Contested Global Order

- How might major power rivals integrate the new disruptors into their strategies? With what impact?
- How might regional challengers utilize these technologies to alter regional balances of power?
- What possibilities exist for non-state actors to integrate and employ disruptive technologies?

Speakers in the fourth panel tackled the complex questions surrounding rivals' ability to integrate disruptive technologies. Both panelists cautioned the audience from believing lofty pronouncements emerging from Beijing and Moscow. Both states are presently dependent on technology from the United States and its allies. Russian and Chinese investment in technologies to compete against Blue demands attention, but the reality of slow integration undermines bold declarations. The 2021 Azerbaijani-Armenian war demonstrated how small states could nimbly integrate technologies to improve battlefield performance. Smaller states such as Estonia, Iran, and Israel utilize cyber and unmanned aerial vehicles (UAVs) to challenge the regional balances of power. Non-state actors' ability to purchase commercial off the shelf technologies will certainly improve their ability to deploy disruptive technologies for deadly effect.

Chinese policy makers and futurists are banking on AI development and integration to cement domestic, regional, and global authority. The same thought leaders recognize the nation's reliance on imported technologies along with the capital to develop indigenous capabilities. One panelist noted that open source analysis of Chinese technological progress disabused him of the notion that China is ten feet tall. In spite of rhetoric emerging from Beijing, the expert argued that Blue should not expect a bolt from the blue that achieves radical effects on the battlefield. The PLA and central leadership distrust the private sector—questioning its ability to deliver or seek funding from outside China to expand business opportunities. Military-Civil Fusion fails, at this point, to deliver and has faced a number of hiccups. Tighter controls over investment, technology transfer, and exports from the United States could curtail China's ability to overturn the geopolitical order or project power with a seamless integration of AI, autonomous systems, and robotics.

Similarly, public statements from Vladimir Putin, Sergey Shoygu, and Valery Gerasimov tout the power of AI, autonomous systems, and robotics, but their rhetoric is mismatched with reality

once Russian progress is placed under the microscope. Russia's defense industrial base wheezes under the pressure to meet the lofty futuristic assertions from Russia's senior leaders. Reliance on foreign hardware and software, continued fielding of legacy systems, and a troubled acquisition process constrains ambition. Where Moscow might be short on capacity, Russian strategists are long on vision. Ministry of Defense officials nervously eye their neighbors' and NATO's integration of UAVs, and they seek to offset this by pushing tactical implementation of robotics down to the company level. They look to AI for improvements in augmenting command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) analysis of real time data. To Russia's credit, they fielded systems in Syria and are standing up public-private ventures to spur native technological creation. Even if Moscow's will is strong, it faces challenges that gives Blue long-term advantages.

Panel 5: The Private Sector as Both Partner and Target

- What should and can be done to improve public-private partnerships?
- How significant are the risks that private sector actors will be targeted with disruptive technologies?

Pulling further on the thread of the private sector and innovation, the fifth panel dove into the weighty subject of public-private partnerships (P3s) with experts evaluating the necessary room for cooperation when the private vastly outpaces public sector innovation. The Cold War history of P3s diverges from today's institutional relationships. Capital and private sector innovation, however, benefit from federal acquisitions to propel the innovation life cycle. Not every strategically latent technology will grow due to federal largesse. More P3 channels are necessary to streamline government adoption of disruptive technologies from the private sector's motors of creation. Risks loom, however. First, commercial enterprises are the target of rival states aiming to steal intellectual property. Second, if government does not have a seat at the table it could be relegated to a backseat driver or behind rivals who shape the beginning of the innovation lifecycle for commercial rather than national security applications. These problems require an active government collaborating with the private sector that employs its scale and acquisitions to guide the private sector without stifling innovation. Current P3 models associated with the services, including NAVAL X, AFWERX and SOFWERX are delivering results but are overshadowed by longstanding DOD procurement and acquisition processes for major defense systems.

Using the commercial space sector as a P3 case study, the panelists elaborated on the possibilities and restraints for P3s. Space is a booming business in the United States and globally since 2015. A torrent of angel funding, venture capital, and special purpose acquisition company investments boosted the totality of startups' commercial space operations. Space is a common site for dual purpose technologies, and nation-states look to lower Earth orbit for economic growth as well as a military domain. The United States is singular in the enormity of domestic capital financing commercial space activities. P3s in the United States take many forms in commercial space and other industries, with one of the most beneficial when the government becomes an anchor tenant. Anchor tenancy establishes long-term benefits when the company reaches maturity, validates the enterprise for other investors, and mitigates risk for investors.

The government's role early on in the investment process can also signal its support without funding. NASA's cooperation with the private space sector is a case study in how NASA stated its ambition to use commercial technology to shape an industry. NASA representatives explicated a multi-year plan that engendered a climate of confidence for investors who believed in the long-term return on investment. Federal engagement indicates faith in a technology or sector that produces a positive outcome without taxpayer dollars. This pattern should be replicated in the future to nourish the United States' competitive nature and innovation.

Overcoming difficulties in other sectors requires a modernized framework to manage P3s. Contemporary economic theory does not offer a manual of how to manage global economic interdependency. The government must toe a delicate line by fostering a welcoming domestic climate for innovation without antagonizing companies by limiting the diffusion of technology. Brokering conversations between entrepreneurs, innovators, and policy makers will reduce friction between disparate parties whose interests can be at odds. P3s' value will only climb in coming decades, and deft management is a key national security goal for the United States' economy, security, and innovative spirit.

Panel 6: Broad Implications for U.S. Military Planners

- What further adaptations to defense strategy are warranted by disruptive new technologies?
- What adaptations at the operational and tactical levels of war are warranted?

The future of military planning is clouded by disruptive technologies that inject more noise into an already messy signal to noise ratio for the observing, orienting, deciding and acting (OODA) loop. Complexity could overwhelm planning on the military IOT battlefield. Panel 6's subject matter experts tackled dilemmas facing senior military leaders posed by disruptive technologies. Traditional notions of war are crumbling, and myriad technologies from cyber to a revolution in sensors demands a force predicated on speed, agility, adaptability, and resilience. Forward-looking leadership must articulate a vision for an agile military alongside setting priorities for the integration of future generations to modernize the institutions that defend the homeland. Defense strategists, however, do not act in a vacuum. Congress' authority over acquisitions and command structure adds another layer of complexity to any strategy for contesting adversary challenges. As one panelist concluded, 1986's Cold War-oriented Goldwater-Nichols Act, originally intended to integrate the services, in some ways hamstrings a twenty-first century force posture fighting in a multi domain context. Tactical decision making on the battlefield cannot be concentrated at the top, even with AI assisted data management systems. Navigating overlapping authorities throughout the kill chain will not be an easy task for military planners, warfighters or leaders. The Department of Defense has taken important steps such as the Joint Artificial Intelligence Committee, to integrate game changing new technologies, but the systemic nature of the challenge should not be understated when crafting the next national defense strategy.

Adapting to disruptive technologies' effect on the spectrum of conflict requires that senior defense leaders think anew about strategic, allied, and homeland defense planning. Ubiquitous sensors, ISR, and combinations of information technology will be vital for collecting information about and analyzing threats, but strategic warning capabilities could still be fooled by adversaries

using many of the same techniques. Surprise attack remains a serious concern, especially where it undermines crisis stability. Improving mutual understanding of how emerging technologies could affect perceptions in a crisis and distort the way that traditional methods of diplomacy are used to avoid and manage crises could be fruitful for Blue and Red. This is especially important in light of widespread use of disinformation and media manipulation methods. Hope that AI tools that support decision-making will enable leaders to achieve cognitive overmatch permeate strategic futurists' analysis, and this will likely benefit all sides rather than give strategic advantage to one competitor over another. The idea of disrupting Red's OODA loop is fraught with risks, including the threat that speedy decision making on the battlefield could squeeze out opportunities for diplomacy. The fully globalized nature of emerging and disruptive technologies exposes the US homeland to a wide range of threats for which defense planners have few answers, whether it is use of the electromagnetic spectrum, new bio or chemical weapons, space, cyber, social media or autonomous vehicles, all of which are available to strong and weak nations, terrorists, and even individual actors. The very concept of defense is in flux.

A revolution is unfolding for operational and tactical affairs, with few facets left untouched by AI, cyber and space assets. Space-based sensors are transforming surveillance by generating reliable targeting, tagging, and locating capabilities. Satellites and ISR can detect tactical movements down to the platoon level, making covert action increasingly difficult. Autonomous robots, fire and forget missiles, and mines are increasingly available to shape the tactical battlefield, even without ethical and moral norms to guide their use. Drone swarms are fast becoming central components of modern military forces, employing sophisticated tactics to strike even strategic targets. Blue can no longer rely on a first mover advantage and must learn to adapt quickly to innovation and surprise from its adversaries.

Panel 7: Specific Implications for the Special Operations Forces Community

- What new opportunities should the SOF community pursue?
- What lessons can it learn from past experience?

SOF is adapting to unprecedented geopolitical and technological changes. New operating environments, technologies, data overload, and asymmetries of power will test SOF's traditional tactics. Some constants will endure. Human capital will survive as the cornerstone of SOF, and molding technology to meet the operator will be more valuable than grafting technology onto SOF units without tailored integration. Institutionally, SOFWERX shortened the distance between technologists and operators to put tools and data in the hands of operators. SOF increasingly integrates data science and champions its utility for meeting mission objectives. While SOCOM prides itself on being an early adaptor and first mover in preparing for the next battlespace, SOF Truths remain valid, especially the precept that SOF cannot be mass produced. Technology is a tool in the hands of exquisitely trained and led operators who match appropriate technologies to mission objectives.

The operating environments of the future are shifting to megacities and the information ecosystem where SOF must operate in conjunction with Red and Blue proxies. Global population booms have created massive human concentrations in the shape of mega cities where SOF must cope with a mixed environment of extreme poverty and technology innovation. Mega cities of the future may incorporate more smart technologies that pose different challenges than current

operating environments. New integrated smart megacities, many with Chinese characteristics, could incorporate AI and IOT sensor networks that facilitate widespread surveillance in denied or contested spaces. SOF will need appropriate technologies to adapt to these conditions. Proxies, who will bear a heavy burden of combat, will assume a newfound significance for urban warfare in traditional and eventually smart megacities. Technologically enabled cities and adversaries will erode the ability to operate discreetly, making information operations critical for promoting narratives in support of partner forces. Technology support to allies and partners, especially in information technologies, will increasingly be a key tool for SOF.

SOF is adapting. The pivot from counterterrorism to great power competition takes place at a time when technology is evolving rapidly and a new generation of operators is preparing to take the field. This convergence of trends in geopolitics, technology and operational culture creates tremendous opportunities for the SOF community to lead the way into the new era of multidomain, complex, integrated warfare.

Center for Global Security Research
Lawrence Livermore National Laboratory
P.O. Box 808, L-189 Livermore, California 94551
https://CGSR.llnl.gov

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-AR-826470