GETTING THE MULTI-DOMAIN CHALLENGE RIGHT

BRAD ROBERTS, EDITOR

Center for Global Security Research
Lawrence Livermore National Laboratory
December 2021

GETTING THE MULTI-DOMAIN CHALLENGE RIGHT

BRAD ROBERTS, EDITOR

Center for Global Security Research
Lawrence Livermore National Laboratory
December 2021

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-978-1-952565-12-0 LCCN-2021924221 LLNL-TR-829304 TID-63030-21

Table of Contents

About the Authors

Michael Albertson is deputy director of the Center for Global Security Research at Lawrence Livermore National Laboratory. His portfolio includes extended deterrence dialogues with NATO and Asian allies, and Russian strategic nuclear arms control issues. He holds a B.A. in international relations and government from Claremont McKenna College, an M.S. in strategic intelligence from the National Defense Intelligence College, and an M.A. in security policy studies from George Washington University.

Benjamin Bahney is a senior fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory. His research focuses on strategic competition in the 21st century in the areas of space, cyber, and advanced science and technology. He received his M.A. in international affairs from U.C. San Diego and a B.A. in history from the University of Pennsylvania.

Paul I. Bernstein is a distinguished fellow at the Center for the Study of Weapons of Mass Destruction, National Defense University and a member of the university's research faculty. He leads the Center's practice in strategic security analysis, and is engaged in a range of policy support, research, and professional military education activities related to weapons of mass destruction, nuclear policy, deterrence, threat reduction, and regional security. He has an M.A. in international affairs from Columbia University.

Kim Budil is the director of Lawrence Livermore National Laboratory. She leads the development and implementation of the Laboratory's scientific vision, goals and objectives, and serves as the Laboratory's highest-level liaison with the Department of Energy, National Nuclear Security Administration, the Lawrence Livermore National Security Board of Governors, the University of California, and other government, public, and private organizations. She received her Ph.D. in engineering/applied science from the University of California, Davis and a bachelor's degree in physics from the University of Illinois at Chicago.

Jacek Durkalec is a senior fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory. His research focuses on U.S. policy of extended deterrence in the context of current global challenges and increasingly integrated spheres of strategic deterrence and influence. He holds a Ph.D. in political science and an M.A. degree in international relations from Jagiellonian University, Krakow, Poland.

Austin Long is vice deputy director for Strategic Stability in the Joint Staff J5 (Strategy, Plans, and Policy). His portfolio includes nuclear, space, missile defense, cyber, information integration, and arms control issues. He received his B.S. from the Georgia Institute of Technology and his Ph.D. from the Massachusetts Institute of Technology.

Michael Markey is a political scientist at Lawrence Livermore National Laboratory. His current research interests include extended deterrence, escalation control, and strategic stability with an emphasis on emerging domains of competition. He holds an M.A. in international affairs from the University of California - San Diego.

Jonathan Pearl is a senior fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory. His work examines the implications of space, nuclear, and advanced technologies on national security and strategic competition. He holds a Ph.D. and M.A. in government and politics from the University of Maryland, and a B.A. in music from Florida Atlantic University.

Anna Péczeli is a postdoctoral research fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory. Her research focuses on U.S. nuclear planning, in particular the changes and continuities in U.S. nuclear strategy since the end of the Cold War. She earned a Ph.D. in international relations from Corvinus University of Budapest.

Brian Radzinsky is a postdoctoral research fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory. His work focuses on strategic assessments, nuclear deterrence, and emerging technologies. He received a Ph.D. in political science from the George Washington University and a B.A. in political science from Reed College.

Brad Roberts is director of the Center for Global Security Research at Lawrence Livermore National Laboratory. He was 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 and led their implementation. He has a B.A. in international relations from Stanford University, an M.A. from the London School of Economics and Political Science, and a Ph.D. in international relations from Erasmus University.

Phillip C. Saunders is director of the Center for the Study of Chinese Military Affairs at the National Defense University. His portfolio includes responsibility for supervising the Center's research on regional, global, and functional security issues. He received an A.B. in History from Harvard University and an M.P.A. and Ph.D. from the Princeton School of International and Public Affairs.

Introduction

Brad Roberts

The time is ripe to take stock of the multi-domain challenge and U.S. response. At this writing in autumn 2021, the Biden administration's National Defense Strategy Review is well underway, with a primary objective to strengthen the integration of capabilities for deterrence. This review follows a period of leadership focus on the Joint Staff and elsewhere in the Department of Defense (DOD) on multi-domain operations and the associated concept and capability development efforts. It comes after nearly three decades of effort by the U.S. defense community to come to terms with the challenges of modern warfare in an increasingly complex geopolitical and technological post-Cold War context.

To take stock of the existing multi-domain deterrence enterprise requires answering a series of questions. These include, for example:

- How much progress have we (the larger defense community, the United States, and its allies) made in coming to terms with the challenges of multi-domain deterrence? By what metrics should we judge?
- Are the major conceptual and definitional issues settled or do they remain in flux?
- What particular challenges have come into better focus as we've worked more deeply into the topic?
- Are responses of the United States and its allies competitive with those of our principal adversaries? By what metrics should we judge? What are the prospects for intensified competition?
- Is deterrence eroding? Strengthening?
- What can and should be done (by the national laboratories, other capability providers, and other stakeholders) to ensure that deterrence remains reliable and effective?
- What can and should be done to mitigate and manage the risks of intensified multi-domain competition in a period of major power rivalry?

The essays collected here offer some answers to these and related questions. They grow out of a campaign of activity that has been underway at the Center for Global Security Research (CGSR) since 2015, which is aimed at understanding the requirements of integrated strategic deterrence. That campaign has included more than 30 workshops and more than 100 speakers. Some of the papers presented

here were developed for a capstone workshop in spring 2021 aimed at surfacing key insights and lessons.

Please note that the views expressed here are those of the authors. They should not be attributed to CGSR, Lawrence Livermore National Laboratory, nor any of its sponsors. I am grateful to the authors for their investment of time and energy in helping to lead this important debate.

Multi-Domain Deterrence: Some Framing Considerations

Paul Bernstein and Austin Long

The New Deterrence Landscape

The defense planning discourse is now replete with references to "integrated," "cross-domain" or "multi-domain" deterrence. Recently, Secretary of Defense Lloyd Austin III outlined an expansive vision of "integrated deterrence" that links all instruments of national power, leveraging a networked set of cutting-edge military capabilities that will enable the United States to act dynamically and unpredictably to deter and respond to threats and attacks by determined adversaries.[1] A revised or updated National Defense Strategy is expected to incorporate this type of approach.

The orchestrated use of capabilities from different operating domains is hardly a new idea. As discussed below, one can point to Cold War examples of concepts designed to do just this to achieve escalation advantage over the Soviet Union. Today's conversation about multi-domain deterrence is shaped by a new strategic and operational context that has emerged in recent years. The United States now faces two near-peer military powers, each of which in its own way is preparing for the possibility of a regional war with the United States by adopting strategies to deter U.S. intervention and place the burden of escalation on Washington in the event of open conflict.

Underwriting these strategies is an array of capabilities that spans the range of warfighting domains, and emerging concepts that aspire to their calibrated or integrated use in ways that are sufficient to significantly damage U.S. military prospects but not so severe as to trigger nuclear escalation. The challenge for the United States is to leverage its own multi-domain capabilities in innovative ways to deter great power aggression and, if necessary, prevail against it without generating potentially catastrophic escalation.

There is, thus, both danger and opportunity in the emergence of great power multi-domain strategic capabilities. These "toolkits" provide the means, potentially, to achieve decisive outcomes short of the nuclear threshold—and thus represent a significant break with earlier concepts that envisioned relatively few steps between conventional and nuclear war in an escalating conflict. The more non-nuclear tools available to manage conflict and underwrite deterrence, the better—at least in theory. In practice, however, there is a lot that remains unknown, including the strategic impact some new domain capabilities could have, either alone or in combination. These could fall well short of nuclear effects but still be highly damaging

1 Lloyd J. Austin III, "The Pentagon must prepare for a much bigger theater of war," *The Washington Post* (May 5, 2021). https://www.washingtonpost.com/opinions/lloyd-austin-us-deter-threat-war/2021/05/05/bed8af58-add9-11eb-b476-c3b287e52a01_story.html. Accessed August 26, 2021.

or consequential in other ways. So multi-domain deterrence will not be devoid of escalation risk—and to the degree that some approaches to integration may be seen (rightly or wrongly) as weakening the firebreak between conventional and nuclear conflict, they could indeed serve to heighten escalation risk.

While close study of the respective Russian and Chinese "way of war" has yielded a growing understanding of how each is preparing to confront the United States, precisely how each would execute a strategy of multi-domain deterrence in a conflict with Washington is also unclear. Russia's thinking about how to send calibrated and coordinated deterrence signals across domains and organizations seems to be further along than China's—but it should be assumed that China will be working toward the required concepts and capabilities. Other chapters in this volume address this "Red" dimension. The fact is that none of the great powers has any experience during war of employing multi-domain strategies to deter, manipulate risk, manage a process of escalation, or impose decisive costs on a peer adversary.

This chapter takes a "Blue" perspective and outlines a number of framing considerations that are shaping and could further shape the U.S. approach to multi-domain deterrence—and that therefore should inform the work of national laboratories and other research and technology organizations seeking to support strategy and capability development. These considerations include the importance of defining deterrence tasks along a continuum of conflict; the character of multi-domain deterrence at the operational and strategic levels of war; and the trajectory of effort required to develop a mature, actionable concept of multi-domain deterrence.

Deterrence Tasks and Phases of Conflict

Deterring Extreme Threats. In the context of intensifying day-to-day competition, deterrence remains important to keep "cold war" tensions from escalating sharply—in the worst and most extreme case to a "bolt from the blue" scenario wherein an adversary launches a no-warning strategic attack. This possibility historically has been seen as extremely unlikely, but in no small part due to efforts to ensure a credible capability for nuclear retaliation following such an attack. While multi-domain capabilities may play a part in deterring this extreme form of aggression, survivable and responsive nuclear forces remain foundational to this task.

Deterring Crises. In contrast, an unfolding crisis continues to be a more likely route to escalation and war; thus, deterring the emergence of acute crises is an important task. Often referred to as general deterrence, this task relies on the perceived combination of Blue's capabilities and commitment to the status quo to convince an adversary that any action that could provoke a crisis is too risky and/or unlikely to yield benefits that clearly outweigh costs. Here, visible progress toward a multi-domain defense posture strengthens deterrence by shaping adversary perceptions of Blue denial capabilities.

Deterring Initial Aggression. It is possible that the combination of Blue capabilities and commitment may be insufficient to deter an adversary from engaging in behavior

that leads to crisis and confrontation. This is most likely when adversaries disagree sharply on a particular status quo, leading to misperception and risk-taking on both sides, as in the Berlin crises of the 1950s and the Cuban Missile Crisis. Deterrence in crisis that seeks to prevent escalation to war, sometimes known as immediate deterrence, requires tailored force posturing, operations, and messaging.

Today, defense planning is largely focused on preparing the joint force to deter initial aggression by a nuclear-armed great power adversary at the regional level. Emerging doctrine for this task emphasizes presenting the adversary with multiple complex, reinforcing, and unexpected operational dilemmas through the coordinated imposition of multi-domain effects. These effects would be the product of precision strike direct fires, information operations, cyber operations, electronic warfare operations, and operations in the space dimension. U.S. Army doctrine for multi-domain operations (MDO) provides the following description:

> MDO provides commanders numerous options for executing simultaneous and sequential operations using surprise and the rapid and continuous integration of capabilities across all domains to present multiple dilemmas to an adversary in order to gain physical and psychological advantages and influence and control over the operational environment.[2]

This embodies a "deterrence by denial" approach focused less on a traditional concept of unacceptable punishment and more on the ability to deliver diverse operational effects in a synchronized or integrated manner in order to surprise or shock the adversary. This synchronization of multi-modal effects would be enabled by advances in intelligence fusion, information sharing, decision processes, and command and control increasingly made possible through artificial intelligence (AI). The deterrence metrics associated with this concept are familiar: raise the expected costs of achieving the goals of aggression and reduce the expected benefits—thereby degrading the adversary's confidence in its overall theory of victory or success.

These deterrence metrics can be aligned with the range of operational needs that have been identified as most important in denying China its objectives in a regional war, to focus on the pacing case for U.S. defense planning. These needs have been articulated in both broad and more granular terms, but generally coalesce around the following:[3]

2 Andrew Feickert, "Defense Primer: Army Multi-Domain Operations (MDO)," Congressional Research Service (April 22, 2021). https://fas.org/sgp/crs/natsec/IF11409.pdf. Accessed August 26, 2021.

3 At a broad level, Vice Chairman of the Joint Chiefs General John Hyten refers to the pillars of the emerging Joint Warfighting Concept: joint fires, command and control, information advantage, and logistics. See Rachel S. Cohen, "COVID-19 Delays Pentagon's Joint Warfighting Plan," *Air Force Magazine* (January 22, 2021). https://www.airforcemag.com/covid-19-delays-pentagons-new-joint-warfighting-plan/. Accessed August 26, 2021. For a more granular description, see for example, Eric Sayers and Abraham Denmark, "Countering China's Military Challenge, Today," Defense One (April 20, 2021). https://www.defenseone.com/ideas/2021/04/countering-chinas-military-challenge-today/173494/. Accessed August 26, 2021.

- a more distributed regional force posture to include austere operating bases;
- innovative logistics and mobility concepts to support a more distributed posture;
- battle networks that are more resilient and better defended from electronic warfare, cyber, and counter-space threats;
- a deeper, more distributed, and more resilient set of theater strike capabilities–both land attack and anti-ship;
- more robust regional missile defense of key facilities, to include against hypersonic missiles; and
- better defense of the homeland from air and missile attacks that might target mobilization, power projection, and industrial base capacities.

This alignment of operational needs and deterrence effects can help research and technology organizations develop responsive initiatives aimed at strengthening multi-domain deterrence at the operational level in the near- to mid-term. These initiatives may focus on the development of domain-specific effects, on concepts for the delivery of combined, cross-domain effects, or on innovation in key enabling capabilities discussed above.

Managing Intra-War Deterrence. Even a robust multi-domain deterrence posture may be unable to prevent a great power war. Such a war may be characterized as being fought over limited objectives, but the underlying political stakes, each side's operational doctrine, and the destructive power of modern non-nuclear weapons all suggest that the risks of escalation could be high. The core deterrence tasks here are to deter adversary escalation and, if escalation occurs, restore deterrence at an acceptable cost. A challenge for multi-domain deterrence in this setting is the more strategic application of non-nuclear capabilities that may be considered by the adversary as most suitable for a strategy of escalation, and the introduction of nuclear signaling or threats. The greater salience of these factors heightens risk and may raise the perceived stakes for one or both sides. Managing intra-war deterrence therefore requires highly tailored deterrence actions and messaging directed at the adversary's most senior leaders that rely on both denial and the threat of punishment.

The task of restoring deterrence after escalation has occurred is particularly challenging because the adversary will have already crossed certain lines despite earlier deterrence threats and may well be fully committed to his course of action. Shaping his perceptions in a way that now induces restraint likely will require taking actions that are unexpected, reveal a vulnerability, impose a meaningful cost, clearly convey a sense of deeper risk, and reflect innovative operational art. Whether such options for tailored deterrence messaging can be developed and delivered, and whether they can be expected to succeed, are open questions–but almost certainly this will require a multi-domain approach that provides military planners with the latitude to create political effects through orchestrated military actions.

Orchestrating military effects across domains will be a difficult task from both operational and deterrence messaging perspectives. The operational challenge

stems from the breadth and diversity of domains as well as the characteristics of the forces that operate in those domains. For example, the undersea element of the maritime domain remains relatively opaque (to most electromagnetic energy, at least) and slow moving, and forces that operate there are often fungible with respect to mission; attack submarines can collect intelligence, attack enemy ships, and attack land targets, as an example. The space domain, in contrast, is highly transparent but increasingly cluttered. Forces in space are by definition fast-moving, having escaped earth's gravity at least temporarily, but have limited fungibility. The cyber domain is large and manmade, often opaque and very fast moving. Forces operating in cyberspace have variable fungibility and often require long lead times to prepare accesses and tools, though this varies by target.

This diversity and variability make orchestrating integrated multi-domain operations analogous to, but far more complex than, combined arms warfare in the terrestrial domains. As military historians attest, the development of combined arms warfare was fraught with failures and operations that did not go quite as planned.[4] Integrating for modern multi-domain warfare will no doubt lead to similar experiences. Orchestrating cross-domain actions with the goal of conveying a tailored deterrence message will be even more challenging. One reason is that an adversary's perceptions of integrated multi-domain operations will be conditioned by both its own biases and the technical limits of its situational awareness across domains. While this is also true with respect to deterring initial aggression, the "fog of war" resulting from the complexity of wartime interactions across domains is likely to make intra-war deterrence substantially more difficult.

There are other complexities in considering the orchestration of effects. One is the timing of signaling using capabilities that may be "fragile" in the sense that adversary countermeasures may be swift following revelation of the capability. For example, offensive cyber capabilities that require exquisite access (e.g., to adversary military systems) may be quickly neutralized once used. This would counsel waiting to reveal the capability until war is certain if not already underway. Yet there may be utility in demonstrating these capabilities during day-to-day competition or in crisis to shape the competition or surprise the adversary, potentially resulting in outsized, even decisive effects on the adversary's calculus.

Additionally, there may be value in multi-domain operations able to produce highly discrete effects observable only to the adversary. For example, some multi-domain effects on adversary space systems might be known only to the adversary. Such operations may help to limit escalation risk and restore deterrence if appropriately executed and messaged. The challenge is to ensure that the effects remain observable exclusively to the adversary and are timely with respect to influencing his

4 By 1939, the German Wehrmacht had achieved an extensive theoretical development of combined arms concepts and gained operational learning in the Spanish Civil War and the "dress rehearsal" occupations of Austria and Czechoslovakia. Yet there were still a number of lessons learned from shortcomings of equipment, training, and organization in the invasion of Poland.

calculus. Once an adversary is committed to conflict, there may be no practical set of discrete multi-domain effects that can significantly shape his calculus.

A final complexity is the asymmetry in dependence on domains (or specific capabilities in domains) between the United States and its adversaries. For example, given the demands of projecting power for "away games" shaped by extended deterrence commitments, the United States is generally more reliant on space systems for communication and intelligence than its adversaries. This produces strong incentives for adversaries to attack in space. By contrast, adversaries may be reliant on systems that are not directly relevant to U.S. military operations, such as those that enable social control.

Integration Across Domains in the Cold War

Despite these complexities, policymakers and defense planners should not despair. During the Cold War the United States struggled with similar challenges of integrating capabilities across emerging domains. By the late Cold War (roughly 1979-1989), the United States had begun to articulate an integrated deterrence strategy that brought together space, counterspace, maritime, and air capabilities to deter Soviet aggression and, if deterrence failed, to achieve escalation advantage in conflict.

The demand for escalation advantage was first specifically articulated in the Carter administration following a review of nuclear targeting policy. As then-Secretary of Defense Harold Brown wrote to President Carter in 1978: "We should also have a capability to threaten escalation. To lend credibility to a U.S. threat to escalate, we need employment options and supporting capabilities which the Soviets might perceive to be advantageous to us."[5]

The supporting capabilities Brown referred to were, in today's parlance, multi-domain. A central goal was the ability to hold Soviet ballistic missile submarines (SSBNs) at risk. Maritime forces were the most direct means to do so and the U.S. Navy publicly articulated this role in its 1980s Maritime Strategy: "…maritime forces can alter Soviet perceptions of the nuclear balance, or to use their term, the correlation of nuclear forces, by destroying their SSBNs and other platforms. The strategy, therefore, discourages escalation and encourages war termination by reducing Soviet confidence in the combat stability of their sea-based nuclear strike forces."[6]

Cognizant of the threat to their SSBNs, the Soviets created "bastions" in the seas near their coast, protected by maritime and air forces. For the United States, a key enabler for credibly projecting power against these bastions was space systems capable of detecting Soviet forces at long ranges. An example is the infrared data provided by U.S. Defense Support Program (DSP) early warning satellites. Under a project named Slow Walker, Navy personnel were detailed to DSP ground stations; the data enabled the tactical fighters that protected U.S. aircraft carriers to intercept

5 Harold Brown, Memorandum for the President, "Nuclear Targeting Policy Review" (1978).

6 U.S. Navy, *The Maritime Strategy: Global Maritime Elements for U.S. National Strategy* (1985).

Soviet bombers at very long ranges, before they could launch cruise missiles at the carrier.[7]

As the Soviets developed space-based surveillance systems, including for ocean surveillance, the Department of Defense (DOD) identified as early as 1976 "an urgent need for the U.S. to have the capability to destroy a few militarily important Soviet space systems in crisis situations or in war… If the U.S. had the capability to destroy the critical target-locating satellites, which are at low altitude and are few in number, the ability of the Soviets to find and target U.S. surface combatants at long range would be greatly degraded."[8] This requirement was publicly articulated during the Reagan administration, which noted that "the lack of a U.S. ASAT [anti-satellite] capability would afford a sanctuary to existing Soviet satellites designed to target U.S. naval and land-based conventional forces."[9] While U.S. deployment of anti-satellite systems was constrained by domestic political and arms control considerations, their potential importance to the mission of holding Soviet SSBN bastions at risk was clearly recognized.

Finally, the Soviets believed, based on intelligence sources, that the United States possessed electronic warfare capabilities that could disrupt their command and control.[10] While it is not clear at the unclassified level what, if any, capabilities the United States actually had developed, a declassified history of the National Security Agency noted: "By the end of the Cold War in 1989 the cryptologic system had lots of shiny new toys, and was using them to very telling effect."[11]

The United States thus had a well-articulated, if not always well-resourced, approach to deterrence that integrated capabilities across domains. Conventional maritime forces would threaten Soviet SSBNs in support of deterrence and, if deterrence failed, escalation advantage. Space and counter-space systems would enable these maritime forces. Electronic warfare would likely have played an equally important supporting role, perhaps analogous to cyber operations in the modern context. This integrated approach took years to develop, but ultimately was effective. As a declassified study of Soviet perceptions in the late Cold War notes bluntly "…the Soviets probably had grave concerns about the survivability of their submarines on patrol…"[12]

7 U.S. Navy, *From the Sea to the Stars: A History of U.S. Navy Space Activities* (2010).

8 NSC staff summary of *Final Report of the Ad Hoc NSC Space Panel—Part II: U.S. Anti-Satellite Capabilities* (1976).

9 White House, *The U.S. Anti-Satellite (ASAT) Program: A Key Element in the National Strategy of Deterrence* (1987).

10 Benjamin Fischer, "CANOPY WING: The US War Plan that Gave the East Germans Goose Bumps," *International Journal of Intelligence and Counterintelligence* (2014).

11 Thomas Johnson, *American Cryptology during the Cold War 1945–1989,* Vol. 4 (Ft. Meade, MD: Center for Cryptologic History 1999: declassified 2007).

12 President's Foreign Intelligence Advisory Board, *The Soviet "War Scare"* (1990).

Developing the Needed Capacities for Multi-Domain Deterrence

As with the Cold War experience, a modern framework for multi-domain deterrence will not be created quickly. Much of the thinking in this area is at an early stage. A good deal of this is conceptual; some is operational; little is based on contemporary real-world experience. The capacity to develop multi-domain tailored deterrence courses of action, deliver them in crisis or conflict, and measure their effects on an adversary's calculus can only be formed through a deliberate, incremental process of "crawl, walk, run."

The DOD community has been in the "crawl" stage for some time, working to frame the problem and develop the intellectual scaffolding needed to support the development of responsive concepts and capabilities. The problem is well understood by now and initial steps have been taken to socialize the unique challenges of multi-domain deterrence among defense leaders and combatant commands. A necessary next step is to begin articulating a multi-domain approach to deterrence in DOD's core strategy and policy documents. This will empower policymakers and military specialists from relevant offices to collaborate across domain boundaries to establish principles and objectives for a closer alignment of capability sets and their fuller integration over time. As a key element of the 2021 strategy review process, this will constitute a strong demand signal from the Department's senior leaders.

This will also accelerate transition to the "walk" stage, which should feature a structured program of operationally-oriented analytics with the goal of gaining a more granular understanding of multi-domain deterrence opportunities and requirements. Key analytic questions include:

- What deterrence challenges are most likely to demand–or are best suited for–multi-domain approaches?
- Which combined domain effects appear to offer the best prospect of achieving deterrence objectives?
- Which combined domain effects appear to carry higher levels of escalation risk?
- How should multi-domain deterrence courses of action be developed, sequenced, and messaged? How should they be evaluated for likely payoff and risk? Are new or different authorities required to plan or execute such options?
- Is it possible to deliberately plan multi-domain deterrence courses of action in support of intra-war deterrence? What kind of adaptive planning techniques are likely to be needed?
- How best to exercise the development and execution of multi-domain courses of action?
- How can the effects of multi-domain deterrence operations be measured?

The analysis program can draw on a wide range of tools and techniques in attempting to answer these and related questions. These include operations research and systems analysis methods, game theoretical approaches, modeling and simulation, advanced computing, and focused, iterative wargaming–though this analytic toolbox itself needs to be upgraded, as experts have noted.[13] The goal is to identify a set of working propositions that can be tested through DOD experimentation and wargaming—and refined as necessary for integration into concepts, exercises, plans, and capability development. In making choices regarding how to substantively focus analytics, some prioritization should be possible across a set of deterrence challenges judged to be most likely, most pressing, and most complex, with some consideration given to wild card possibilities. As this body of work makes progress and begins to yield actionable results, the basis will exist to more fully develop a planning framework for multi-domain deterrence that can serve as a guide for planning.[14] This would mark achievement of a more mature conceptual and planning capacity and the transition to the "run" phase in the development of multi-domain deterrence.

As a final thought, the role of artificial intelligence merits a brief comment in this discussion. As an analytic tool or part of a suite of tools employed to help answer the questions posed above, AI may prove to be of value—and research and technology organizations that can leverage AI may be able to perform unique types of analysis. As an element of solutions or proposed deterrence courses of action, the picture may be more complex. Clearly, some concepts of multi-domain operations for deterring initial aggression, as framed earlier in this discussion, rely heavily on expected advances in AI. This bullish take on AI envisions it as allowing the joint force to synchronize information and capabilities from across domains at speeds and scales that are not possible today. In support of this vision, there seems to be wide acceptance in the national security community of AI as a key enabler of required concepts and capabilities at the operational level of war and in deterrence by denial approaches, even if there is skepticism in some quarters regarding the ability of AI to deliver on its promise.[15]

13 Former Undersecretary of Defense for Policy Michèle Flournoy has observed that emerging concept development is not adequately supported by robust analysis, wargaming, and field experimentation. "The department's analytic, simulation, and experimentation tools and activities are simply not keeping pace with the changing threat environment. Far more analysis, anchored by experimentation at scale, is desperately needed so that novel operational concepts can be analyzed and tested in realistic scenarios." Michèle Flournoy and Gabrielle Chefitz, "Sharpening the U.S. Military's Edge: Critical Steps for the Next Administration," Center for a New American Security (July 13, 2020). https://www.cnas.org/publications/commentary/sharpening-the-u-s-militarys-edge-critical-steps-for-the-next-administration. Accessed August 26, 2021.

14 For some thoughts on the need for multi-domain deterrence frameworks, see Vincent Manzo, "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?" Strategic Forum, National Defense University Institute for National Strategic Studies (December 2011). https://www.law.upenn.edu/live/files/1323-manzo-deterrence-and-escalation (accessed August 26, 2021) and Paul Bernstein, "Toward an Integrated Strategic Deterrent," in Brad Roberts, ed., *Fit for Purpose: The U.S. Strategic Posture in 2030 and Beyond* (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2020), pp75-89. https://cgsr.llnl.gov/content/assets/docs/The-US-Strategic-Posture-in-2030-and-Beyond.pdf. Accessed August 26, 2021.

15 For a cautious take on the promise of artificial intelligence, see Melanie Mitchell, "Why AI is Harder Than We Think," Santa Fe Institute (April 2021). https://www.arxiv-vanity.com/papers/2104.12871/. Accessed August 26, 2021.

Perceptions of AI at the strategic level of war seem to be markedly different. Many (though certainly not all) analysts of strategic stability dynamics view AI as a source of anxiety and potential instability when considered as a factor that may be introduced into the system of nuclear deterrence. The stability of this system is viewed as critically dependent on human control and thus uniquely vulnerable to the insertion or overlay of forms of autonomy that theoretically could influence decisionmaking or otherwise weaken human agency. This is seen as heightening the risk of catastrophic outcomes.

This dichotomous view of AI as a feature of operational- and strategic-level military systems may not persist, depending on how AI capabilities develop, but analysts and practitioners of multi-domain deterrence should be mindful of it.

Multi-Domain Operations and the Deterrence Calculus

Jonathan Pearl and Brian Radzinsky

Introduction

The U.S. military is urgently pursuing the capabilities, doctrine, and concepts it perceives as necessary to undertake multi-domain operations (MDO). Although MDOs have been a feature of warfare for almost as long as there have been wars, current efforts are driven by a new sense of urgency. MDOs are central to the Department of Defense (DOD)'s thinking on how to deter and defeat aggression by nuclear-armed major-power adversaries. However, efforts to implement the MDO concept remain aspirational, and the relationship between multi-domain operations and its analogue—multi-domain deterrence (MDD)—is still poorly understood. This chapter explores the MDO-MDD relationship and offers preliminary recommendations for advancing an MDD agenda. We begin by discussing the growing interest and activity in MDOs, and identify the factors driving the current sense of urgency, to better integrate MDO and deterrence concepts and capabilities. We find that MDOs already are a part of some deterrence activities, but that the growing number of tools is creating new complexities and uncertainties about future MDO and MDD plans and operations. We then discuss the evolving relationship between MDOs and deterrence, focusing on how MDOs can be used to increase an adversary's expected costs and risks of escalation and decrease an adversary's expected benefits. We recommend that future MDO/MDD discussions take an objective-oriented approach, focusing on how to shape and integrate MDD efforts to meet broader campaign objectives. We conclude by offering some thoughts on the potential benefits and insights that would be provided by this approach, and on the limits of the MDD concept.

A Growing Interest in Multi-Domain Operations (MDO)

The past decade has witnessed a substantial increase in U.S. military interest in multi-domain operations (MDO). To offer a sense of this increase, one recent U.S. Army compendium of publications lists more than 25 MDO-related studies from the 2016–2019 timeframe alone. These publications deal with the subject at a general level and address a range of specific topics, including targeting, special operations in the gray zone, and employment in joint military exercises.[16]

For the military services, MDO offers a response to the military challenges posed by major power rivals, which have made the exploitation of information, time, and space central to their theories of victory. MDOs are thought to offer the promise

16 U.S. Army Combined Arms Center, *Catalog: Multi-Domain Operations*, No. 19-19 (September 2019). https://usacac.army.mil/sites/default/files/publications/19-19.pdf. Accessed November 24, 2021.

to U.S. warfighters of regaining the initiative in a great power military confrontation by allowing for faster and better decisionmaking, and the calibrated execution of operations from, in, and through multiple domains.

Successful implementation of the MDO concept, it is argued, would present U.S. adversaries with multiple "operational and/or tactical dilemmas" that negate their strengths.[17]

MDO terminology has evolved over time. Earlier discussions tended to speak of "multi-domain battle." More recent discussions focus on the concept of "all-domain operations."[18] Despite these differences, the motivations behind these discussions have been remarkably consistent. There is a robust consensus among DOD leadership, civilian and military, that the ability to successfully operate within and across multiple domains in an integrated fashion is essential to success in future military and geopolitical competition.

Much of the recent thinking on MDO has come from the military services.[19] Their publications tend to treat MDO as a capability to be provided by the services to the Joint Force. Recent examples of this literature include two Army studies (2018, 2021), a joint Army-Marines white paper (2018), and Air Force doctrine (2020).[20]

The Joint Staff has also expressed substantial interest in, and a commitment to, MDO. Most recently, this has been evident under the rubric of All-Domain Operations (ADO). ADO has been the foundational paradigm for the Joint Staff's forthcoming Joint Warfighting Concept, as well as the supporting Joint All Domain Command and Control (JADC2) strategy and infrastructure, both of which are currently under development.[21]

17 This includes assessing the operating environment and responding with multi-domain effects in much less time than is typical for the current pace of operations—a matter of hours, minutes, or even seconds, compared to today's multi-day process of analyzing the operating environment and executing a global response. U.S. Army, "Army Multi-Domain Transformation: Ready to Win in Competition and Conflict," Chief of Staff Paper #1 (March 23, 2021). https://www.army.mil/article/244543/army_releases_information_paper_on_multi_domain_transformation. Accessed November 24, 2021. Miranda Priebe, Douglas C. Ligor, Bruce McClintock, Michael Spirtas, Karen Schwindt, Caitlin Lee, Ashley L. Rhoades, Derek Eaton, Quentin E. Hodgson, and Bryan Rooney, *Multiple Dilemmas: Challenges and Options for All-Domain Command and Control* (Santa Monica, CA: RAND Corporation, 2020).

18 Colin Clark, "Gen. Hyten on the New American Way of War: All-Domain Operations," Breaking Defense (February 18, 2020). https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/. Accessed November 24, 2021.

19 Miranda Priebe et al., Multiple Dilemmas: *Challenges and Options for All-Domain Command and Control.*

20 U.S. Army, "The U.S. Army in Multi-Domain Operations 2028," TRADOC Pamphlet 525-3-1 (December 6, 2018), p17. Headquarters, Department of the Army, *Army Multi-Domain Transformation: Ready to Win in Competition and Conflict, Chief of Staff Paper #1* (March 16, 2021). https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf. Accessed November 24, 2021. For the Army-Marine paper, see Kevin M. Woods and Thomas C. Greenwood, "Multidomain Battle: Time for a Campaign of Joint Experimentation," *Joint Force Quarterly* 88 (January 9, 2018). https://ndupress.ndu.edu/Publications/Article/1411615/multidomain-battle-time-for-a- campaign-of-joint-experimentation/. Accessed November 24, 2021. The Air Force doctrine is Curtis E. Lemay Center for Doctrine Development and Education, *Air Force Doctrine Publication (AFDP) 3-99, Department of the Air Force Role in Joint All-Domain Operations* (October 8, 2020), p30. https://www.doctrine.af.mil/Doctrine-Publications/AFDP-3-99-DAF-Role-in-Jt-All-Domain-Ops-JADO/. Accessed November 24, 2021.

21 Colin Clark, "Gen. Hyten on the New American Way of War: All-Domain Operations," Breaking Defense (February 18, 2020). https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/. Accessed November 24, 2021. See also Theresa Hitchens, "JADC2 Strategy Hits SecDef's Desk 'In Days;' Tech Demos Already Planned," Breaking Defense (April 21, 2021). https://breakingdefense.com/2021/04/jadc2-strategy-hits-secdefs-desk-in-days-tech-demos-already-planned/. Accessed November 24, 2021.

The forthcoming Joint Warfighting Concept is itself noteworthy as it will attempt to synthesize the concept development efforts of the individual services and present a coherent vision for how the U.S. military can leverage ADO/MDO in a future fight against a major power rival.[22]

MDO Efforts Remain Aspirational

Yet for all this churn, the MDO vision and its implementation remain aspirational. The Joint Staff is still working on the Joint Warfighting Concept and the networking capabilities and approaches necessary to support an all-domain fight. Individual services have been assigned key supporting roles for the Joint Warfighting Concept and have been assigned parallel efforts to flesh out key ADO concepts: joint fires (assigned to the Navy), joint command and control (Air Force), and congested logistics (Army).[23] The services are still developing, testing, and evaluating their homegrown MDO-related capabilities and concepts, such as the Army's Multi-Domain Task Forces, and subordinate components like the Intelligence, Information, Cyber/Electronic Warfare, and Space (I2CEWS) battalion.[24]

In addition, conceptual ambiguities persist despite the enormous efforts and investments undertaken by the services and the Joint Staff. There remains no official definition of an operational domain in the DOD dictionary. Nor is there a single accepted definition of a domain in the broader literature. In official statements and documents, U.S. officials alternately treat domains as a physical region, a facet of the operating environment, and an environment through which effects can be delivered. For instance, the former vice chairman of the Joint Chiefs of Staff, General John Hyten, has spoken of ADO as combining "air, land, sea, space, cyber, and [the electromagnetic] spectrum."[25] Others treat the information environment or even cognitive variables as distinct domains. As we discuss below, there is also a lack of clarity on the relationship between MDO/ADO and the multiple deterrence concepts discussed over the past several years, including cross-domain deterrence and integrated strategic deterrence.

22 Tom Greenwood and Pat Savage, "In Search of a 21st-Century Joint Warfighting Concept," War On The Rocks (September 12, 2019). https://warontherocks.com/2019/09/in-search-of-a-21st-century-joint-warfighting-concept/. Accessed November 24, 2021. See also Theresa Hitchens, "Hyten: Joint Requirements for All Domain Out By June," Breaking Defense (May 13, 2021). https://breakingdefense.com/2021/05/hyten-joint-requirements-for-all-domain-out-by-june/. Accessed November 24, 2021.

23 Theresa Hitchens, "COVID Delays Joint Warfighting Concept: Hyten," Breaking Defense (January 22, 2021). https://breakingdefense.com/2021/01/covid-delays-joint-warfighting-concept-hyten/. Accessed November 24, 2021.

24 Sydney J. Freedberg Jr., "BREAKING: New Army Long-Range Units Head to Germany," Breaking Defense (April 13, 2021). https://breakingdefense.com/2021/04/breaking-new-army-long-range-units-coming-to-germany/. Accessed November 24, 2021.

25 Colin Clark, "Gen. Hyten on the New American Way of War: All-Domain Operations," Breaking Defense (February 18, 2020). https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/. Accessed November 24, 2021.

The Growing Sense of Urgency in MDO Discussions

Even a casual observer might note that there is nothing fundamentally new about the practice and concept of MDO. As a recent RAND Corporation study notes, "humans have used armies and navies in tandem for thousands of years."[26] Former Navy Secretary Richard Spencer in 2019 similarly observed "[w]e are in multidomain every single day."[27] To that end, the secretaries of the Army, Navy, and Air Force in 2019 cited multiple examples of MDOs, including the use of an air wing on an aircraft carrier to deliver strikes and project power against naval and land targets, and the use of communications and missile warning satellites to send information directly to forces in the field to guide targeting efforts.[28] Historically, the U.S. military already has wartime experience integrating so-called kinetic and non-kinetic operations across domains. For instance, U.S. military pilots employed electromagnetic spectrum operations in Vietnam to locate, jam, and then defeat Soviet-made radars.[29] What, then, is new about MDO? What is driving the current sense of urgency in MDO discussions?

First, the nature and pace of technological developments over the past decade have significantly increased the perceived complexity of multi-domain warfare. This includes new tools and means of conflict, such as the emergence of offensive cyber capabilities.[30] It includes new threat vectors, such as the concern about cyber threats against critical infrastructure, or the use of counterspace weapons to hobble power projection.[31] It also includes new pathways for escalation, influence, and coercion—and the prospect for increasingly fast decision cycles or observe, orient, decide, and act (OODA) loops. In sum, existing challenges are becoming more complex and difficult, while new challenges of increasing complexity are appearing simultaneously.

Second, there is a perception today—which is hardly unique to the current era—that we rest on the precipice of a technological revolution that is fundamentally changing the nature of competition, deterrence, escalation dynamics, and war. For

26 Miranda Priebe et al., *Multiple Dilemmas: Challenges and Options for All- Domain Command and Control*; Michael Spirtas, "Toward One Understanding of Multiple Domains," The RAND Blog (May 2, 2018). https://www.rand.org/blog/2018/05/toward-one-understanding-of-multiple-domains.html. Accessed November 24, 2021.

27 David Vergun, "Multidomain Operations Rely on Partnerships to Succeed," U.S. Department of Defense News (February 12, 2019). https://www.defense.gov/Explore/News/Article/Article/1755520/multidomain-operations-rely-on-partnerships-tosucceed/. Accessed November 24, 2021.

28 Ibid.

29 James R. Brungess, Setting the Context: *Suppression of Enemy Air Defenses and Joint War Fighting in an Uncertain World* (Maxwell AFB: Air University Press, 1994). https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0054_BRUNGESS_SETTING_CONTEXT.pdf. Accessed November 24, 2021.

30 Jim Garamone, "Esper Describes DOD's Increased Cyber Offensive Strategy," U.S. Department of Defense News (September 20, 2019). https://www.defense.gov/Explore/News/Article/Article/1966758/esper-describesdods-increased-cyber-offensive-strategy/. Accessed November 24, 2021.

31 On critical infrastructure, see National Infrastructure Advisory Council (NIAC), *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017). https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf. Accessed November 24, 2021. On space, see Benjamin Bahney and Jonathan Pearl, "Why Creating a Space Force Changes Nothing," *Foreign Affairs* (March 26, 2019). https://www.foreignaffairs.com/articles/space/2019-03-26/why-creating-space-force-changes-nothing. Accessed November 24, 2021.

many observers, the United States is confronting a technological arms race in which the winner will be able to attain military supremacy and overmatch capability. As General Hyten noted in February 2020:

> *"[all-domain operations are] the biggest key to the future of the entire budget…if we figure that out, we'll have a significant advantage over everybody in the world for a long time, because it's the ability to integrate and effectively command and control all domains in a conflict or in a crisis seamlessly…and…[n]obody knows how to do that."*[32]

General Hyten's comments imply that if the United States does not attain its ADO goals, our adversaries could potentially enjoy such advantages by gaining them first. Although it is not clear if the technologies enabling ADO/MDO will confer first-mover advantages, the U.S. military perceives them as such. These perceptions are driving America's desire to become the first to master MDO.

Third, there is a growing appreciation in U.S. defense circles that key competitor states are organizing around MDO concepts, working hard to develop and integrate these capabilities, and then leveraging these efforts in well-defined theories of victory.[33] There is also a perception in the United States that major power competitors perceive significant first-mover advantages to the adoption and development of critical and emerging technologies.[34] This makes the perceived threat from MDO/ADO—and the perceived risk of falling behind our adversaries—more tangible and more impactful.

From Multi-Domain Operations to Multi-Domain Deterrence

Most treatments of MDO primarily address issues related to fighting and winning wars. Less often discussed is the utility and role of multi-domain capabilities for managing deterrence relationships. The Biden administration has reiterated that deterrence remains the "cornerstone" of U.S. defense strategy, and administration leaders have linked successful deterrence to the development of integrated multi-domain warfighting capabilities.[35] This view is shared by military leaders. For instance,

32 Colin Clark, "Gen. Hyten on the New American Way of War: All-Domain Operations."

33 At the highest level, adversary theories of victory are rooted in a belief that they need to be capable of winning quickly, that they need to be able to impose costs and risks in multiple domains, and that their escalatory threats (and thus deterrence threats) will be most credible if they leverage perceived asymmetries in stake, geography, and governance. See Brad Roberts, *On Theories of Victory, Red and Blue*, Livermore Papers on Global Security No. 7 (Livermore, CA: Lawrence Livermore National Laboratory, Center for Global Security Research, 2020). See also Brad Roberts, *The Case for U.S. Nuclear Weapons in the 21st Century* (Stanford, CA: Stanford Security Studies, 2016).

34 White House, *National Strategy for Critical and Emerging Technologies* (October 2020). https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf. Accessed November 24, 2021.

35 Todd C. Lopez, "Defense Secretary Says 'Integrated Deterrence' is Cornerstone of U.S. Defense," DOD News (May 3, 2021). https://www.navy.mil/Press-Office/News-Stories/Article/2592817/defense-secretary-says-integrateddeterrence-is-cornerstone-of-us-defense/. Accessed November 24, 2021.

one U.S. Army publication argues that "to deter aggression, the Joint Force must have an irrefutable, demonstrated ability to fight and win" using MDOs in support of U.S. power projection capability.[36] However, there does not yet appear to be a consensus amongst DOD leaders on the relationship between MDOs and deterrence. Further, intellectual leaders recognize that there is much more work to do in devising specific operational tools to achieve these deterrence ends in practice, and in transforming a discussion that until now has largely focused on multi-domain operations into one focused on multi-domain deterrence.

Moving from multi-domain operations to multi-domain deterrence requires understanding the requirements for successful deterrence and the ways that MDO can contribute to meeting these requirements. At a basic level there are four elements of any deterrence strategy.

First, whether one is operating in a single domain or in multiple domains, there are two fundamental approaches to deterrence strategy: deterrence by punishment and deterrence by denial.[37] To punish, one threatens to impose costs and risks on an adversary if they take an undesired action. To deny, one attempts to convince an adversary that it will fail to reap the expected benefits from an undesired action, disincentivizing them from attempting to secure such benefits in the first place.

Punishment and denial strategies can take different forms depending on the circumstances. The targets of punishment strategies will vary based on what the adversary prioritizes and values. Denial strategies are likely to vary based on assessments of how the adversary would attempt to secure its aims, how the adversary gauges its probability of winning, how the adversary assesses the importance of a quick victory compared to a war of attrition, and so forth. In practice, however, denial and punishment strategies can overlap. For instance, one element of a denial strategy might be to make an adversary's operations so difficult, uncertain, and complex that it refrains from taking that action. This is synonymous with making adversary operations seem so costly that the adversary is dissuaded from attempting them at all.

There is no requirement that a deterrence strategy opt for either punishment or denial. U.S. policy has long been to leverage both pathways by combining elements of punishment and denial in an overall deterrence strategy. It is nevertheless important to distinguish between the two approaches because they tend to have different informational and capability requirements.

Second, the fundamental task of deterrence is to shape an adversary's behavior by influencing their perceptions of the costs, risks, and benefits of action. The adversary must perceive a tight connection between its actions and the potential outcome. This means that the adversary must perceive that the other side has the will and

36 Department of the Army, Headquarters, *Army Multi-Domain Transformation Ready to Win in Competition and Conflict, Chief of Staff Paper #1.*

37 Glenn Snyder, *Deterrence and Defense* (Princeton, NJ: Princeton University Press, 1961).

ability to follow through on its deterrent threats. As a result, in crafting a deterrence strategy one must closely consider an adversary's specific objectives, risk tolerance, pain points, and force structure when deciding how to apply various tools and tactics. The mix of threats and inducements that would deter one potential adversary are not necessarily those that would deter another. U.S. strategic thought has long recognized the necessity of tailoring deterrence to the specific values, priorities, and capabilities of adversaries.

However, a key component of influencing adversary perceptions is also understanding one's own values, priorities, and risk tolerance. These too must be aligned with a deterrence strategy for the strategy to be credible. For example, future U.S. deterrence strategies likely will need to devote considerable attention to convincing an adversary that the United States has the will to follow through on its deterrent threats in the face of high potential costs for doing so. Against a future peer or near-peer adversary, the United States may find that successfully prosecuting deterrence strategies requires it to accept high costs or a degree of risk that it would prefer to avoid. Signaling credibility will be even more complicated if adversaries perceive themselves to have a favorable asymmetry of stake, particularly in scenarios where the United States is projecting force far from its shores.[38] This is arguably a change from much of the post-Cold War period, during which the United States has possessed overwhelming military superiority, a fact that has tended to make U.S. threats inherently credible.

Third, deterrence strategies can be developed to influence adversaries in a range of situations. At the macro level, deterrence relationships consist of multiple, overlapping, interactive efforts to manipulate costs and risks at critical junctures. The practice of deterrence is not only to prevent discrete actions but to shape broader political and military outcomes toward a desired end state. Some deterrence theorists refer to this distinction as the difference between general and immediate deterrence. Even if an adversary is not deterred from attempting to challenge the status quo (general deterrence) it might still be deterred from resorting to armed conflict or engaging in certain forms of violence (immediate deterrence). The requirements for deterring these different actions are likely to vary significantly. Nevertheless, the basic framework for a deterrence strategy—manipulating an adversary's perception of possible risks and rewards—applies across these circumstances. Further, deterrence is relevant across the spectrum of competition—from peacetime to crisis and war and through war termination. Deterrence strategies must be concerned with the large as well as the small.

Finally, to have a meaningful and tangible discussion about the application (as opposed to the theory) of deterrence, it is essential to consider concrete scenarios of interest involving specified aims and particular adversaries. This means identifying

38 Brad Roberts, "A Review and Assessment from an American Perspective," in Brad Roberts, ed., *Taking Stock: U.S.-China Track 1.5 Nuclear Dialogue* (Livermore, CA: Lawrence Livermore National Laboratory, Center for Global Security Research, 2020), p23.

who is adopting the deterrence posture, who they are seeking to deter, what action(s) they are seeking to deter, and how they are seeking to deter those actions. Crafting a general deterrence strategy may involve a wide-ranging review of how both military and non-military tools of statecraft can be combined to shape an adversary's view of the risks and rewards of revisionist behavior. General deterrence may also require moving beyond the traditional American approach to deterrence, which aims to influence an adversary's willingness to do something it would otherwise do, and to consider other influence strategies—such as dissuasion—which aims to influence an adversary's desire to do something in the first place.

In contrast, crafting an intra-crisis or intra-war deterrence strategy likely requires an understanding of the escalation dynamics of particular conflicts, and how adversaries are likely to choose from among available options across phases and types of conflict. Without this understanding, it would be difficult for the United States to anticipate how to deter such escalation. Crafting intra-crisis and intra-war deterrence strategies may require the development of a range of detailed scenarios and potential responses, informed by a robust understanding of adversary priorities, capabilities, doctrine, escalatory thresholds, and risk perceptions.

Ultimately, deterrence requires convincing the adversary that its "theory of victory" is flawed and if implemented, will result in costs that far exceed potential gain. It also requires convincing them that their attempts to escalate out of a situation are likely to fail because escalation does not provide them with a clear or easy path to victory, and instead risks the adversary finding itself in a far more damaging situation should it choose to escalate. Finally, overall deterrence of conflict and war is bolstered by developing credible capabilities to affect the adversary's escalation calculus.

With these points in mind, let us turn to the concept of multi-domain deterrence (MDD). Arguably, the United States already has a strong general foundation in deterrence strategy and theory, but more work needs to be done to understand the requirements of MDD and the complications introduced in deterring a resolved major-power adversary.

The first step is to recognize that MDD, like MDO, is already a well-established practice in some areas, providing a basis on which to build a more robust strategic framework. Indeed, while the concept of MDD is often treated as something new, the reality is that MDD is already a core part of the U.S. deterrence equation. In fact, the MDD concept may be inherently appealing to U.S. observers precisely because it carries a sense of familiarity.

U.S. nuclear deterrence provides an illustrative example. Here, it is widely believed that the credibility of our nuclear deterrent lies not only in the weapon systems and our force structure, but also in the efficacy of capabilities in multiple domains for

nuclear command, control, and communications (NC3) and early warning.[39] Similarly, one might observe that fleet ballistic missile submarines must master the maritime domain to generate effects on land with support from capabilities on land, in air, and in space. Modern nuclear deterrence is a highly multi-domain operation.

The United States has also undertaken MDD operations in a crisis atmosphere. For example, in the 1995-1996 Taiwan Straits Crisis, the United States responded to Chinese missile tests, force mobilizations, and naval and amphibious exercises by eventually sailing the USS Nimitz and her battle group through the Taiwan Strait, while at the same time pursuing diplomatic activities to manage the crisis.[40] Although the military dimension of the U.S. response reflected some degree of symmetry with Chinese actions, the response was also arguably a prime example of MDD in action.

If MDD is not new, then why does it tend to be perceived as such? One plausible explanation is that the growing number of MDD tools, threat vectors, and escalation pathways make our current situation seem novel. For instance, one can posit many hypothetical threat scenarios today that were largely unimaginable 10-20 years ago, such as the use of cyber tools to degrade nuclear deterrence-related infrastructure, the use of counterspace weapons as a counter-integrated air defense system (IADS) tool, and the use of artificial intelligence (AI)-enabled information warfare tools to influence public opinion or augment human decision making. Little is understood about how such hypothetical activities would impact deterrence across different scenarios. Meanwhile, MDD planning efforts are accelerating, as evidenced by senior U.S. military officials' efforts to craft a "global integration of deterrence," or "the use of all means…to make potential enemies think twice about attacking," according to a recent media report.[41]

This combination of significant and growing interest in a multi-domain approach to deterrence, coupled with a recognition of the complexities of such an approach, suggest that much more work remains in crafting a deterrence strategy that leverages MDO for strategic effect. While MDO and MDD are well-established facets of our military planning and activities, the relationship between operations and deterrence remains poorly understood and defined. In moving from MDO capabilities and doctrine

39 U.S. Strategic Command, "Statement of Charles A. Richard, Commander, United States Strategic Command, Before the Senate Committee on Armed Services," (February 13, 2020), https://www.stratcom.mil/Portals/8/Documents/2020_USSTRATCOM_Posture_Statement_SASC_Final.pdf, accessed December 1, 2021; Joint Chiefs of Staff, "Joint Publication 3-14, Space Operations April 10, 2018," *Incorporating Change* 1 (Revision October 26, 2020), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14ch1.pdf?ver=qmkgYPyKBvslZyrnswSMCg%3D%3D, accessed November 24, 2021; Curtis E. LeMay Center for Doctrine Development and Education, "Air Force Doctrine Publication (AFDP) 3-72, Nuclear Operations: Nuclear Command, Control, and Communications" (last updated December 18, 2020); U.S. Space Force, "Fact Sheet: Space Based Infrared System" (March 22, 2017), https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197746/space-based-infrared-system/, accessed November 24, 2021; U.S. Department of Defense, *Nuclear Posture Review* (2018); U.S. Space Force, "Fact Sheet: Upgraded Early Warning Radars" (March 22, 2017), https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197738/upgraded-early-warning-radars/, accessed November 24, 2021.

40 Douglas Porch, "The Taiwan Strait Crisis of 1996: Strategic Implications for the United States Navy," *Naval War College Review* 52, no. 3 (Summer 1999), pp15-48; Allen S. Whiting, "China's Use of Force, 1950-96, and Taiwan," *International Security* 26, no. 2 (Fall 2001), p122; John F. Copper, *Taiwan's Mid-1990s Elections: Taking the Final Steps to Democracy* (London: Praeger, 1998), p130.

41 Colin Clark, "Gen. Hyten on the New American Way of War: All-Domain Operations."

to a MDD strategy, the United States needs to think as broadly as possible about how MDO can be used to increase an adversary's expected costs and risks of escalation while decreasing an adversary's expected benefits.

One might counter that the concept of using MDOs to pose multiple dilemmas to an adversary is relevant to deterrence. However, DOD has tended to focus on this concept of multiple dilemmas in an operational sense, rather than in terms of deterrence. Thus, notwithstanding the deterrence benefits of a credible warfighting capability, there remains important ground to tread in more explicitly linking the multiple dilemmas concept to deterrence strategy.

In recent years, DOD has begun advancing key MDD-related concepts and capabilities, including those in support of the European Deterrence Initiative (EDI) and Pacific Deterrence Initiative (PDI). Yet the prevailing approach in these efforts seems to be guided by a limited form of deterrence by denial—meant to convince the adversary that fighting will not be profitable—coupled with the pursuit of overmatch capability. Such efforts will need to be expanded in the coming years.

More broadly, the threat environment is evolving, and we do not yet have good insight into which of its aspects are fundamentally changing, and which will continue to resemble the past. How to integrate the growing number of MDO capabilities into our deterrence activities, to better understand their various impacts on deterrence relationships, to determine the right degree of integration, and to understand the overlap between deterrence requirements and warfighting will all be critical questions to address moving forward.

Toward an Actionable Agenda for MDD

What tangible steps can we take toward crafting an actionable MDD agenda? What should be our core organizing principles in this endeavor? We contend that a singular focus on improved multi-domain capabilities likely will not make the MDD challenge more tractable. Instead, we recommend a shift from a capabilities-oriented approach toward a scenario-based, objectives-oriented approach. As the National Defense Strategy Commission argued in 2018:

> *The United States needs more than just new capabilities; it urgently requires new operational concepts that expand U.S. options and constrain those of China, Russia, and other actors…The unconventional approaches on which others rely, such as hybrid warfare (warfare combining conventional and unconventional elements), gray-zone aggression (coercion in the space between peace and war), and rapid nuclear escalation demand equally creative responses…Unfortunately, the innovative operational concepts we need do not currently appear to exist. The United States must begin responding more effectively to the operational challenges posed by*

our competitors and force those competitors to respond to challenges of our making.[42]

The Commission's points about operational concepts arguably apply just as well to deterrence-related issues.

The EDI and PDI are important examples of real-world efforts to meet these needs, including by folding up multi-domain capabilities into an objective-oriented, region-specific framework. The current focus on operational capabilities like pre-positioned and distributed forces, integrated air and missile defense, ground-based long-range fires, and persistent ISR are an important step forward.[43] However, there remains significant conceptual work ahead in terms of mapping such capabilities to coherent deterrence frameworks, as well as practical work, including through experimentation, exercises, and continued force posture evolution.

In addition, these initiatives will likely need to be expanded beyond a limited form of deterrence by denial to include: efforts to signal to an adversary in peacetime that it is unlikely to succeed, efforts to support rapid force application to dispel adversary confidence if deterrence fails, efforts to signal to an adversary that the United States has the will to assume substantial risk and costs in service of its strategic aims, and so forth. These and other considerations are important to supporting a comprehensive and effective deterrence strategy.[44]

As these and other efforts move forward, our core organizing principle and starting point for planning should encompass the adversary's theory of victory and our own. First, since MDD strategies are ultimately about influencing an adversary's behavior—e.g., by increasing their expected costs and risks of escalation, or by decreasing their expected benefits—they should be targeted at negating an adversary's metrics of success. At the highest level, our key competitors likely believe that success depends on keeping a war with the United States short, on being able to credibly threaten the United States and our allies with costs and risks in multiple domains to induce restraint, and on leveraging perceived asymmetries in stake, geography,

42 National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (2018), pviii.

43 Philip Davidson, "Transforming the Joint Force: A Warfighting Concept for Great Power Competition," speech given at West 2020, San Diego, CA (March 3, 2020). https://www.pacom.mil/Media/Speeches-Testimony/Article/2101115/transforming-the-joint-force-a-warfighting-concept-for-great-power-competition/. Accessed November 24, 2021.

44 In addition, there are other forms of deterrence by denial, aside from what some have labeled a Clausewitzian conception of deterrence, in which deterrence depends on convincing an adversary that there is a high likelihood that the United States will win in a decisive battle. A complementary approach to deterrence by denial would place increased emphasis on ambiguity, deception, unpredictability, and dissuasion to "win without fighting." A non-Clausewitzian approach to MDD would also consider how MDO might be leveraged to influence adversary psychology, emotions, domestic divisions, and so forth to deter an adversary from taking unwanted actions. In some instances, such approaches might provide a pathway to achieve political objectives, especially in situations where a decisive operational victory is seen as elusive or excessively costly. Greater clarity about the underlying logic of how MDO translates into deterrence outcomes would help highlight where operational and deterrence requirements overlap and where they diverge, potentially requiring unique concepts and capabilities for each.

and governance.[45] Thus, targeted MDD strategies should seek to prevent them from achieving a quick victory, denying the ability to impose meaningful effects in multiple domains, and reducing key asymmetries.

Second, MDO and MDD planning should focus on the United States' own emerging theory of victory. While part of the U.S. theory of victory necessarily includes thwarting that of an adversary, this theory will likely also have (and need to have) its own distinct priorities and aimpoints. MDD and MDO frameworks should incorporate these "pro-active" elements of the U.S. theory of victory as well as those objectives that respond to adversary moves and counter-moves.

In short, there is a need to design MDD campaigns around objectives, rather than tactics. A representative list of these campaign objectives might include the following:

- Prevent Red from imposing faits accomplis on the United States and our allies
- Prevent Red from rapidly escalating out of a conflict via a limited regional nuclear strike
- Prevent Red from taking a specific action (e.g., strikes against critical infrastructure or NC3)
- Force Red to solve multiple dilemmas and/or escalate out of proportion with the expected benefit of an action (e.g., require a sharp escalation to achieve a minor goal, or prevent them from keeping a conflict contained)
- Force Red to choose between core goals and increase required investments to achieve each of them
- Force Red down pathways that increase U.S./allied commitment and escalation credibility
- Force Red to operate in a more symmetric environment (e.g., by turning an away game into more of a home game)
- Shape the future geopolitical environment in a favorable way for Blue interests (e.g., by strengthening key institutions, alliances, and creating a more stable balance of power)

A campaign-focused approach provides a U.S. response to the strategic campaigns envisioned by key competitor states. Russian military thinkers, for instance, envision a number of strategic campaigns designed to contribute to a political victory against the United States and its allies.[46] Chinese military thinkers also focus on a number

45 Brad Roberts, *Theories of Victory, Red and Blue*, Livermore Papers on Global Security No. 7 (Livermore, CA: Lawrence Livermore National Laboratory, Center for Global Security Research, 2020); and Brad Roberts, *The Case for U.S. Nuclear Weapons in the 21st Century* (Stanford, CA: Stanford Security Studies, 2016).

46 Michael Kofman, Anya Fink, and Jeffrey Edmonds, *Russian Strategy for Escalation Management: Evolution of Key Concepts* (Center for Naval Analyses, 2020); Dave Johnson, *Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds*, Livermore Papers on Global Security No. 3 (Livermore, CA: Lawrence Livermore National Laboratory, Center for Global Security Research, 2018).

of joint and deterrence campaigns.[47] For both Russian and Chinese thinkers, the framework of strategic campaigns provides a way to make sense of the complexities of multi-domain strategic competition and warfare.

From this notional list of objective-oriented MDD campaigns, we might infer that we are on the right track toward supporting PDI/EDI goals by developing capabilities such as ground-based long-range fires and distributed pre-positioned forces and equipment (e.g., to even out the conventional balance and prevent faits accomplis), space-based persistent ISR (e.g., to reduce surprises and improve targeting), integrated air and missile defense, and forward-deployed homeland missile defense assets (to limit Red power projection in the region and vertical escalation options). Other efforts supporting these goals are the creation of multi-domain task forces and related units such as the Army's I2CEWS unit established to counter China (with a second one planned for Russia) and the development of resilient space architectures (e.g., to increase the costs and deny the benefits of striking these assets).[48] Strikingly, much of this capability development seems to focus on better integrating our existing or potentially upgraded technology rather than on futuristic tools. This suggests that we should be cautious about overweighting the importance of futuristic technology in prosecuting successful MDO/MDD campaigns for at least the near term, notwithstanding the potential value of new technologies.

This notional list of objective-oriented MDD campaigns also suggests, once again, that our future deterrence posture should probably devote at least as much attention to strategies of denial as to strategies of punishment. While reciprocal strike capabilities can, in theory, be an important part of the MDD mix, it is plausible that strategies of punishment will be relatively less important in the future for achieving the aims of a status quo power like the United States.

The Limits of MDD

As we have argued, there is a critical and growing need for the United States to evolve our MDD concepts, strategy, and capabilities. We believe that a campaign-oriented approach would be particularly helpful for advancing these ends. However, we also believe that it is important to properly calibrate our expectations about MDD and its limitations, of which there may be several.

First, we believe that much of the MDD challenge moving forward is likely to be concerned with conventional conflict or competition below the level of armed conflict. If this is indeed the case, there are several implications. If MDOs and new technologies make low-cost, low-risk offense more attainable, then we may need to

47 Zhang Yuliang, *Science of Campaigns* (Montgomery, AL: PLA Academy of Military Science, 2006), translated by China Aerospace Studies Institute, Air University. https://airuniversity.af.edu/Portals/10/CASI/documents/Translations/2020-12-02%20In%20Their%20Own%20Words-%20Science%20of%20Campaigns%20(2006).pdf Accessed December 7, 2021.

48 Sydney J. Freedberg Jr. and Colin Clark, "Hack, Jam, Sense & Shoot: Army Creates 1st Multi-Domain Unit," Breaking Defense (January 24, 2019), https://breakingdefense.com/2019/01/hack-jam-sense-shoot-army-creates-1st-multi-domain-unit/, accessed December 7, 2021; Department of Defense, *National Security Space Strategy Unclassified Summary* (January 2011), https://www.hsdl.org/?view&did=10828, accessed December 7, 2021.

be prepared for even the best MDD strategies to fail. The history of conventional deterrence, after all, is far less strong than the history of nuclear deterrence. The implication here is that MDD strategists may need to treat deterrence as a dynamic enterprise that requires regular recalibration.

By the same token, however, adversaries' belief in the ability to fight a purely conventional war depends on the continued credibility of nuclear deterrence. Ironically, U.S. success in prosecuting an MDO/MDD strategy might lead adversaries to attempt to compensate for U.S. overmatch through threats of nuclear brinkmanship and escalation. MDO and MDD concepts should seek to avoid creating perverse adversary incentives that may escalate to nuclear use. However, it may also be difficult to dispel such incentives outright if the United States succeeds in mastering MDO. Consequently, U.S. deterrence strategy will need to consider how to manage such risks as its MDO capabilities mature.

A related problem arises from the coexistence of multi-domain warfighting capabilities with increasingly intense forms of political and societal warfare. Whereas the animating concern for the Defense Department is the integration of multi-service and multi-domain capabilities for military effect, national leaders may also have to contend with non-military or non-kinetic forms of strategic conflict that may take place alongside more traditional armed conflict. U.S. deterrence strategy will also need to consider the efficacy of MDD for preventing non-military acts that are militarily and politically significant.

Second, greater dependence on MDD may substantially increase the challenge of credibly signaling deterrence threats to an adversary. MDD is premised not on leveraging weapon systems across domains, but rather on the effective integration of capabilities from multiple domains for deterrence effect. The operational advantages of integrating multiple systems across domains may not be transparent or legible to outsider observers, including potential adversaries. If we develop a strong set of MDD capabilities, but our adversaries are unable to properly calibrate risk due to ineffective signaling and communication, even the best strategies and tools may not have the desired deterrent effect. It is unclear for now whether this signaling limitation will be an inescapable part of the practice of MDD. Regardless, we will likely need to figure out how to simplify and enhance our signaling posture moving forward.

Third, it is not yet clear how the adoption of MDO and the development of MDD approaches will affect the need to provide national leaders with credible escalation management options. MDOs promise warfighters the ability to make decisions at the speed of information, but escalation management may also require capabilities to exert downward pressure on the pace and intensity of military operations. Given the services' interest in doing more complex tasks faster, there may be fewer incentives for MDO planners to incorporate de-escalation and war termination into operational concepts, and fewer opportunities for implementing them in practice. Consequently, MDD strategists may find peculiar challenges to controlling escalation during MDOs. This suggests a disconnect between the logic of MDOs and MDDs, which strategists

on both sides of the equation will need to address to provide sufficient opportunities for escalation management.[49]

Finally, even if the United States develops mastery over MDO and strengthens the connection between MDO and MDD, it may still face persistent and inherent asymmetries in power projection capabilities in a range of scenarios. Multi-domain operations cannot fully overcome the geographical advantages of potential U.S. adversaries. Reducing these asymmetries likely will require maintaining and growing ally and partner willingness to run risks for joint benefit. In other words, MDO and MDD will not obviate the basic reality that U.S. security depends on its alliance relationships. This in turn requires an appreciation of the asymmetries of stake and exposure to risk that define U.S.-alliance relationships. Ultimately, the most sophisticated MDD strategies and capabilities will not be a substitute for this classic problem of extended deterrence as we look to the future.

49 This dynamic could be stabilizing in some cases if the United States is able to credibly signal that it will not be able to precisely control the pace and nature of escalation. But such strategies could prove dangerous if they open the door to runaway escalation.

On the Hierarchy of Domains

Michael Markey

As technological innovation continues to open up new domains for military competition and conflict, a question naturally arises about whether effective deterrence requires that the United States and its allies achieve dominant positions in each and every domain. An affirmative answer is suggested by the argument in which a chain is only as strong as its weakest link. In deterrence strategy, the weakest link equates with any domain where one side enjoys superior means to impose costs upon its adversary and also to protect itself from whatever costs the adversary might seek to impose. Accordingly, there is a widespread expectation that multi-domain competition can intensify and destabilize Great Power relations.

But there is another and better way to think about this question. In fact, all domains are not equal from the perspective of their relevance to the nature and dynamics of particular conflicts. In any particular conflict, a hierarchy of domains can be discerned. Victory will likely go to the actor who better understands and prepares for that hierarchy. This way of thinking is reinforced by the observation that history is unkind to powers that have bet on innovative new military technologies without first reflecting on and developing the needed strategic thought about conflict.

Thinking Hierarchically

That rising powers are interested in disruptive new technologies and their military applications should come as no surprise. For rising powers, investments in such technologies and applications are generally irresistible. The novelty seems to promise a future position of military dominance in the new domain that will produce decisive strategic advantages against the military strengths of an established hegemon. These expectations are reinforced by a conviction that hegemons are slow to adapt to paradigm-shifting innovations because they are wedded to what worked for them previously and have become conservative and risk averse.[50] Risk-tolerant rising powers may then embrace new technologies in pursuit of first-mover advantages. As Michael Horowitz argues:

> *"First movers that innovate and generate new ways of producing military power can gain significant advantages; the exploitation of these advantages then can usher in power transitions, exposing status quo powers that can become overmatched paper tigers. Rising powers that become first movers are especially likely to experience large gains in relative power".*[51]

50 Robert Gilpin, *War and Change in World Politics* (Cambridge: Cambridge University Press, 1981).

51 Michael Horowitz, *The Diffusion of Military Power* (Princeton, NJ: Princeton University Press, 2010).

Conspicuously, those large gains—if achieved—can prove to be short-lived because most Great Power conflicts are not resolved via quick victory; rather, they devolve into a war of attrition. Cathal Nolan has observed that great power conflicts in the modern period have "nearly always proved in the end to be attritional."[52] Furthermore, the decisive actions of these attritional wars have almost always occurred in the land domain, whatever other domains might have been in contention at the outset. Even the influential naval theorist Julian Corbett argued for the importance of the land domain over the maritime when he argued shaping actions occur at sea but the center of gravity for any nation is on the land.[53] We can see examples of this phenomenon in 20th century great power clashes when dominance in the air and undersea domain, while threatening—like that achieved by Germany in the First and Second World Wars—was not capable of undermining land and maritime power of Allies; to win a great power conflict, a state must win an attritional battle for the contested space and, so far at least, this space has almost always been in the land domain.

This is not to say, however, that most domains can be ignored at the expense of the land domain. Although the land domain is the center of gravity for most states in most conflicts, it is possible to discern a multi-domain web of influence built around it. Some domains, like the maritime and air domains, may be utilized to directly influence or shape operations on the land. This results from strikes against land targets from the sea or air, the entry of forces by air or sea, and interdiction of lines of communication and supply. Other domains influence the land domain more tangentially by acting on the maritime or air domains. Undersea dominance, for example, impacts land operations mostly via influencing the maritime domain via the sinking of merchant ships or warships; the use of submarines for cruise missile strikes allows for some direct impact on land. Newer domains, like outer space and cyberspace, are capable of influencing actions in the land domain by enhancing command and control (or degrading the adversary's command and control), but as of 2021 are incapable of producing decisive kinetic effects on the battlefield as significant as those emanating from the air and maritime domains (see Figure 1).

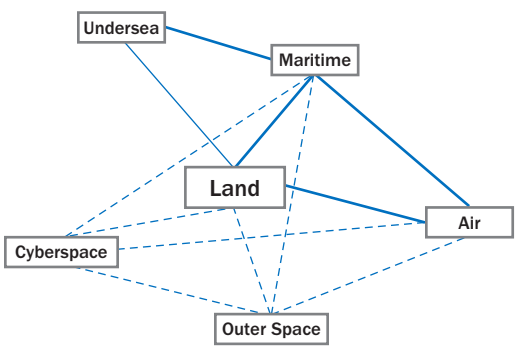


Figure 1. Hierarchy and Connectivity Between Domains. The land domain occupies the center of the hierarchy as the decisive domain. Lines show interactions across domains and the ability to shape or influence other domains. Solid lines connote kinetic, battlefield effects while dashed lines are less impactful or secondary effects, like enabling effective communications or disrupting lines of communication.

52 Cathal Nolan, *The Allure of Battle* (New York: Oxford University Press, 2017).

53 Julian Corbett, *Some Principles of Maritime Strategy* (1911).

Another perspective on assessing the maturity of a domain is whether military forces in a particular domain can directly impact operations in other domains. In other words, the more easily power is translated across domains then the more mature the domain. We can also surmise that innovations that enable seamless translation of force across domain boundaries—enabling cross- and multi-domain operations—are those that are most likely to upset military balances and provide for competitive advantage. Without the development of such innovations, a rising power's hope to undermine U.S. military superiority by dominating an emerging domain will likely be dashed.

Establishing Priorities

In meeting the demands of multi-domain competition, the United States has so far emphasized assembling the chain and then strengthening the weak links. There are two alternatives to this approach. One is to prioritize more robust capabilities in what is considered the oldest land, air, maritime, and undersea domains while also increasing investments in what appears to be the maturing outer space and cyberspace domains. These new investments should focus on the aforementioned innovations that enable the transition of military power from and through the new domains into the more decisive and mature domains. The logic of such a posture is that it hedges against a strategic surprise and ensures sufficient capabilities are in place for flexible multi-domain deterrence (MDD) posturing against potential adversaries. The other alternative is to tailor capability development to the particular requirements of the types of conflicts for which U.S. adversaries are preparing.

The leaders of China and Russia have clearly signaled their desire to remake the regional orders in Asia and Europe by weakening regional institutions, pushing America out, and dominating former U.S. allies. They seek to accomplish this by deterring intervention of American air and maritime forces with salami-slicing political strategy to slowly re-make the status quo. Their military planners have relied primarily on ground-based anti-access/area denial (A2/AD) assets, like robust integrated air defenses or anti-ship cruise and ballistic missiles, to threaten U.S. superiority in the air and maritime domains while slowly building capabilities to execute a fait accompli or coup de main. They have also placed large bets in the new cyberspace and outer space domains, hoping these new domains will prove decisive in undermining U.S. dominance in the older domains.

As a result, China and Russia both have a robust understanding of multi-domain deterrence and have integrated their conventional forces in a manner to support operations in, through, and across domains.[54, 55] Overall, Russia has put its primary emphasis on the land domain, while China has focused primarily on the maritime domain. Overall, their MDD postures and operational capabilities are formidable. What tailoring does this require of the United States and its allies and partners?

54 Dima Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy." *Proliferation Papers* No. 54, IFRI (November 2015).

55 Dean Cheng, "How China's Thinking About The Next War," Breaking Defense (May 19, 2021).

America's military posture in East Asia is aimed primarily at deterring Chinese attempts to upset the status quo via a fait accompli. The most worrying scenario involves an attempt by Beijing to capture Taiwan by force. The decisive domain in this conflict, unsurprisingly, is the land domain. But this is a domain in which the United States has no capabilities to bring to bear. Instead, we seek to deter this Chinese action by threatening to raise Chinese costs, via punishments, by attacking Chinese assets and capabilities in other domains. Some of these threats could directly impact China's ability to support an invasion of Taiwan by disrupting Chinese shipping or preventing Chinese air operations over Taiwan, or increasing the costs for China in other spheres, by conducting cyber attacks against critical infrastructure. However, these deterrents are not as credible as direct obstacles in the critical land domain.

Efforts to deter a revanchist Russia are similarly focused on preventing a fait accompli in the land domain. Here too the United States is significantly underinvested and compensates with reliance on multi-domain means to deter Russian aggression with the threat of various actions that would raise the costs for Russian aggression.

In both cases, the current U.S. deterrent posture looks largely sufficient for purposes of deterrence. Despite decades of effort and significant investments to prepare for regional wars against U.S.-backed alliances, the leaders of China and Russia have proven reluctant to directly challenge U.S. military means or American resolve to defend allies. This is not an argument, however, for complacency. Intent can change much more quickly than capability and we are entering a more dangerous phase when Russian and Chinese leaders may perceive a limited window of relative strength from which to engage in militarily risky opportunistic aggression. Similarly, future political crises could undermine the regime stability in Beijing or Moscow and external aggression has been a gambit for consolidating domestic public support by dictators in the past.

On Allies and Partners

One of the virtues of MDD is the opportunity it presents for new forms of burden sharing among the United States and its allies and partners. Such sharing has the twin benefits of increasing capacity while reducing costs.

Consider first a Taiwan contingency. For the critical land domain, Taiwan can and should contribute the needed defensive capabilities. For the maritime domain, Taiwanese land-based, long-range attack capabilities can and should complement U.S. strike assets. The United States can and should invest in a MDD posture that scales across the region—including other allies, like Australia and Japan, if possible and appropriate—and offers a more flexible strategic posture. In this vision, the United States acts as a force multiplier for regional partners who invest in less mobile, land-based deterrents while depending on the U.S. to compete with China in other supporting domains.

A NATO/Russia contingency has similar considerations. NATO members under direct Russian threat, like the Baltics and Poland, can and should focus investments on

deterrents in the land domain, while the more multi-domain capable states, like the United States, the UK, and France, provide other aspects of the MDD posture and augment the land domain as appropriate. Linking investment in the most important domains to partners with the greatest stakes bolsters the credibility not only of their conventional deterrent but also the extended deterrence guarantees of the United States.

Russia's Approach to Modern Strategic Conflict

Jacek Durkalec

Over the last three decades, Russia has studied the U.S. way of war that triggered "a fundamental reappraisal" of Moscow's approach to modern strategic conflict.[56] While this "reappraisal" was initially largely unnoticed in the West, this changed after 2014 when Russia embarked on its aggressive actions against Ukraine—part of an overall campaign to upend the post-Cold War European security order. What the Western analysts discovered is how far Russia has gone in conceptualizing modern conflict and translating its ideas and concepts into concrete capability investments and actions.[57] This chapter seeks to explain key elements of Russia's approach to modern strategic conflict. It explores key drivers of Russia's preparation to modern strategic conflict, key pillars of its approach, and Moscow's plans on how to remain competitive in the future.

Drivers

Russia's preparations for a modern strategic conflict gained a new speed after the 2008 Russia-Georgia war. Shortcomings of Russia's military performance triggered ambitious military reform initiated by defense minister Anatoly Serdyukov. However, the perceived urgency to transform Russia's military to realities of modern war preceded the conflict with Georgia and was motivated by several external and internal factors.

For Russia's political-military leadership, the rebuilding of military muscles was essential for Russia's survival as a sovereign state—that is, a state that has power to actively shape regional and global developments according to its own interests. The disarray and chaos of the 1990s and perception that Russia's interests were largely ignored by the West fueled a narrative that the United States and its allies took advantage of the vacuum created by the collapse of the Soviet Union. If Russia

56 Brad Roberts, *Toward New Thinking About Our Changed and Changing World: A Five-Year CGSR Progress Report* (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2020), p14. https://cgsr.llnl.gov/content/assets/docs/CGSRfiveDIGITAL.pdf. Accessed September 3, 2021.

57 This was highlighted by a series of Center for Global Security Research (CGSR) workshops and publications on multi-domain strategic competition and deterrence that put an emphasis on understanding the wars that U.S. major adversaries are getting to fight. For a summary of CGSR findings, see: Brad Roberts, *Toward New Thinking About Our Changed and Changing World: A Five-Year CGSR Progress Report*, op. cit., pp14-20. Relevant CGSR workshop summaries include: "De-Escalation and War Termination In Multi-Domain Regional Wars," May 25 and 26, 2021; "The 2021 Defense Strategy Review and Modern Strategic Conflict," December 15-17, 2020; "Winning Conventional Regional Wars Against Nuclear-Armed Adversaries," November 20-21, 2019; "Multi-Domain Strategic Competition: Rewards and Risks," November 13-14, 2018; "Strengthening Deterrence for 21st Century Strategic Conflicts and Competition: Accelerating Adaptation and Integration," November 14-15, 2017; and "Countering Russia's Strategy for Regional Coercion and War," January 19-20, 2016. All summaries are available at https://cgsr.llnl.gov/workshops.

wouldn't push back, the narrative continued, it would be "destroyed and enslaved."[58] The distrust of Russia's ruling elite to the United States was further incited by fears of a Western-sponsored "color revolution" that would lead to a regime change. The result of these deeply embedded perceptions was that Russia was in a strategic competition with the United States and its allies long before the phrase "strategic competition" returned to the Western lexicon.

The process of transforming of Russia's military was also driven by sober recognition of its military weaknesses. The U.S. military actions against Iraq in 1991, Kosovo in 1999, Afghanistan in 2001, and Iraq in 2003 demonstrated the unprecedented ability for America to globally project its power. In contrast, the two Chechen wars and war with Georgia, even if successful, demonstrated how unfit the Russia military was to compete with relatively weak military opponents.

While preponderance of the U.S. military during this unipolar moment was a point of reference for Russia, it was not a model. For Moscow's political and military leadership, emulating the Western way of war was neither feasible nor desirable. Instead, the country directed its focus on identifying key asymmetric strengths that it could exploit to its own advantage, as well as on negating key Western strengths. By choosing to act asymmetrically, Russia's leadership chose to compete and seek dominance in areas that the West was unwilling to engage in due to inability or unpreparedness; resorted to ways and means that are rejected by Western standards; leveled the playing field by outmatching quality with quantity; and exploited its unique advantage gained from quick decisionmaking and follow-up actions provided by its political system and geography.

Russia's adaptation to requirements of modern strategic conflict was oriented towards the future. It was informed by assessments of projected changes in military balance that were based on the military foresight about the future character of warfare.[59] Russia's political and military leaders took into account what kind of capabilities the United States may obtain in the future and actively worked to neutralize any potential military advantage that the United States might gain.

> *"We stopped paying the required attention to defense and security issues… Furthermore, our country, formerly protected by the most powerful defense system along the length of its external frontiers overnight found itself defenseless both from the East and the West. It will take many years and billions of rubles to create new, modern and genuinely protected*

58 Robert Kupiecki and Marek Menkiszak, eds., Interview with Defense Minister of the Russian Federation Sergey Shoygu for *Moskovskiy Komsomolets, Documents Talk. NATO–Russia Relations after the Cold War* (Warsaw, Poland: Polish Institute of International Affairs, 2020), p598. https://www.pism.pl/upload/images/artykuly/b36eaf82-d6e0-44d1-b335-55a2be0bd15d//1621865078970.pdf. Accessed September 3, 2021.

59 General of the Army Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces, "The Value of Science is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review* (January-February 2016). https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf. Accessed September 3, 2021.

borders… In general, we need to admit that we did not fully understand the complexity and the dangers of the processes at work in our own country and in the world. In any case, we proved unable to react adequately. We showed ourselves to be weak. And the weak get beaten".

-Vladimir Putin, 2004[60]

"…we still spend 25 less on defense than the United States… Our responses will be asymmetrical, but they will be highly effective…"

-Vladimir Putin, 2007[61]

"Forms of armed conflicts are becoming increasingly sophisticated. The efficacy of an armed conflict and victory always lie with those who have the strongest spirit and better weapons than their opponents, and who use them better than a potential enemy… We need to take a modern approach in our thinking; we always need to work with an eye toward the future."

-Vladimir Putin, 2013[62]

"… we need to be very astute in tracking any changes in the balance of forces and military-political developments in the world, especially along the Russian border, and take timely action to adjust plans so as to neutralize potential threats our country may face…"

-Vladimir Putin, 2016[63]

"…If the West continued to behave as it did during the period of Gorbachev's rule… I think they would have succeeded in accomplishing the task they set themselves—the task of destroying and enslaving our country… in 1999, the process of returning to commonsense began…."

-Sergey Shoygu, 2019[64]

Pillars

Russia's military transformation to requirements of modern strategic conflict was deliberate, focused, and long term. This process is still ongoing. What has radically

60 President of Russia, "Address by President Vladimir Putin" (September 4, 2004). http://en.kremlin.ru/events/president/transcripts/22589. Accessed September 3, 2021.

61 President of Russia, "Transcript of Press Conference with the Russian and Foreign Media" (February 1, 2007). http://en.kremlin.ru/events/president/transcripts/24026. Accessed September 3, 2021.

62 President of Russia, "Expanded meeting of the Defence Ministry Board" (December 10, 2013). http://en.kremlin.ru/events/president/news/19816. Accessed September 3, 2021.

63 President of Russia, "Expanded meeting of the Defence Ministry Board" (December 22, 2016). http://en.kremlin.ru/events/president/news/53571. Accessed September 3, 2021.

64 Robert Kupiecki and Marek Menkiszak, eds., Interview with Defense Minister of the Russian Federation Sergey Shoygu for *Moskovskiy Komsomolets*, op. cit., p598.

changed since the process began is that Russia's political and military leaders are increasingly confident about the progress that was made. They also appear to project growing confidence that military balance in the Euro-Atlantic region is evolving in a direction favorable to Russia. This is reflected in statements made by Russia's political and military leaders.

> *"…military power and ability to respond to threats must be such that no one else in the world is tempted to test them…development plans for the armed forces are both large-scale and impressive… people will realize the full sense of this impressiveness once all of our plans have been carried out."*
>
> -Vladimir Putin, 2012[65]

> *"We have done a great deal over the past years to strengthen our defense capability. But we still lack many things… At the same time, many factors, such as military factors, our history and geography, and the general mood in the Russian society, allow us to say confidently that today we are stronger than any potential aggressor. I repeat, any aggressor."*
>
> -Vladimir Putin, 2016[66]

> *"Apparently, our partners got the impression that it was impossible in the foreseeable historical perspective for our country to revive its economy, industry, defense industry and armed forces to levels supporting the necessary strategic potential… No, nobody really wanted to talk to us about the core problem, and nobody wanted to listen to us. So, listen now."*
>
> -Vladimir Putin, 2018[67]

> *"We were always catching up… Today, we have a unique situation in our new and recent history. They try to catch up with us. Not a single country possesses hypersonic weapons, let alone continental-range hypersonic weapons."*
>
> -Vladimir Putin, 2019[68]

> *And when you consider, as they continue to do in the U.S. by force of inertia, that the balance of power has worked in your favor, various ideas can come*

65 President of Russia, "Expanded meeting of the Defence Ministry Board" (March 20, 2012). http://en.kremlin.ru/events/president/news/14808. Accessed September 3, 2021.

66 President of Russia, "Expanded meeting of the Defence Ministry Board" (December 22, 2016).

67 President of Russia, "Presidential Address to the Federal Assembly" (March 1, 2018). http://en.kremlin.ru/events/president/news/56957. Accessed September 3, 2021.

68 President of Russia, "Defence Ministry Board meeting" (December 24, 2019). http://en.kremlin.ru/events/president/news/62401. Accessed September 3, 2021.

to mind, including not very sensible ones… Not only can it, Russia is already fully effective in opposing America.

-Sergey Shoygu, 2019[69]

This confidence may be merely a message for domestic political consumption. It also may be a part of information confrontation with the West—that is, Moscow's attempt to convince the Western audience that Russia is stronger than it actually is.[70] The growing confidence can also reflect the genuine assessment of Russia's growing power. Over the last decade, Russia has made substantial progress in preparing for modern strategic conflict. Development of military concepts was followed by a sustained process of force posture enhancements, investments in readiness, and reforms of its command and control system that transformed intellectual foundations into tangible capabilities.

Conceptual Foundations

Building on the rich Soviet tradition of military thought, Russia has developed a set of coherent concepts that guide its approach to effectively competing in peacetime, crisis, and war. All of these concepts taken together serve as a building blocks of what can be defined as Russia's theory of victory—that is, Russia's approach to achieve its political aims short of war, in a short war, or protracted war if such a conflict would become unavoidable.[71]

Russia's military doctrine distinguishes between three types of conflicts: local, regional, and large-scale conflict. Local conflicts are to be fought with limited forces such as its war against Georgia in 2008 or its proxy war against Ukraine. Regional conflicts are expected to involve two or more states in a region, including coalition forces. An example of a regional war is a war with NATO. In Russia's thinking, such war is unlikely to be confined to geographic sub-regions such as the Baltic Sea region but will encompass a front from Norway in the north to Turkey in the south. It would be also a war with an entire Russia and would be characterized by constant threat of the use of nuclear weapons. For Russia's military strategists, a large-scale (strategic) war is a conflict that may draw the largest global powers, countries from other regions, and large coalitions that would pursue radical political and military goals through all

69 Robert Kupiecki and Marek Menkiszak, eds., Interview with Defence Minister of the Russian Federation Sergey Shoygu for *Moskovskiy Komsomolets*, op. cit., p597.

70 For an insightful analysis of the evolution of information confrontation in Russian strategic thinking about multi-domain conflict, see: Lesley Kucharsky, "Russian Multi-Domain Strategy against NATO: information confrontation and U.S. forward-deployed nuclear weapons in Europe" (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2018). https://cgsr.llnl.gov/content/assets/docs/4Feb_IPb_against_NATO_nuclear_posture.pdf. Accessed September 3, 2021.

71 For a thorough analysis, see: Brad Roberts, *On Theories of Victory: Red and Blue*, Livermore Papers on Global Security No.7 (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2020). https://cgsr.llnl.gov/content/assets/docs/CGSR-LivermorePaper7.pdf. Accessed September 3, 2021.

available means, including the use of nuclear weapons.[72] While Russia's doctrine distinguishes between local, regional, and large-scale wars, it treats them in a holistic and highly interdependent way. On the one hand, success in a local war depends on credible capabilities and actions to deter a regional war. Likewise, achieving aims in a regional conflict requires taking active steps to deter large-scale strategic war. On the other hand, success in local and regional wars depends on the ability to convince opponents that Russia is prepared to fight and win a regional or large-scale war.

In its approach to modern strategic conflict, Russia blurs the line between peace and war. This is because in Russia's thinking, peacetime competition and war cannot be separated. The former is indispensable for preparing conditions for success in the latter and vice versa. The success in wartime depends on peacetime efforts to gradually weaken opponents in political, economic, and military terms. It follows the logic that it is much harder to win with an adversary that is politically cohesive, militarily prepared, economically resilient and determined to fight.[73] Similarly, the success in peacetime rests on the perceived willingness to risk the war. An important implication of this is that Russia is engaged in information confrontation (or in what is defined by Western analysts as "hybrid warfare") not out of its weakness but out of pragmatism. As long as Russia would perceive the West as a challenge to its interests and potential military threat, it would seek to weaken it in peacetime to set conditions for success in war. It will also continue to play on fears of war to achieve its goals without the need to fight.

Russia has a full-spectrum approach to shaping peacetime competition and warfighting. Its approach to strategic deterrence involves integrating all available military, nuclear, and non-nuclear capabilities, as well as non-military tools at its disposal. While these tools are used simultaneously, the emphasis shifts depending on the context. In peacetime confrontation, non-military means play a leading role while military tools take on a largely supportive role. As explained by General Valery Gerasimov, Chief of the Russian General Staff, modern conflicts—defined as "conflicts below the threshold of war"—are "conducted by the integrated employment of political, economic, informational, and other non-military means, all implemented with reliance on military force."[74] The balance shifts in wartime. According to Gerasimov, war is conducted "on the basis of coordinated employment of military and non-military means with the decisive role of the armed forces." In such circumstances "non-

72 See more: Dave Johnson, "Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds," Livermore Papers on Global Security No. 3. (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2018), p63. https://cgsr.llnl.gov/content/assets/docs/Precision-Strike-Capabilities-report-v3-7.pdf. Accessed September 3, 2021.

73 Andrew Monaghan, *How Moscow Understands War and Military Strategy* (Arlington, VA: CNA, 2020), pp16-17. https://www.cna.org/CNA_files/PDF/IOP-2020-U-028629-Final.pdf. Accessed September 3, 2021.

74 Dave Johnson, "NATO Collective Defense in the Era of Unpeace," in *NATO in the Era of Unpeace: Defending Against Known Unknowns*, Dominik P. Jankowski, Tomasz Stępniewski, eds. (Lublin, Poland: Institute of Central Europe, 2021), p32. https://ies.lublin.pl/wp-content/uploads/2021/03/nato-in-the-era-of-unpeace_calosc-1.pdf. Accessed September 3, 2021.

military means, which influence the course and outcome of wars, provide and create the conditions for the effective use of military force."[75]

While assessing its readiness to wage local, regional, or large-scale conflicts, Russia's military leaders continue to see the utility of calculating a "correlation of forces and means"—that is, comparing quantitative and qualitative characteristics of friendly and enemy forces to determine which of the opposing sides has a military edge.[76] Russia's approach to warfighting also relies on other closely related and mutually reinforcing concepts, such as:

- achieving advantage in the initial period of war which it sees as having decisive impact for determining its outcome;[77]
- "preemptive neutralization" of adversary's action through the strategy of active defense;[78]
- gaining advantage through asymmetric and indirect actions, including *maskirovka* and *voennaya khitrost* (military cunning);[79]
- successful conduct of various strategic operations, including strategic operations to destroy critically important targets (SODCIT) to achieve political and military goals;
- escalation management that relies on an ability to inflict prescribed doses of "deterrent damage" that are calibrated "to sober but not enrage" the opponents, that is, to induce their capitulation on Russia's terms by generating their fear and restraint rather than anger and counter-escalation;[80]
- the whole-nation approach to territorial defense by preparing the whole economy, population, and territory of the state for war, including a protracted war if efforts to win quickly and decisively fail.

75 Ibid., p33.

76 See more: Clint Reach, Vikram Kilambi, Mark Cozad, *Russian Assessments and Applications of the Correlation of Forces and Means* (Santa Monica, CA: RAND, 2020). https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4235/RAND_RR4235.pdf. Accessed September 3, 2021.

77 See more; Michael Kofman, "It's Time to Talk about A2/AD: Rethinking the Russian Military Challenge," War on the Rocks (September 5, 2019). https://warontherocks.com/2019/09/its-time-to-talk-about-a2-ad-rethinking-the-russian-military-challenge/. Accessed September 3, 2021.

78 Dave Johnson, "Review: General Gerasimov on the Vectors of the Development of Military Strategy," *Russian Studies Series* 4, no. 19, NATO Defense College (March 30, 2019). https://www.ndc.nato.int/research/research.php?icode=585. Accessed September 3, 2021.

79 Timothy L. Thomas, "Russian Military Thought: Concepts and Elements," MITRE (August 2019), pp5-10. https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf. Accessed September 3, 2021; Andrew Monaghan, op. cit., p16.

80 See more: Brad Roberts, *On Theories of Victory: Red and Blue,* op cit.; Michael Kofman, Anya Fink and Jeffrey Edmonds. *Russian Strategy for Escalation Management: Evolution of Key Concepts* (Arlington, VA: CNA, 2020). https://www.cna.org/CNA_files/PDF/DRM-2019-U-022455-1Rev.pdf. Accessed September 3, 2021.

A series of CGSR workshops highlighted that Russia's conceptual and doctrinal developments has placed it ahead of the United States and its allies in creating a coherent theory of victory. Though impressive, however, Russian strategic thought is not free from shortcomings. One notable example is that in their approach to escalation management, Russian political and military leaders seem to underestimate NATO's cohesion and resolve to respond to Moscow's escalatory steps to induce de-escalation. While attempts to "sober but not enrage" the United States and its allies might induce the desired restraint, they might unleash a reply far beyond what Russia contemplated. A more complete "theory of victory" requires Russia to recognize the risks of provoking escalation—and the costs of miscalculation—more deeply.[81]

Modernized Equipment

Russia's military concepts were translated into concrete military investments that significantly enhanced its capability to implement its theory of victory. These improvements were facilitated by its determination to implement State Armament Programs (SAPs) starting with SAP-2020, the first successful and fully funded such program in the post-Soviet period.[82]

SAP prioritized modernizing and diversifying Russia's strategic nuclear forces, which included the deployments of RS-24 Yars intercontinental ballistic missiles and Borei class ballistic missile submarines armed with Bulava submarine-launched ballistic missiles, along with introducing novel systems such as the Avangard hypersonic glide vehicle. As the result, the share of modern weapons in Russia's nuclear forces reached 86 percent by December 2020. This sharply contrasted with the state of Russia's nuclear forces in 2000 when the number dropped to 35 percent.[83] The return on investment was more than just a greater credibility of Russia's nuclear deterrence. The modernization restored the value of strategic nuclear weapons in shaping

81 See: "Winning Conventional Regional Wars Against Nuclear-Armed Adversaries," 6th Annual Deterrence Workshop Summary (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, November 2019), p5. https://cgsr.llnl.gov/content/assets/docs/Winning-Conventional-Regional-Wars-Summary.pdf, accessed September 3, 2021; "De-Escalation and War Termination In Multi-Domain Regional Wars," workshop summary (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, May 25-26, 2021), p11, https://cgsr.llnl.gov/content/assets/docs/DEWT_Workshop_Summary.pdf. Accessed September 3, 2021.

82 The SAP is a multi-volume document approved by the Russian president that sets out plans for acquisition, repair, and upgrade of military equipment. It also allocates funding for research and development. Each SAP covers a 10-year period with detailed plans only for the first five years and a list of general priorities for the remaining five years. As the SAP is updated every five years, the second half of each SAP overlaps with the new program. The exception was SAP-2020 as it was followed by SAP-2027 that was implemented from 2018. The principal performance indicator of SAPs is the share of "modern" equipment in Russia's military arsenal. SAPs are subject of strict classification. However, Russia's political and military officials, including Putin, provide annual updates about their implementation, which is strictly monitored. See more: Julian Cooper, "The Russian State Armament Programme, 2018 – 2027," *Russian Studies* 1, no. 18, NATO Defense College (May 2018). https://www.ndc.nato.int/news/news.php?icode=1167, accessed September 3, 2021. Accessed September 3, 2021; Richard Connolly, Mathieu Boulegue, "Russia's New State Armament Programme. Implications for the Russian Armed Forces and Military Capabilities to 2027," Chatham House (May 10, 2018). https://www.chathamhouse.org/2018/05/russias-new-state-armament-programme. Accessed September 3, 2021.

83 President of Russia, "Expanded meeting of the the Defence Ministry Board" (December 21, 2020). http://en.kremlin.ru/catalog/persons/90/events/64684. Accessed September 3, 2021.

peacetime competition, intra-war deterrence, and increased a number of credible limited and large-scale strike options during wartime.

Russia's ability to achieve advantage in the initial period of warfare, destroy critically important targets, and manage escalation was sharply strengthened by its effort to significantly expand the number of its dual-capable ground-, sea-, and air-launched long-range precision strike systems. Russia equipped 13 missile brigades with ballistic and cruise variants of Iskander missiles (9M720/SS-26 Stone and 9M728), fielded at least three battalions of the 9M729/SSC-8 Screwdriver ground-launched intermediate-range cruise missiles, and deployed the Kalibr family of cruise missiles aboard its navy's surface ships and submarines.[84] According to the Russian Ministry of Defense, the number of delivery vehicles for Russia's long-range cruise missiles grew by 13 times between 2012 and 2020 while the number of land-based, sea-, and air-launched missiles grew by 37 times.[85]

Russia also improved its general purpose forces. By December 2020 the share of modern weapons and equipment in Russia's military forces was over 70 percent, in comparison to a critical low of 12 percent in 2000.[86] Defense of Russia's territory against aerospace attack was augmented by the planned deployment of 56 batallions of S-400 Triumf surface-to-air missiles. Russia also upgraded missile defense around Moscow and other air defense systems, including the medium range S-350 Vityaz missile and the Pantsyr-S short-range missile.[87] Its multi-domain toolkit of asymmetric capabilities to negate the U.S. military advantage was supplemented with new electronic warfare systems, cyber capabilities, and counter-space weapons.

The achievements of SAPs are impressive despite all their shortcomings and problems that Russia encountered during their implementation. The "modernization" largely focused on upgrading existing systems along with introducing brand platforms and weapons based on new designs at a modest pace. SAPs were tormented with missing set targets and delays of highly expected weapon programs such as Armata T-14 tanks or PAK-DA, a new strategic bomber. Full implementation of SAPs was difficult not only because of over-optimistic timelines and technical problems, but also economic difficulties that resulted from the drop of oil prices and Western economic sanctions that had been in place since 2014.

Combat-Ready Forces at High Readiness

The modernization effort initiated in 2008 enabled Russia to fulfill the dreams of Soviet military practicians and theoreticians, including Marshal Ogarkov, to create combat-ready forces held at high-readiness. This drastically amplified its ability to act

84 *Russia's Military Modernisation. An Assessment* (London: International Institute of Strategic Studies, 2020), pp76, 92.

85 TASS, "Number of long-range cruise missile carriers in Russia up 13 times since 2012" (December 22, 2020). https://tass.com/defense/1238697. Accessed September 3, 2021.

86 President of Russia, "Expanded meeting of the the Defence Ministry Board" (December 21, 2020), op. cit.

87 *Russia's Military Modernisation: An Assessment,* op. cit., p74.

with speed and surprise. The transformation was particularly visible in the Russian army. According to Russia's officials, by 2019 a permanently ready professional "core" of Russia's Ground Forces and Airborne Forces consisted of 136 battalion tactical groups (BTGs). This sharply contrasts with pre-2008 data, when only 17 percent of Russia's ground troops units were stand-by combat ready.[88]

To enhance its capability to fight any type of conflict, Russia has been regularly conducting large-scale annual strategic-level exercises (ZAPAD, VOSTOK, TSENTR, KAVKAZ) that are unique in their aims, size, and frequency, but also lack of transparency. Such exercises serve various purposes. They enable Russia's forces to train between local, regional, and large-scale conflicts. They test and enhance Russia's ability to redeploy its own forces across its vast territory. With its significant nuclear component, these exercises make Russia's forces better integrated to achieve strategic effects during a conflict. Such exercises are also instrumental in preparing the entire nation for fighting a large-scale war. Annual strategic-level exercises are often coordinated with internal security exercises aimed at securing Russia's rear through sealing its borders, controlling mass demonstrations, and protecting strategically important objects. The exercises involve various civilian entities, including Russia's ministries of health, transport, communications, industry and trade, and finance, as well as the Central Bank and the Bank of Russia.[89]

The ultimate test of readiness of Russia's military troops are the large-scale combat readiness checks also known as snap exercises. Such exercises have been conducted at the level of an entire military district or branch of the armed forces. Their number rose from one in 2013 to around five in 2016, and have become routine.[90] In addition to enhancing combat training, snap exercises have also played a direct role in supporting Russia's operations. Reflecting Russia's military emphasis on military cunning, such exercises masked preparations for the annexation of Crimea and the backing of separatists in eastern Ukraine. They were also instrumental in enabling intervention in Syria in 2015.[91]

To further enhance time-space advantage provided by the combat-ready forces, in recent years Russia made also significant changes in deployments of ground forces on its borders. Russia augmented the level and number of units deployed on its western border; significantly strengthened its forces in the Southern Military districts, including units deployed in occupied Crimea; and has augmented its military

88 Ibid., pp66, 70.

89 Dave Johnson, "VOSTOK 2018: Ten years of Russian strategic exercises and warfare preparation," *NATO Review* (December 20, 2018). https://www.nato.int/docu/review/articles/2018/12/20/vostok-2018-ten-years-of-russian-strategic-exercises-and-warfare-preparation/index.html. Accessed September 3, 2021. Dave Johnson, "ZAPAD 2017 and Euro-Atlantic security," NATO Review (December 14, 2017). https://www.nato.int/docu/review/articles/2017/12/14/zapad-2017-and-euro-atlantic-security/index.html. Accessed September 3, 2021.

90 Johan Norberg, "Training for War Russia's Strategic-level Military Exercises 2009-2017," FOI-R--4627—SE, FOI (October 2018), pp41-44. https://www.foi.se/rest-api/report/FOI-R--4627--SE. Accessed September 3, 2021.

91 Dave Johnson, "Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds," op. cit., p10.

capabilities in the Arctic. What made Russia's forces even more capable to fight was experience gained during military operations, including in Syria and Ukraine.

Command and Control

Over the last decade, Russia has made significant changes in its command and control (C2) system at the strategic, strategic operational, and tactical levels.

The central nerve of Russia's C2 during peacetime competition and warfare is the National Center for Direction of Defense (NCDD) activated in 2014. In peacetime, NCDD plays a role of the main coordination point during military exercises and operations. It also constantly monitors the security environment, conducts forecasting and modeling of future wars, and monitors implementation of SAPs. In wartime, NCDD is designed to fulfill the function of a supreme command center by bringing together key political and military decision-makers and connecting through digital systems all levels of military C2 from strategic-operational to tactical levels. In this function, NCDD serves as the interface and central link between the national political leadership, including President Putin, the General Staff, the Defense Ministry, and combined strategic commands (OSKs) down to mobile headquarters. The Center is also important tool for managing strategic deterrence, including the use of nuclear weapons.[92] While it is still a work in progress, NCDD enhances one of the greatest advantage of Russia over the United States and NATO—that is, the speed of its decisionmaking.

The innovation that enhanced Russia's C2 at the strategic-operational level was the creation of a highly flat, simple, and effective administrative, planning, and operational C2 system. This followed more than 20 years of debates, discussions, planning, and bureaucratic politics. The central feature of the new C2 system are five Combined Strategic Commands (OSKs), each responsible for a separate strategic direction. Four OSKs were created in 2010 based on newly restructured military districts: OSK Western Military District, OSK Southern Military District, OSK Central Military District, and OSK Eastern Military District. The fifth OSK was created in December 2014 based on the Northern Fleet. With the establishment of OSKs, all peacetime and wartime operations within each strategic direction are centralized under the command of a single commander. Each OSK commander is put in direct peacetime and wartime control of all units from all of the service branches and combat arms within the territory of the military district. The only exception are nuclear, aerospace, and airborne forces that remain under the command of the General Staff. Such solution streamlined the command structure and addressed C2 problems that became apparent in the Russia and Georgia in August 2008 when Russian operations suffered from poor coordination between the different service branches.[93]

92 See more: Dave Johnson, "NATO Collective Defense in the Era of Unpeace,"op. cit., pp40-42; *Russia's Military Modernisation: An Assessment*, op. cit., p38.

93 See more: Greg Whisler, "Strategic Command and Control in the Russian Armed Forces: Untangling the General Staff, Military Districts, and Service Main Commands (Part Three)," *Journal of Slavic Military Studies* 33, no. 2 (November 2, 2020).

Russia has also reformed its tactical-operational command structure to reorient its forces to the possibility of participation in a major, near-peer war. After 2013, the brigades of its Ground Forces were converted to divisional-level structures, reversing decisions taken in 2008. In 2014-2015, Air Defense brigades once again became Air Defense divisions and regiments. In 2015, Russia also created Aerospace Forces by merging the Air Force and the Space Forces. This change has brought together fixed-wing aviation, army aviation helicopters, long-range air-defense systems, and the strategic missile defenses around Moscow, as well as military space launch sites and space vehicles.[94]

The changes in C2 structures made by Russia over the last decade also reflect the "whole of nation" approach to warfare. During wartime, NCDD combines more than 40 military, police, economic, infrastructure, and other authorities under the stewardship of the armed forces' General Staff. At the strategic-operational level, each OSK is supported by the Military District (Wartime). During wartime, this entity takes control over regional and local governments and assumes direct responsibility for the mobilization of reservists, industrial production and transportation, and for implementing martial law and internal security.[95]

Plans

Even though Russia's political and military leaders are satisfied with its growing capabilities to wage modern strategic warfare, the modernization process is not finished. There are a number of reasons for this. First, despite remarkable progress, not everything that was originally envisioned was achieved. The level of modern military equipment is uneven across different services. Apparent gaps still exist, including an absence of modern transport aircraft that would enhance both the mobility and deployability of Russia's forces. Second, the quantitative and qualitative correlation of forces and means in certain areas are still seen by Russia as unfavorable. For example, Russian and Western military analysts estimate that even though Russia has capabilities to mitigate effects of an aerospace attack against Russian territory, Russia's defensive and offensive Aerospace Forces capabilities are insufficient for denying such an attack involving the conquering aerospace dominance or gaining of strategic initiative.[96] Lastly and even more importantly, in view of President Putin, the competition for a military edge never ends as other countries, including the United States, are reacting to Russia's progress. Even if Russia did fill existing gaps, it has no choice but to keep on investing to preserve any advantage

94 *Russia's Military Modernisation: An Assessment*, op. cit., pp32-34.

95 Greg Whisler, op. cit., p247.

96 See: Dmitry (Dima) Adamsky, "Moscow's Aerospace Theory of Victory: Western Assumptions and Russian Reality," CNA (February 2021), pp17-18. https://www.cna.org/CNA_files/PDF/IOP-2021-U-029278-Final.pdf. Accessed September 3, 2021. Clint Reach, Vikram Kilambi, Mark Cozad, "Russian Assessments and Applications of the Correlation of Forces and Means," op. cit., pp122-130.

that it thinks it has—or create a new one. In addition, Russia needs to hedge against geopolitical and technical surprises.[97]

The constraining factor for Russia's political leadership in investing in future capabilities is avoiding being dragged into a senseless arms race—that is, being forced to spend more on defense that it can afford with a crippling effects on its economy.[98] The solution to this is a continued reliance on asymmetric means as well as "on brains, intellect, discipline and organization when handling relevant tasks."[99]

> *"… if we allow ourselves to relax even for a minute, if we make a single significant mistake in modernizing the Army and the Navy and training military personnel, the situation will change very quickly, in light of the speed of global events. It can change in the wink of an eye…"*
>
> -Vladimir Putin, 2016[100]

> *"… our goal is not a one-time rearmament, after which we can forget about the Army and Navy for decades. The Army and Navy must always have the best equipment and technology… our equipment must be better than the world's best if we want to come out as the winners. This is not a game of chess where we can sometimes accept a tie. It concerns the military organization of the nation. Our equipment must be better. We can do it and we are doing it in the key spheres. But we must also do it in all spheres."*
>
> -Vladimir Putin, 2019[101]

> *"We have not done everything we wanted. But we are on the right track and will continue our efforts to ensure the ultimate security of the Russian Federation and its people…"*
>
> -Vladimir Putin, 2020[102]

97 For a discussion on tripolar U.S.-Russia- China strategic balances in 2030, see CGSR workshop reports: "Fit For Purpose? The U.S. Nuclear Posture in 2030 and Beyond," June 8-10, 2020; and "The Next U.S. Strategic Posture — And The Posture After Next," July 8-10, 2020. https://cgsr.llnl.gov/workshops. Accessed September 3, 2021. See also: Anya Loukianova Fink, "Russia's Assessment of the 2030 Strategic Balance," *Fit for Purpose? The U.S. Strategic Posture in 2030 and Beyond*, Brad Roberts, ed. (Livermore, CA: Lawrence Livermore National Laboratory, 2020). https://cgsr.llnl.gov/content/assets/docs/The-US-Strategic-Posture-in-2030-and-Beyond.pdf. Accessed September 3, 2021.

98 President of Russia, "Vladimir Putin's annual news conference" (December 23, 2016). http://en.kremlin.ru/events/president/news/53573. Accessed September 3, 2021.

99 President of Russia, "Expanded meeting of the Defence Ministry Board" (December 22, 2017). http://en.kremlin.ru/events/president/news/56472. Accessed September 3, 2021. Putin reiterated these sentiments in 2019 and emphasized that Russia's competitive advantage lies in "brains, intelligence, better organization of work, minimizing theft and negligence, and concentrating efforts on key areas will lead us to a high state of defense capability." See: President of Russia, "Defence Ministry Board meeting" (December 24, 2019). op. cit.

100 Speech of President Vladimir Putin at the expanded meeting of the Defence Ministry Board (December 22, 2016).

101 Speech of President Vladimir Putin at the Defence Ministry Board meeting (December 24, 2019), op. cit.

102 President of Russia, "Vladimir Putin's annual news conference" (December 17, 2020). http://en.kremlin.ru/events/president/news/64671. Accessed September 3, 2021.

"There is something I really need to underscore. It is absolutely unacceptable to stand idle. The pace of change in all areas that are critical for the Armed Forces is unusually fast today. It is not even Formula 1 fast—it is supersonic fast. You stop for one second and you start falling behind immediately. We must by no means rest on our laurels."

-Vladimir Putin, 2020[103]

Russia works on clarifying its level of ambition for SAP-2033. The wish list is long and if the ambitious goals are to be met with similar budget as in the case of SAP-2020 and SAP-2027, it translates to a cost of roughly 21 trillion rubles.[104]

Building on modernization steps taken so far, Russia is in a good position to qualitatively and quantitatively expand its strategic arsenal if it chooses to do so. Modernizing its strategic forces will remain a key priority as Russia seeks to improve its position in defining a new "security equation" for strategic stability and hedges against a world without strategic arms control. According to a Russian proposal, such an "equation" should be jointly developed with the United States and take into account all factors affecting strategic stability, including all offensive—that is, nuclear and non-nuclear—and defensive systems capable of attaining strategic goals, such as "emerging kinds of weapons prospective technologies, as well as new political realities."[105] Importantly, with regards to defensive systems, the new "strategic equation" should set quantitative and geographical limits for deploying missile defense systems.[106]

Russia is likely to continue its efforts to radically expand its arsenal of precision-guided missiles. To "consolidate the potential of non-nuclear deterrent capability provided by high-precision missiles," it plans to double the number of such systems.[107] The efforts would likely involve "Tsirkonization" and further "Kalibrization" of Russia's surface and submarine fleet. This would enable Russia in the next decade to narrow the gap with the U.S. naval cruise missile capacity.[108] Russia's efforts may also involve deploying more ground-launched intermediate range systems as Moscow plans to

103 President of Russia, "Expanded meeting of the the Defence Ministry Board" (December 21, 2020), op. cit.

104 TASS, "Budget of Russia's new state arms procurement program to be over 21 trillion rubles" (April 13, 2021). https://tass.com/defense/1277655. Accessed September 3, 2021.

105 Interfax, "Future Russia-U.S. strategic equation should include nuclear and non-nuclear weapons - Russian deputy FM," Interfax (November 30, 2020). https://interfax.com/newsroom/top-stories/70491/. Accessed September 3, 2021.

106 Ibid. See also: President of Russia, "Meeting of President of Russia Vladimir Putin with senior Defence Ministry officials, heads of federal agencies and defence industry executives" (November 10, 2020). http://en.kremlin.ru/events/president/news/64392. Accessed September 3, 2021. President of Russia, "Presidential Address to the Federal Assembly" (April 21, 2021). http://en.kremlin.ru/events/president/news/65418. Accessed September 3, 2021.

107 Russian Defence Ministry, "Russian Defense Ministry Board Session 2020" (2020). http://itogi2020.mil.ru/itogi2020_en/. Accessed September 3, 2021.

108 H.I. Sutton, "Russia Increasing Submarine Cruise Missile Capacity as U.S. Navy Decreases Its Own," RUSI Commentary (August 19, 2021). https://rusi.org/explore-our-research/publications/commentary/russia-increasing-submarine-cruise-missile-capacity-us-navy-decreases-its-own. Accessed September 3, 2021.

"take all response measures… in the shortest time possible" if such missiles are deployed by the United States in Europe or in the Indo-Pacific.[109]

Its aerospace defense would be further improved by deployments of advanced S-500 air and missile defense systems and investing in technologies to counter hypersonic weapons. Russia's political and military leadership anticipate that any advantages from being the only country to deploy hypersonic weapon systems would wane over the next two decades as other countries, including the United States, are developing similar capabilities. According to Putin, Russia is "on the right track and [is] working hard" on this problem.[110]

Russia will also continue to incrementally increase the capabilities of its general purpose forces. By the end of 2024, Russia's Ministry of Defense plans to increase the proportion of modern weapons and equipment in the Army and the Navy to 75.9 percent.[111]

Last but not least, Russia is also no exception in its hopes to leverage the benefits provided by its investments in emerging and disruptive technologies. One of the objectives of SAP-2033 is to further "improve the quality of weapons and equipment and increase their output" through the "broad use of artificial intelligence in creating military products… [expansion of] the product line of reconnaissance and attack unmanned aerial vehicles, laser and hypersonic systems and weapons based on new principles of physics, as well as robotic systems capable of performing a variety of tasks on the battlefield."[112]

Russia's plans appear overambitious. With its failures in recent years to develop and deploy capabilities built on new designs, these plans should be treated with a grain of salt. Still, dismissing them would be a mistake. Russia is now in a much better position to achieve its ambitious goals than during the previous decade. The starting point of Russia in 2020 is radically improved than in 2008. The further modernization of military equipment is much easier to achieve, thanks to a decade of intensive force modernization that put its military industry back on track.

What should be also taken into account by Western observers is that Russia is likely to continue improving its theory of victory for modern strategic conflict. While doing so, it will continue to build on its coherent set of ideas developed so far. Sustaining combat-ready forces will be much easier for Russia than creating them from scratch, as was the case in 2008. The strategic operational and tactical command and control system also requires only incremental improvements, not revolutionary changes. Thus, the challenges that Russia currently poses to the Euro-Atlantic security order are likely

109 President of Russia, "Expanded meeting of the Defence Ministry Board" (December 21, 2020), op. cit.

110 President of Russia, "Vladimir Putin's annual news conference" (December 17, 2020), op. cit.

111 Russian Defence Ministry, "Russian Defense Ministry Board Session 2020" (2020), op. cit.

112 President of Russia, "Meeting of Russian Federation Security Council" (November 22, 2019). http://en.kremlin.ru/events/president/news/62096. Accessed September 3, 2021.

to increase over the next decade, not decrease. What could make the competition with Russia even more difficult than today is the growing confidence its political and military leaders have in its capability to prevail in modern strategic conflict. As a result, we must ask: If in the recent decade Russia acted aggressively out of weakness, how would it act out of the perception of its own strength?

China's Approach to Multi-Domain Conflict

Phillip C. Saunders[113]

China's approach to warfare in the new military domains of cyberspace, outer space, and multi-domain warfare is well developed and robust. This is the product of decades of study, analysis, and preparation by scholars, strategists, and leaders of the People's Liberation Army (PLA), building on guidance from the Chinese Communist Party (CCP) that has increasingly emphasized the critical role information plays in modern warfare. The CCP's most recent guidance calls for the PLA to focus on winning "informationized local wars."[114]

To explicate China's approach to multi-domain complexity, this short chapter proceeds as follows. It begins with a review of the roles of cyberspace and outer space in China's military strategy. It then discusses the steps China has taken to integrate multi-domain operations into its plans and forces, focusing primarily on conventional operations. It closes with an assessment of Chinese leadership views of the balance of multi-domain power and of its competitive position vis-à-vis the United States.

"The New Commanding Heights"

Like the United States and Russia, China conceives of military domains that encompass both the traditional domains of air, land, and sea and the new domains of cyberspace and outer space. PLA theorists often discuss the electromagnetic spectrum as a domain in its own right. In PLA operational thinking, the nuclear dimension of modern warfare is generally treated as distinct from conventional warfare.[115] PLA theorists also discuss separate information and cognitive domains (the latter encompassing adversary psychology and morale and thus the political will to continue combat operations).[116]

113 Dr. Saunders is Director of the Center for the Study of Chinese Military Affairs, part of National Defense University's Institute for National Strategic Studies. The views expressed are his own, and do not necessarily represent those of the National Defense University, the Department of Defense, or the U.S. government.

114 M. Taylor Fravel, "Shifts in Warfare and Party Unity: Explaining Changes in China's Military Strategy," *International Security* 42, no. 3 (Winter 2017/2018), pp37-83.

115 Chinese thinking on "integrated strategic deterrence" views offensive and defensive nuclear, conventional, outer space, and cyberspace capabilities as all contributing toward strategic deterrence, but does not focus on operations that integrate nuclear and conventional weapons. See Michael S. Chase and Arthur Chan, "China's Evolving Strategic Deterrence Concepts and Capabilities," *The Washington Quarterly* 39, no. 1 (2016), pp117-136.

116 Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," *China Brief* 19, no. 16 (September 6, 2019). https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/. Accessed November 23, 2021.

For the purpose of winning informationized local wars, the information domain is deemed critical. China pursues information dominance as the essential enabler of "integrated joint operations," which envision close cooperation among all the PLA services at the strategic, operational, and tactical levels to produce success on the modern battlefield. In turn, the cyber and space domains are viewed as crucial in the competition for information dominance and critical for the PLA's ability to conduct integrated joint operations. This way of thinking is clearly set out in China's 2015 white paper on military strategy.[117]

First, on the military role of cyberspace, the white paper reads:

> *Cyberspace has become a new pillar of economic and social development, and a new domain of national security. As international strategic competition in cyberspace has been turning increasingly fiercer, quite a few countries are developing their cyber military forces. Being one of the major victims of hacker attacks, China is confronted with grave security threats to its cyber infrastructure. As cyberspace weighs more in military security, China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability.*

Cyberspace and networked command and control systems are viewed as critical for conducting integrated joint operations, because they facilitate the flow of information across services and across various levels of command. The speed of information flow and rapid decisionmaking is critical to gaining the initiative on the battlefield.[118]

In terms of outer space, the white paper states:

> *Outer space has become a commanding height in international strategic competition. Countries concerned are developing their space forces and instruments, and the first signs of weaponization of outer space have appeared. China has all along advocated the peaceful use of outer space, opposed the weaponization of and arms race in outer space, and taken an active part in international space cooperation. China will keep abreast of the dynamics of outer space, deal with security threats and challenges in that domain, and secure its space assets to serve its national economic and social development, and maintain outer space security.*

117 State Council Information Office, "China's Military Strategy" (May 26, 2015). https://china.usc.edu/prc-state-council-chinas-military-strategy-2015-may-26-2015. Accessed November 23, 2021.

118 See Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND Corporation, RR-1708-OSD, 2018). https://www.rand.org/pubs/research_reports/RR1708.html. Accessed November 1, 2021.

Space is an equally important domain for informationized warfighting. It is important for the surveillance of adversary forces, helping to locate and identify targets. It provides timing and location information to improve the accuracy of precision-guided munitions. It provides communications support for command-and-control systems, especially for mobile PLA units deployed out of reach of land-based systems.[119]

As noted above, the PLA sees these domains as the "new commanding heights in strategic competition."[120] Accordingly, it competes to strengthen its position. It focuses on two core tasks. One is to prepare to conduct kinetic and non-kinetic attacks to degrade and deny the adversary's use of cyber networks and space systems. The other is to protect against adversary attack by improving resilience and defensive measures so as to maintain its own access. Both offense and defense are important to the PLA, but the Chinese emphasis has shifted over time. Its initial focus was on the offense; this followed from an assessment that the U.S. military is heavily dependent on vulnerable systems in cyberspace and outer space. The PLA could exploit the American vulnerability via asymmetric offensive attacks. But the need for a reliable defense has begun to come into focus as PLA efforts to exploit space and cyber for their own military advantages are gradually creating similar dependencies and vulnerabilities.

These developments in China's concepts and capabilities for war in cyberspace and outer space are stepping stones toward development of a comprehensive approach to multi-domain warfare. As one PLA author has described it, all-domain operations can potentially achieve decisive results "by layering effects in multiple domains, controlling new domains to gain the strategic initiative, and striving for comprehensive superiority through cross-domain integration."[121]

Operationalizing Multi-Domain Warfare

The process of operationalizing cyberspace and outer space as warfighting domains and of developing a comprehensive approach to operational integration is well advanced in China. One clear marker is the major reorganization of the PLA in 2016 to bring together space, cyber, electronic warfare, and psychological warfare all into one organization—the Strategic Support Force (SSF). This force serves two purposes. It works like a military service to organize, train, and equip PLA forces to operate in these strategic domains. It also has an operational role in supporting national level

119 See Deng Cheng, "Space and Chinese National Security: China's Continuing Great Leap Upwards," in Joel Wuthnow, Arthur S. Ding, Phillip C. Saunders, Andrew Scobell, and Andrew N.D. Yang, eds., *The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context* (Washington, DC: NDU Press, 2021), pp311-337.

120 State Council Information Office, "China's Military Strategy."

121 Zhang Qianyi [张谦一], "Exploring Ways to Generate All-Domain Combat Capability," [探索全域作战能力生成路径], *PLA Daily* [解放军报] (September 25, 2018). http://www.81.cn/jfjbmap/content/2018-09/25/content_216591.htm. Accessed November 23, 2021. Cited in Derek Solen, "Chinese Views of All-Domain Operations," China Aerospace Studies Institute (August 30, 2020). https://www.airuniversity.af.edu/CASI/Display/Article/2310442/chinese-views-of-all-domain-operations/. Accessed November 23, 2021.

and regional military commanders in developing plans and conducting operations.[122] In principle, this provides a means to integrate SSF capabilities with the theater commander's direct control over land, air, and maritime forces (including Rocket Force conventional missile capabilities). In practice, we are starting to see joint exercises at the theater level that integrate SSF capabilities, including sometimes at the tactical level (e.g., army battalion air defense exercises that included air force radar units and SSF support).[123] It is worth noting that even though the SSF integrates most PLA cyberspace capabilities, responsibility for computer network defense lies with the Central Military Commission (CMC) Joint Staff Department's Information and Communications Bureau.[124]

The PLA organizational reforms that support improved multi-domain integration are mirrored by an increased focus on multi-domain warfare in the development of PLA doctrine. That increased focus has been driven in significant measure by the evolution of the PLA concept of jointness.

The initial PLA concept of jointness, as reflected in the "New Generation Operational Regulations" published in 1999, focused on "coordinated joint operations." It sought cooperation between and among the separate services.[125] Various types of joint campaigns were explicated in PLA doctrinal writings, tried out in exercises, and made available as options for joint commanders. But the PLA did not have standing joint command structures or communications systems that could work across service boundaries, which greatly impeded progress.

A refined definition of jointness, which forms the intellectual basis for the 2016 PLA reforms, focuses on "integrated joint operations."[126] This concept defines joint operations as the default "basic form of operations" at the strategic, operational, and tactical levels. This thinking incorporates the PLA's focus on informationized warfare and benefits greatly from progress in developing communications systems such as the

122 John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era, China Strategic Perspectives* 13 (Washington, DC: NDU Press, 2018). https://inss.ndu.edu/Media/News/Article/1651882/chinas-strategic-support-force-a-force-for-a-new-era/. Accessed November 23, 2021.

123 John Chen, Joe McReynolds, and Kieran Green, "The PLA Strategic Support Force: A 'Joint' Force for Information Operations," in *The PLA Beyond Borders*, pp151-179.

124 John Costello and Joe McReynolds, *China's Strategic Support Force*, pp25, 53.

125 See David M. Finkelstein, "Thinking About the PLA's 'Revolution in Doctrinal Affairs,'" in *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army*, David M. Finkelstein and James Mulvenon, eds. (Alexandria, VA: CNA Corporation, 2005), pp1-27.

126 The concept of "integrated joint operations" as the main form of PLA operations was adopted in 2004, but authoritative explication of the concept and formal guidelines for how to implement it were delayed until the November 2020 "Guidelines on Joint Operations of the Chinese People's Liberation Army (Trial)." See Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND, 2020), pp6-8, https://www.rand.org/pubs/research_reports/RRA394-1.html. Accessed November 23, 2021.

Integrated Command Platform that can work across service boundaries and the 2016 military reforms that established standing joint command and control structures.[127]

Both the revised military strategic guidelines that Xi Jinping issued in 2019 and the PLA's authoritative "Guidelines on Joint Operations of the Chinese People's Liberation Army (Trial)" issued in November 2020 continue to use the term "integrated joint operations." However, other PLA writings are moving beyond this term to an in-depth exploration of multi-domain operations.

New thinking about multi-domain operational operations is reflected in the latest (2020) version of the Science of Military Strategy (prepared by China's National Defense University).[128] The chapter on operational guidance (作战指导, *zuozhan zhidao*) states that the "basic form of warfare" has shifted from "integrated joint operations" (一体化联合作战, *yiti hua lianhe zuozhan*) to "multi-domain integrated joint operations" (多域一体化联合作战, *duo yu yiti hua lianhe zuozhan*).[129] The latter refers to an "advanced stage" of joint operations consisting of a high level of operational coordination across domains, including land, sea, air, space, cyber, and the electromagnetic spectrum, as well as the cognitive domain (智, zhi).

Some PLA writings draw heavily on U.S. terms and concepts, including Joint All-Domain Operations (JADO), Multi-Domain Battle (MDB), and Multi-Domain Operations (MDO). They make frequent use of the term All-Domain Operations (全域作战, *quanyu zuozhan*)—a slightly different term than used in the NDU *Science of Military Strategy*.[130]

A common element of these writings is an emphasis on applying capabilities across domains in order to compensate for relative weaknesses in single domains; such an approach, PLA strategists argue, opens windows of superiority which can be exploited operationally to maneuver or conduct attacks to seize the initiative.

An important difference between these PLA writings and U.S. Joint All-Domain Operations is how to plan for a loss of "directed cooperation" across domains as wartime damage is done. In the U.S. military, operators are given "commander's intent" and expected to continue operations even if communications and coordination are lost. In the PLA, operators have far less autonomy in such circumstances.[131]

There is also a debate among PLA military experts about whether the individual services should be capable of acting in multiple domains and of coordinating actions in all domains. One article essentially called for individual PLA services to

127 For further analysis of this evolution, see David M. Finkelstein, *The PLA's New Joint Doctrine: The Capstone of the New Era Operations Regulations System* (Arlington, VA: CNA, 2021). https://www.cna.org/CNA_files/PDF/The-PLAs-New-Joint-Doctrine.pdf. Accessed November 23, 2021.

128 *The Science of Military Strategy* [战略学] (Beijing: National Defense University Press, 2020).

129 Ibid., pp264, 267. See Joel Wuthnow, "What I Learned From the PLA's Latest Strategy Textbook," *China Brief* 21, no. 11 (May 25, 2021). https://jamestown.org/program/what-i-learned-from-the-plas-latest-strategy-textbook/. Accessed November 23, 2021.

130 Derek Solen, "Chinese Views of All-Domain Operations," China Aerospace Studies Institute (August 31, 2020). https://www.airuniversity.af.edu/CASI/Display/Article/2310442/chinese-views-of-all-domain-operations/. Accessed November 23, 2021.

131 Ibid.

replicate the strike capabilities of multiple services and have the organic intelligence, surveillance, and reconnaissance (ISR) and targeting capabilities to conduct independent operations.[132] While not very joint (in calling for duplication of capabilities in different services), this may be an effort to achieve resilience in the face of degraded communications by allowing units of a single service to conduct all-domain operations on their own.

In sum, there is abundant evidence that the PLA's concept development experts are actively engaged in understanding the operational requirements of successful multi-domain operations, including how to divide responsibilities among the services, how to coordinate operations across services, and how to continue to operate in an environment of degraded communications and command and control. PLA authors are also enthusiastic about the potential for artificial intelligence and other aspects of intelligentized warfare to help provide solutions to these challenges and create operational advantages, including by faster decision cycles.

China's Assessment of its Multi-Domain Competitiveness

As China (like the United States) conceives itself as being in a strategic competition over these capabilities, how do China's leaders assess their own competitive position? Do they think that the PLA is behind, equal to, or ahead of the U.S. military in adjusting to multi-domain complexity?

There is no obvious answer to this question. There are some indirect indicators pointing in opposite directions. On the one hand, Xi Jinping seems to anticipate that China will only emerge as a military peer to other major modern powers in the middle of the next decade, implying that China is still far behind. On the other hand, his military and political assertiveness in the maritime environment and other domains suggests that he is already more willing to accept military risk, implying that China has already caught up enough to adopt a more aggressive stance.

What might "enough" mean? China does not necessarily need to compete with the United States for the latest and best technical solutions across the board, though in some sectors it is doing quite well in this regard. For the purposes of deterrence and coercion, it merely needs to have the means to credibly threaten to exploit U.S. dependencies and vulnerabilities in the new domains, while being resilient in the face of American efforts to exploit Chinese vulnerabilities. As the United States is the more dependent and more vulnerable party, China's leaders may conclude that it is already in a position of strategic advantage in these domains. Moreover, they may assess that this asymmetry will persist despite China's own growing dependence on cyberspace and outer space, especially if China is able to incorporate defense and greater

132 Wu Zhonghe [吴中和] and Zhu Xiaoning [朱小宁], "Viewing 'All-Domain' from a Wider Perspective," [以更宽广的视角看'全域'," PLA Daily [解放军报] (April 26, 2018). http://www.81.cn/jfjbmap/content/2018-04/26/content_204708.htm, cited in Derek Solen, *Chinese Views of All-Domain Operations*, pp5-6. Accessed November 23, 2021.

resilience into its cyber and space capabilities. It is worth remembering that offensive cyber capabilities and counter-space capabilities don't work in the same way as conventional or nuclear "counter-force" capabilities; successful attacks on adversary space and cyber capabilities don't necessarily protect your own satellites or networks.

The discussion illuminates the difficulty of accurately gauging the balance of capability and capacity to secure the benefits of, and manage the risks of, multi-domain complexity. We should all understand the lurking danger: miscalculation could lead to deterrence failure and unwanted escalation. Both China and the United States are preparing for a high-end conventional conflict employing advanced capabilities. Both have information warfare doctrine that involves efforts to target adversary sensors and command and control networks to disorient the adversary and force it to fight with individual weapons and units rather than as an integrated, networked force. Both emphasize the importance of seizing the initiative in a conflict to achieve decisive impact. At the same time, both militaries hope to leverage advanced sensors, command and control networks, and precision strikes to achieve synergistic and often cross-domain effects for their own forces.

Neither China nor the United States has experience in employing such capabilities against military peer competitors, though they do have some limited experience in employing such capabilities against less capable militaries. These factors, combined with the intense secrecy that surrounds actual capabilities, suggest a high potential for overestimating one's own capabilities and underestimating the adversary's. This creates a heightened risk of deterrence failure based on miscalculation. The significant risk of misperceiving the balance of capabilities suggests that intensifying U.S.-China multi-domain competition could be far less stable than many assume.

The New Domains, Emerging Technologies, and Strategic Competition

Anna Péczeli and Benjamin Bahney

Today's multipolar, multi-domain environment creates many new challenges to strategic competition. The number of capabilities that can impose strategic effects has increased, as have the number of states that are able to challenge the United States. Both Russia and China have modernized their military capabilities and acquired certain competitive advantages over the United States and its allies. The growing significance of emerging technologies has created new asymmetries in the force structures of great powers, altered the nature of strategic competition, and increased the requirements for designing and executing successful military strategies. Although it is clear that nuclear parity is no longer the only determining factor of stability, there are widely opposing views about the potential effects of new technologies. While there are a number of ways that emerging technologies could support stability, they also have the potential to undermine it. This essay unpacks how strategic stability, emerging technologies, and the new military domains are linked together in the current environment of great power competition. The first section examines the evolution of the concept of strategic stability and the main challenges to stability today. The next part describes the benefits, costs, and risks of multi-domain competition, followed by a section that dives deeper into the main challenges of multi-domain competition. The fourth part describes the options to manage the costs and risks through cooperation, while the final section concludes with a number of recommendations for long-term competition.

Strategic Stability and Competition in a Historical Context

With the Soviet acquisition of nuclear and then-thermonuclear weapons, leaders in Washington and Moscow in the 1950s realized that large-scale wars between nuclear armed powers could not be won and therefore must not be fought. Over the course of the Cold War, both the United States and the Soviet Union believed that strategic stability was a helpful concept for managing competition and avoiding major war between the two superpowers. The concept was primarily used in a bilateral sense, and with a focus to avoid nuclear war particularly due to fears over surprise attack.[133] The core idea was to stabilize the Cold War competition by ensuring that both sides had the ability to strike back with a devastating nuclear attack even if one of them attempted a disarming first strike.

Over the next few decades different interpretations of strategic stability emerged. These led to three distinct concepts of strategic stability: first-strike stability, crisis

133 Linton Brooks, "The End of Arms Control?" *Daedalus* 149, no. 2 (2020), pp84–100.

stability, and arms race stability. First-strike stability means that there are no incentives to use nuclear weapons first in a crisis. This line of thinking led to a greater focus on increasing the survivability of nuclear forces and strengthening the command and control (C2) systems. Crisis stability is a slightly broader concept since it means that in a crisis there are no incentives to be the first to use any form of military force. Those in pursuit of crisis stability focus on reducing the pressures to escalate a crisis into an all-out war that the participants may not be able to control. Finally, arms race stability means that neither side can improve its relative position by building up its nuclear arsenal. Seeking these three goals simultaneously was seen as a way to keep the strategic competition under control with important implications for modernizing the nuclear force and managing great power relations. In practice, this required developing force structures that minimized the likelihood of a first strike, pursuing arms control arrangements that capped the arms race, limiting vulnerabilities, and extending decision-making timelines for leadership. It also required implementing nuclear reductions where it was possible.[134]

However, history shows that the United States never fully accepted mutual vulnerability and consistently sought a qualitative advantage in strategic forces, meaning that America never completely accepted the idea of the nuclear revolution. Early in the Cold War, competition led to arms racing. The U.S. strategic advantage in the early 1960s alarmed the Soviet politburo, and as a result they moved to counterbalance the bomber advantage of the United States with a large silo force by the late 1960s. A similar dynamic in the late 1970s led the Soviets to counterbalance the U.S. ballistic missile submarine (SSBN) advantage with new mobile Soviet intercontinental ballistic missiles (ICBMs) and more survivable command and control.[135] But despite these competitive arms development dynamics, throughout the Cold War both sides saw it advantageous to limit the numbers of strategic arms where possible and to limit the competition in specific ways to reduce fears of a first strike.

Altogether, strategic stability and competition in the Cold War was nuclear-centric and bilateral. The great powers focused on the survivability of their forces while maintaining rough quantitative parity in strategic nuclear weapons. Today, the ambition to maintain quantitative nuclear parity between the United States and Russia has not disappeared, but become less prominent in the overall strategic relationship of the two states. The strategic competition is broadening not just horizontally, but also vertically. First, the security environment has become more multipolar. Due to its growing political, economic, and military influence, China has become an important strategic competitor to the United States. Biden administration officials refer to China as America's pacing threat that can pose a systemic challenge to the United States.

134 Elbridge Colby, "Defining Strategic Stability: Reconciling Stability and Deterrence," in *Strategic Stability: Contending Interpretations*, Elbridge Colby and Michael S. Gerson, eds. (Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, 2013), pp47–49.

135 Brendan Green, *The Revolution that Failed: Nuclear Competition, Arms Control, and the Cold War* (Cambridge, UK: Cambridge University Press, 2020).

The second major change occurred in the actual number and variety of forces that have a strategic effect, such as missile defenses, long-range conventional strike, cyber, and counter-space capabilities of the United States. Russia and China are increasingly capable of imposing these strategic effects by decrementing the expected efficacy of the other side's strategic and conventional forces. In addition, these new capabilities provide the ability to cripple an enemy society for longer periods of time without an overwhelming nuclear attack. Besides creating greater variety in available offensive and defensive strategic forces, these emerging technologies also increase asymmetries in force structures, which makes it more challenging to manage great power competition. As a result of the growing asymmetries, the principle of quantitative parity in nuclear weapons is no longer adequate to create stability.[136]

The 2018 National Defense Strategy Commission emphasized that U.S. adversaries are blurring the lines between conventional, unconventional, and nuclear approaches, and they are also blending nuclear, space, cyber, conventional, and unconventional means in their warfighting doctrines.[137] Due to the complexity of this multipolar and multi-domain strategic environment, it has become more difficult to distinguish between peacetime, crisis, and war, and it has also become more difficult to distinguish between stability and instability. Since there are no absolute conditions of stability or instability, it is more useful to consider it as a continuum, where U.S.-Russia and U.S.-China relations are somewhere on the scale between the two absolutes.

Understanding the Benefits, Costs, and Risks of Multi-Domain Competition

Emerging technologies have several disruptive effects and competition in the new domains have the potential to undermine strategic stability in various ways.[138] However, emerging technologies do not only pose dangers. They also open opportunities to exploit certain disruptive benefits that could actually support strategic stability and reduce the likelihood of war.[139]

A number of emerging technologies are newly present in the cyber and space domains, like cyber and directed energy weapons, but the growth of military operations in these domains highlight how they interact with nuclear forces. When looking at

136 Heather Williams, "Asymmetric arms control and strategic stability: Scenarios for limiting hypersonic glide vehicles," *Journal of Strategic Studies* 42, no. 6 (2019), pp789–813.

137 National Defense Strategy Commission, "Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission" (November 2018).

138 Jacek Durkalec et al., "Multi-Domain Complexity and Strategic Stability in Peacetime, Crisis, and War" Center for Global Security Research, Lawrence Livermore National Laboratory (2021). https://cgsr.llnl.gov/content/assets/docs/CGSR_Annotated_Bibliography_Emerging_Tech.pdf.

139 Brad Roberts, "Emerging and Disruptive Technologies, Multi-domain Complexity, and Strategic Stability: A Review and Assessment of the Literature," Center for Global Security Research, Lawrence Livermore National Laboratory (February 2021). https://cgsr.llnl.gov/content/assets/docs/EDT_ST2_BHR_2021.3.16.pdf. Accessed October 14, 2021.

the positive side and the disruptive benefits of these domains, there are seven main areas of focus:[140]

- Efficiency: cyber and space domains can improve the efficiency of military operations both in terms of cost and risk due to the enhanced intelligence and communication infrastructure they provide.
- Integration: these domains enable great powers to integrate both military and economic power at unprecedented levels.
- Operating under the threshold: the cyber and space domains offer a number of alternative tools of military and political influence that can provide benefits without having to cross the threshold of war.
- Amplification: emerging technologies have the ability to enhance the reliability of C2 systems, and improve intelligence, surveillance, and reconnaissance (ISR). As a result, they can act as a force multiplier by making military operations more efficient.
- Positive interference with other domains: due to improved ISR capabilities, emerging technologies can enhance transparency and improve the quality of assessments about the intentions and military actions of the adversary.
- Arms control benefits: these new domains can also help to advance arms control in the nuclear or conventional domains by using, for example, artificial intelligence (AI)-enabled space capabilities for verification.
- Last, we note that the cyber and space domains are largely out of the public eye. This provides a unique venue for signaling, cost imposition, and bargaining between states where audience costs are low.

In comparison to these benefits, there are a number of potential dangers that arise from the widespread use of emerging technologies. In this regard, three main themes dominate the discourse.[141] First, competition and conflict in the cyber and space domains have a strong potential to increase the fog of war. Strategic stability between adversarial states has been greatly aided by transparency, clear and direct communication, and signaling.[142] At the same time, these emerging domains are better suited to shielding information, and provide opportunities for deception and deliberate misinformation campaigns. This makes it very difficult to assess the intentions, military capabilities, and even maneuvers of adversaries, and it could make unwanted escalation or misunderstandings more likely between the great powers.

140 Jon R. Lindsay and Erik Gartzke, "Politics by many other means: The comparative strategic advantages of operational domains," *Journal of Strategic Studies* 43 (2020). https://doi.org/10.1080/01402390.2020.1768372. Accessed October 14, 2021.

141 Jacek Durkalec, et al., "Multi-Domain Complexity and Strategic Stability in Peacetime, Crisis and War."
Jon R. Lindsay, and Erik Gartzke, "Politics by many other means: The comparative strategic advantages of operational domains."

142 Erik Gartzke and Jon R. Lindsay, "Thermonuclear cyberwar," *Journal of Cybersecurity* 3, no. 1 (March 2017), pp37–48.

The second danger is about vulnerabilities: In a multi-domain environment, new technologies can create new vulnerabilities for the operation of both nuclear and conventional forces. Advancements in technology—introducing new vulnerabilities—could endanger C2 and ISR systems that underpin crisis stability.

The last theme is negative interference with other domains. A great example is offensive cyber capabilities that could disable nuclear C2 systems. If one side wins the competition in the cyber domain and can reliably undermine the other side's nuclear forces, first strike stability is in doubt for the weaker side which will give the stronger side a pronounced advantage in brinksmanship and crisis bargaining. If the weaker side is aware of this disadvantage, it will likely lead them to build up new C2 systems as well as perhaps more diverse weapons to build their way out of this situation.

Today, it is clear that the competition in the new domains is well underway. Both Russia and China have increased their investments in cyber and outer space capabilities. Emerging technologies have become critical in how the great powers deploy and operate their conventional and nuclear forces. This intensifying competition creates new dilemmas for the United States about how much restraint to show, and how intensely it should pursue the disruptive benefits of the new domains.[143] Russia and China are already conducting offensive operations in the new domains, directly threatening the U.S. homeland without crossing the threshold of armed attack. This raises important questions about the practice of deterrence both above and below the threshold of nuclear war. While emerging technologies provide new means of exploitation for adversaries, they also offer numerous benefits to the United States and its allies. The cyber and outer space domains add important non-nuclear capabilities to the strategic toolkit, which can strengthen the credibility of deterrence by reducing the reliance on nuclear threats in situations where they are not credible.

Another characteristic of the multi-domain competition is that it crosses many traditional boundaries. Important national capabilities are owned and operated by private sector entities. The fading lines between military and commercial actors create new vulnerabilities for enemy exploitation, but they also create new opportunities for innovation and public-private partnerships that could potentially improve situational awareness and help the United States to stay ahead of its adversaries.[144]

As highlighted above, competition in the new domains has many risks. While adversaries might intend to use emerging technologies to achieve strategic advantage early in a conflict and force the United States and its allies to capitulate, these new forms of competition can increase the fog of war and lead to unwanted escalation. Both Russia and China have been thinking about all-domain escalation for many

143 Jacek Durkalec, Paige Gasser, and Oleksandr Shykov, "5th Annual LLNL Deterrence Workshop Multi-Domain Strategic Competition: Rewards and Risks," workshop summary, Center for Global Security Research, Lawrence Livermore National Laboratory (December 2018). https://cgsr.llnl.gov/content/assets/docs/Deterrence_Workshop_Summary_Final2018.pdf. Accessed October 14, 2021.

144 Jonathan Reiber,"A Public, Private War: How the U.S. government and the U.S. technology sector can build trust and better prepare for conflict in the digital age," Center for Long Term Cyber Security White Paper Series, University of California - Berkeley (2019). https://cltc.berkeley.edu/2019/12/17/a-public-private-war/. Accessed October 14, 2021.

years, which gives them a certain degree of confidence about their ability to control a conflict. This creates a dual challenge for the United States: first, it needs to develop the necessary strategic thought to fight these types of new conflicts, and second, it needs to revise its operational plans to be able to escalate a conflict on its own terms to prevent a conventional fait accompli by its adversaries while also offering the necessary off-ramps to avoid an all-out nuclear war.

The Challenges of Competition in a Multi-Domain Environment

The first main challenge of multi-domain competition is integrating the different capabilities in the strategic toolkit. Integration offers many potential benefits to the United States and its allies. Russia and China have already begun integrating their new military strategic capabilities. They have also updated their strategic doctrine, developed new operational concepts, and implemented key institutional reforms. In order to counter these strategies and remain competitive, the United States and its allies will also need to better integrate its strategic capabilities.

Emerging technologies add a great degree of complexity to great power competition. As a result, the United States and its allies will first need to agree on the most important deterrence goals and then work to understand how domain-specific capabilities can help to achieve those goals. These deterrence goals should be tailored to specific adversaries and specific scenarios, which requires a clear understanding of Russian and Chinese capabilities, concepts, and theories of victory. Integrating capabilities across domains will require coordinated planning between regional combatant commands and the functional combatant commands in order to conduct operations with cross-domain effects. The United States has already made progress here, but further cooperation is needed with allied partners to develop an allied, multi-domain theory of victory.

There are many challenges of multi-domain integration.[145] The new domains are surrounded by a certain degree of secrecy, their expert community continues to operate in silos, and the strategic thinking is still far behind Russia and China. Moreover, strategic concepts are under-developed in these domains. The new vulnerabilities created by emerging technologies complicate deterrence strategy, while concepts like escalation, de-escalation, and signaling are still poorly understood in cyber space and outer space. Finally, the simultaneous development of a great variety of tools creates many competing demands, which further complicate integration.

The next major challenge of multi-domain competition is balancing the benefits and risks of the application of emerging technologies. In light of the advancements in Russian and Chinese modernization efforts, it is clear that a purely defensive strategy is a losing one for the United States and its allies. While increasing resilience to exploitation and reducing vulnerabilities should be part of the response, repeated

145 "Setting Priorities for Deterrence Integration," workshop summary, Center for Global Security Research, Lawrence Livermore National Laboratory (2021).

cyber attacks and the extensive counter-space capabilities of Russia and China make it imperative to compete on the offensive side as well. The United States will need to invest more in its own counter-space capabilities and expand its offensive cyber capabilities. Increasing the variety of non-nuclear strategic tools to complicate the adversaries' risk calculus is a crucial aspect of staying ahead in the competition, but the United States also needs to maintain a certain degree of restraint to avoid an unintended arms race, or an unwanted escalation.

Thus, the final challenge is maintaining a certain degree of stability and controlling great power competition. The aforementioned benefits and dangers of the new domains are relevant to all three concepts of strategic stability. However, the strategic community is deeply divided about the potential effects of emerging technologies, and every observation and hypothesis in the literature is contradicted by an entirely opposite conclusion by other scholars.[146]

In the case of first-strike stability, the optimistic expectation is that emerging technologies will support greater stability because a disarming first strike is more difficult to accomplish in the face of a greater variety of strategic tools. This line of thinking argues that in a multi-domain environment there is no escape from some form of retaliation after a first strike. Only offensive actions in outer space and cyber space that have a pronounced and targeted damage-limiting effect would guarantee major benefits that could outweigh the risks of escalation.[147] In addition, emerging technologies like laser communications and quantum key distribution can strengthen communications security, increase the survivability of forces, enhance the efficiency of C2 systems, and make early warning systems more capable and reliable. Advances in the miniaturization and proliferation of small satellites could have similar effects, making counterspace first strikes much more challenging. These effects would also support greater first-strike stability since they make the prospect of success less likely for a surprise attack and therefore reduce the incentives for preemption.

In contrast, the rather pessimistic view suggests exactly opposite conclusions. Emerging technologies could significantly undermine first-strike stability by increasing the incentives to strike first in these other domains. Advancements in the cyber and space domains dramatically increase the ability to fight at more intense speed and accuracy, and they also open up new ways to keep the enemy's C2 systems under threat.[148] These domains are also less visible to the public, making them more attractive areas for sparking conflict. This is because national leaders may have

146 Brad Roberts, "Emerging and Disruptive Technologies, Multi-Domain Complexity, and Strategic Stability: A Review and Assessment of the Literature."

147 Jacek Durkalec, Paige Gasser, and Oleksandr Shykov, "5th Annual LLNL Deterrence Workshop Multi-Domain Strategic Competition: Rewards and Risks," workshop summary, Center for Global Security Research, Lawrence Livermore National Laboratory (December 2018), pp11–12. https://cgsr.llnl.gov/content/assets/docs/Deterrence_Workshop_Summary_Final2018.pdf. Accessed October 14, 2021.

148 Michael C. Horowitz, "When speed kills: Lethal autonomous weapon systems, deterrence and stability," *Journal of Strategic Studies* 42, no. 6 (2019), p782. https://doi.org/10.1080/01402390.2019.1621174. Accessed October 14, 2021. Jacek Durkalec, Paige Gasser, and Oleksandr Shykov, "5th Annual LLNL Deterrence Workshop Multi-Domain Strategic Competition: Rewards and Risks."

more political leeway to walk away from a conflict that has gone poorly in areas that are out of the public eye and which preclude success in a more generalized conflict. Further, artificial intelligence is leading towards more militarily useful automated target recognition and faster decision-making, leading to potential improvements that militaries can harness for damage limitation and first strike capabilities. These factors make a decisive preemptive action seem like a high payoff strategy with great battlefield advantages for the side that strikes first.

From the perspective of crisis stability, emerging technologies could improve stability because they provide more non-nuclear options like conventional strike, cyber attack, or counterspace in a crisis. The greater variety of available tools makes the enemy's risk calculus more difficult and provides a high degree of credibility to deterrence threats even below the nuclear threshold.[149] The improvements in ISR capabilities through proliferated satellites and communications also make the enemy's actions more transparent, which reduces the likelihood of miscalculation and reinforces crisis stability.[150] Better information is likely to lead to better informed decisions, and machine learning and AI tools could provide significant benefits to information gathering and analytics. Lastly, a better and more secure information infrastructure could also support more direct channels of communication between world leaders, which improves signaling and reduces the risks of misunderstandings.

On the flip side, emerging technologies could also undermine crisis stability by compressing decision times for leaders. With the advent of hypersonic weapons and the automation of certain military capabilities, political leadership faces a growing challenge of shrinking decision times to detect an attack and decide about the use of force particularly in cases where key elements of the military force posture cannot afford to absorb a first strike.[151] Losing crucial time to have a consultative process and deliberate based on accurate and verified information both puts a huge pressure on leadership and increases the likelihood of mistakes. This creates a strong incentive to automate certain systems and reduce human control where one side's key forces cannot survive a first strike. However, over-reliance on autonomous systems has its own dangers. If the data is automatically believed and not double-checked by humans, it may result in automation bias.[152] If the information is unreliable

149 Brad Roberts, *Toward New Thinking About Our Changed and Changing World: A Five-Year CGSR Progress Report* (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2020), p63. https://cgsr.llnl.gov/content/assets/docs/CGSRfiveDIGITAL.pdf. Accessed October 14, 2021.

150 Zachary S. Davis, *Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise* (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2019), p11. https://cgsr.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf. Accessed October 14, 2021.

151 Adam Lowther and Curtis McGriffin, "America Needs a 'Dead Hand,'" War on the Rocks (August 16, 2019). https://warontherocks.com/2019/08/america-needs-a-dead-hand/. Accessed October 14, 2021.

152 Beyza Unal and Patricia Lewis, "Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences," Chatham House (January 2018), p9. http://www.menacs.org/wp-content/uploads/2018/01/Beyza_Cybersecurity-nw.pdf. Accessed October 14, 2021.

or manipulated by adversaries, policy makers will not be able to make accurate and effective decisions in a crisis.

Regarding arms race stability, the optimistic prediction is that the multi-domain environment creates new vulnerabilities among the great powers, and the recognition that mutual vulnerability is inescapable will eventually push them towards restraint and negotiated limits.[153] In the past, great powers have often competed to create the next most advanced weapon system to gain a competitive edge over their adversaries. However, many of these technological advancements did not last long, as either countermeasures were developed or the other great powers caught up.[154] The cyclical nature of technology development suggests that competition and the arms race in emerging technologies will not be the permanent solution in the long run because the new domains actually reinforce mutual vulnerability.

The opposing view to this prediction again suggests very different outcomes: Emerging technologies can provide major advantages to those who deploy a technology first or can sustain an advantage. One of the best examples is quantum computing that would provide an ability to penetrate sensitive communications, along with outmaneuvering and sabotaging the military operations of adversaries without the other side even noticing this vulnerability.[155] If a breakthrough in quantum communications is revealed, it could lead to technological deterrence through denial, an increased psychological impact of vulnerability, and a high payoff for the first to master it. These first-comer advantages create strong incentives for great powers to continue to compete in emerging technologies, and they undermine arms race stability. As long as the United States, Russia, and China believe that there are competitive advantages still to be gained and there is less risk in competing for these gains, they are not going to agree to mutual restraint and arms control.

In light of all these controversies, settling the dispute over whether a technology actually supports strategic stability or undermines it will be heavily dependent on the technologies in question, the specific scenario, the adversary, the timeline, and also the general status of great power relations. The application of these technologies will bring completely different benefits and risks in peacetime, crisis, and war.[156]

153 David C. Gompert and Phillip C. Saunders, "Sino-American Strategic Restraint in an Age of Vulnerability," Strategic Forum (January 2012), pp1–2. http://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-273.pdf. Accessed October 14, 2021.

154 Clarence Abercrombie and Heather Venable, "Muting the Hype over Hypersonics: The Offense-Defense Balance in Historical Perspective," War on the Rocks (May 28, 2019). https://warontherocks.com/2019/05/muting-the-hype-over-hypersonics-the-offense-defense-balance-in-historical-perspective/. Accessed October 14, 2021.

155 Elsa B. Kania and John K. Costello, "Quantum technologies, U.S.-China strategic competition, and future dynamics of cyber stability," 2017 International Conference on Cyber Conflict, Washington, DC (2017), p95. https://ieeexplore.ieee.org/document/8167502. Accessed October 14, 2021.

156 Brad Roberts, "Emerging and Disruptive Technologies, Multi-Domain Complexity, and Strategic Stability: A Review and Assessment of the Literature."

Managing Costs and Risks through Cooperation

There are essentially two ways to manage the costs and risks of multi-domain competition: by pursuing dialogue and cooperation where possible, and setting the right goals for long-term competition.

The United States has long tried to engage Russia and China on the topic of strategic stability. However, Beijing has repeatedly rejected the U.S. invitation to join these talks, and the Russian dialogue has also been rather sporadic and not necessarily productive. Over the past two decades, both states have argued that it is the United States that undermines strategic stability by its pursuit of absolute security.[157] Although both states claim in their rhetoric that their investments in new military capabilities are a response to U.S. developments, the advancements in Russian and Chinese military capabilities—including in emerging technologies like directed energy and counterspace weapons—have come a long way from the status quo ante. In fact, a thorough analysis of their modernization programs shows little to no evidence that their actions were driven by the desire to restore strategic stability.[158] Therefore, it seems that strategic stability remains an important concept in the rhetoric of all great powers, but in practice it has only limited the military developments of the United States. In the new multi-domain environment, there are clear signs of the Russian and Chinese ambition to continue to compete for military advantage, which makes it very difficult to have an honest discussion about strategic stability, restraint, and arms control. Elements of uncertainty and instability are likely to be part of great power relations in the foreseeable future.

In the U.S.-Russia relationship, Russia has long considered strategic stability in a much broader sense than the United States. The Russian interpretation of strategic stability includes nuclear capabilities, conventional precision strike, missile defense, and emerging technologies in the cyber and space domains, as well as information operations and broader political factors. The Russian approach has elements of hard power and soft power, and traditional military and political-psychological tools.[159] Because Russia has been paranoid about U.S. and NATO encirclement, its stability concept is mainly about a predictable environment. Moscow has been seeking restraint and arms control only in areas where it thought the United States could undermine the credibility of the Russian deterrent, and it also carefully guarded its zone of influence by creating a weak periphery with Russia-friendly leaders.[160]

During the Obama and Trump administrations, U.S.-Russian strategic stability talks did not accomplish much. Strategic relations have worsened, President Putin has

157 Ibid.

158 Jacek Durkalec, Paige Gasser and Oleksandr Shykov, "5th Annual LLNL Deterrence Workshop Multi-Domain Strategic Competition: Rewards and Risks."

159 Heather Williams, "Asymmetric arms control and strategic stability: Scenarios for limiting hypersonic glide vehicles."

160 Brian Rose, "Rethinking Approaches to Strategic Stability in the 21st Century," workshop summary, Center for Global Security Research, Lawrence Livermore National Laboratory (February 2017). https://cgsr.llnl.gov/content/assets/docs/StrategicStabilitySummaryFeb2017.pdf. Accessed October 14, 2021.

undermined the European security architecture in many different ways, and Russian paranoia remains over U.S. preemptive actions and covert operations aimed at regime change in Moscow. Russia has embarked on a modernization path that intends to achieve integrated strategic effects with a great variety of more survivable nuclear tools, and with additional non-nuclear tools as well. In light of all these developments, it seems questionable whether the United States and Russia still have a common understanding of the utility of strategic stability, and the meaning of this concept in the post-Cold War security environment.[161]

In the U.S.-China bilateral relationship, the situation is equally complicated. While the U.S. approach to strategic stability remains centered around crisis stability and arms race stability, China prefers a broader approach that looks at the general military balance. Beijing seems reluctant to use the concepts of the Cold War in its strategic relationship with the United States. Although both sides accept a certain degree of mutual vulnerability in their relationship, Beijing has long been pushing for an official U.S. statement about mutual vulnerability. China sees the U.S. refusal to do so as an indication of America's intentions to seek absolute security.[162] The invitations from the United States to join the Strategic Stability Dialogue have also sowed confusion in Beijing since the Chinese believe that strategic stability talks are only appropriate among nuclear equals. They saw these efforts of engagement as a plot to involve China in arms control and put restraint on its military modernization. Similarly to Russia, China is also worried about U.S. advancements in missile defense and counterforce capabilities that could undermine the credibility of the Chinese nuclear deterrent.[163]

Altogether, there is not much overlap between the strategic stability concepts of the United States, Russia, and China. Both Russia and China have included a broader set of issues under this umbrella, and they accuse the United States of undermining strategic stability. With the advent of multi-domain challenges and the increasing integration of forces, the complexity of the problem only became worse. Both Russia and China have made serious progress with integrating their strategic forces, a process that includes a growing number of emerging technologies. As described above, certain applications of these technologies might provide more stability between the great powers, but it is also very likely that new areas of vulnerability and instability will emerge. Developing a common understanding of strategic stability is further complicated by the fact that the United States, Russia, and China have different interpretations about the significance of the new domains. For example, Russia and China are increasingly looking at the cyber and space domains as important tools to shape the battlefield before an armed conflict would occur. At the same time, from a U.S. perspective, cyber capabilities are just one item in the toolbox, and

161 Brad Roberts, "Strategic Stability Under Obama and Trump," *Survival* 59, no. 4 (2017), pp47–74.

162 Brad Roberts, ed., *Taking Stock: U.S.-China Track 1.5 Nuclear Dialogue* (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2020). Accessed October 14, 2021. https://cgsr.llnl.gov/content/assets/docs/CGSR_US-China-Paper.pdf.

163 Brian Rose, "Rethinking Approaches to Strategic Stability in the 21st Century."

they have been mostly used for signals intelligence and counterterrorism.[164] While there are such divergent views among the great powers about the utility of emerging technologies and the role of the new domains, it will be very difficult to come to a mutual understanding of strategic stability in a multi-domain environment.

In order to start a constructive dialogue, the United States, Russia, and China should agree on a few basic principles. Two of these—restraint and formal dialogue—should be key. Strategic stability in the past has always included the logic of equilibrium in some aspect of the military balance. In a multi-domain competitive environment this will probably mean quantitative equilibrium in some cases and qualitative equilibrium in others. It has also included elements of restraint and arms control to cap the destabilizing effects of arms racing. Even if the United States does not accept a mutual vulnerability relationship with China, there may be areas of the multi-domain competition that Washington and Beijing may be mutually inclined to avoid. Lastly, strategic stability has historically been the most successful between adversaries when they were willing to sit down and discuss their concerns in some kind of official framework.

From a U.S. perspective, it will be key to recognize that it cannot deny Russia and China the basic means to defend their core national security interests. However, the United States must remain focused on the ability to deny them both conventional and nuclear fait accomplis against its regional allies and partners while also maintaining effective international norms in peacetime.

Setting the Right Goals for Long-Term Competition

Since both Russia and China have dramatically built up their military capabilities over the past few years, restoring stability will also require some competitive response from the United States, especially in the cyber and space domains. This is important not only for stability in the new domains, but also to hedge against a future that is increasingly uncertain and may bring strategic surprise.

In terms of capabilities, Russia and China have both invested in counter-space arsenals, as well as new space capabilities to enable their military forces. These are aimed to prevent the United States and its allies from intervening in a regional conflict and make sure that they can successfully create a conventional fait accompli. Both Russia and China see U.S. advantages in space-based capabilities as crucial to respond rapidly in a crisis, strike precisely, project power globally, and command and control forces in multiple distant theaters simultaneously. Russia and China have postured their counter-space capabilities to counter these advantages, as they asymmetrically hold U.S. capabilities at risk. Therefore, in the space domain, the United States needs to maintain its advantages by defeating or denying the most

164 Ibid.

threatening adversary uses of space.[165] While the United States should improve the resilience of its space-based assets and expand its own set of counter-space capabilities, this is not only a capability problem. It will be equally important to demonstrate that the United States has the political will to protect its interests, and that it has the capability to act in an appropriate and proportionate way.

Similarly, the appropriate mix of capabilities should also include more counterforce capabilities in cyberspace along with a strong emphasis on increasing the resilience of the military and civilian infrastructure. Since Russia and China rely on deterrence by denial, the United States should work with allies to break that up by increasing technology cooperation and by helping allies achieve more in their own cyber and outer space capabilities. In addition, the United States should also increase the risks for Russia and China to attack these capabilities by setting escalatory thresholds in its declaratory policy.

While developing a full spectrum of offensive capabilities will be important to complicate adversary risk calculus, the United States and its allies should only use these assets when absolutely needed, and only in an appropriate and proportionate way to preserve alliance unity—as well as to uphold the principles of international law.

In terms of integration, the United States and its allies should work to better understand how cross-domain effects can be orchestrated in joint and allied military operations. It is also important to continue conventional-nuclear integration and explore what more can be done in "left of launch" to counter long-range missile threats with non-kinetic options.

Altogether, Russia and China are already engaged in a strategic competition with the United States and its allies. Therefore, focusing exclusively on defense is not a winning strategy. It remains important to avoid the unintended costs and risks of multi-domain competition, but the United States will also need to pursue certain strategic benefits to avoid a major war with its adversaries. This will require close coordination with allies, better integration of the strategic toolkit, and a whole-of-government approach.

165 Benjamin Bahney, ed., *Space Strategy at a Crossroads: Opportunities and Challenges for 21st Century Competition* (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2020). https://cgsr.llnl.gov/content/assets/docs/space-strategy-at-a-crossroads.pdf. Accessed October 14, 2021.

Building U.S. Capacity for Multi-Domain Challenges

Michael Albertson

As the previous chapters have amply laid out, the security environment requires the United States to consider where multi-domain approaches provide the best solution to its current and anticipated operational challenges. An initial answer is that most, if not all, identified operational challenges will have multi-domain solutions, or at least should incorporate these approaches when analyzing problems. Upon further review, some challenges may have a single solution within a specified domain, as there may be ways in which tactics or operations can be adapted or new tools developed within a single domain that significantly heightens our capabilities to solve hard operational problems. There have been times in politics and warfare when a single approach or a single technology has enjoyed a period of dominance. These periods are usually brief, however. Adversaries adapt or mimic. Greater complexity often requires new strategies, operations, and tactics to increase benefits.

However, these new strategies, operations, and tactics bring with them a set of structural and bureaucratic challenges that stymie the ability to build U.S. capacity. In the modern strategic environment, everything that has been defined as a challenge likely remains so because it cannot be solved cleanly in a single domain with a single tool or by a single bureaucratic entity. The challenge is not for a lack of tools. The tools themselves are likely already in the toolkit or are in some stage of conception or research and development. More tools are always needed, but the sheer relative size of the U.S. defense budget makes this a problem of prioritization and cost-efficiency rather than a lack of strategic thinking and resources.

Instead, the central question facing the United States is whether it has the right people and the right bureaucracy to find the answers to hard problems by combining experiences working in multiple domains, comparing the strengths and weaknesses of both red and blue, and bringing a variety of organizational perspectives to the table. The challenge is always in finding the craftsperson or artisan who knows how to concurrently use the tools to best effect to solve hard operational problems.[166] These people are rare in organizations, and they have not been consciously developed over the past three decades to tackle the problems facing the United States. Hence the organizations and agencies able to do this kind of thinking over sustained periods—that is, beyond the tenue of a specific gifted individual analyst or leader—are also

166 For example, key to DARPA's Mosaic Warfare concept is developing and fielding "mosaic enablers," the people capable of determining and integrating the various capabilities. Lt. Gen. David A. Deptula USAF (Ret.) and Heather Penney, "Mosaic Warfare," *Air Force Magazine* (November 1, 2019). https://www.airforcemag.com/article/Mosaic-Warfare/#:~:text=Mosaic%20warfare%20is%20one%20answer%3A%20a%20way%20of,environment%20and%20the%20shortcomings%20of%20the%20current%20force. Accessed October 13, 2021.

rare. All too often, a rigid mindset is applied to the problem. A person or organization having a hammer in its hands wants to use the hammer for every task and does not even speak the language or understand the lexicon of the person with the saw or the screwdriver, much less know how to use the other tool to greatest effect.

So how to overcome these structural and bureaucratic challenges to build capacity? The first step is understanding the problem of perspective in tackling the challenges with multi-domain solutions. Two strong emotional responses are frequently displayed in articles and workshop discussions when it comes to the issue of multi-domain complexity.[167] These are evinced by organizational leadership and mirrored in their organizations and bureaucratic culture. The first response is one of attraction—the topic is large, challenging, alluring, or at the forefront of modern competition, for example, and thus must be the core organizational focus moving forward. Multi-domain deterrence, strategic competition, and emerging and disruptive technology—these have become the new national security buzzwords after two decades spent inside the lexicon of counterterrorism and counterinsurgency. The desire is to tackle the entire subject holistically, depict it graphically, and master it. Viewers receive complex depictions of the wide view of the overall multi-domain problem, accompanied by graphics of the overall complexities of a multi-domain environment and dire warnings of the adversary's integrated capabilities. What is lacking, however, is the ability to zoom in to particular problem sets, break this view down to its smaller components, and identify existing or desired connective tissues which will knit all of the pieces together to form a more effective whole.

The other response is one of repulsion. This challenge is so immense, so murky, and so complex that leadership and organizations are reluctant to venture outside of their own domain or their existing analytic skill set. Barriers exist to exploring and understanding new domains—challenges with mastering a new lexicon of new terms, acronyms, bureaucracies, and classification barriers, for example—creating a high entry point necessary to being considered an expert in the field. The risks to rewards here is apparent, as it is far easier to stay within a lane, particularly in areas like cyber and space. Both have seen massive bureaucratic growth, thus providing clear paths for one to develop a monodisciplinary career. Moreover, there are few professional incentives for people to be jacks of all trades: to leave comfort zones in a single domain, to learn and grow in another, and return to apply their knowledge with a wider and fresher perspective. Even rarer are those who already exist in an organization who capable of doing this work after two decades of focus elsewhere.

Both these reactions lead to frustration. Organizations, leaders, and people become disillusioned because they rush to do everything or learn everything at once. Alternatively, these entities are reluctant to move out of their comfort zone, stymied by

167 See, for example, the materials in Mike Albertson, "Annotated Bibliography: Setting Priorities for Deterrence Integration," Center for Global Security Research, Lawrence Livermore National Laboratory (August 30, 2021). https://cgsr.llnl.gov/content/assets/docs/Deterrence_Integration_Annotated_Bibliography.pdf. Accessed October 13, 2021. See also the workshop summary https://cgsr.llnl.gov/content/assets/docs/Workshop_Summary_Integration2021.pdf.

real or imagined roadblocks warning that their expertise in a particular domain is not at all applicable to another, or that knowledge of Red is unimportant to understanding the problems of Blue. Senior leadership grows impatient. They feel that they, the ones with the least amount of time available for strategic thinking, are forced to deal with the challenges of adjudication and integration of the multi-domain toolkit because of their wider bureaucratic remit. But looking below them, they find they lack the people and the teams of strategic thinkers capable of applying multiple perspectives to these issues: the blue and the red, the regional and the functional, the policy and the intelligence, the various domains.

All of this reinforces the perception of the sense that the United States will never get this challenge of multi-domain right. At the same time, there is a growing sense that adversaries have studied, mastered, and implemented these concepts and operations.[168] Organizations instead spend time pursuing false leads—coming up with new concepts, new names, new terms, and new titles for already explored territory—rather than venturing further in an organized fashion. Jumps between terminologies and definitions add to the confusion and increase the delay. So again, where does the United States find the people, how does it create the organizations and empower the leadership to grow them, and how should the work be organized around these issues to build meaningful capacity?

The next step is to recognize is that this is not an impossible task. The key operational challenges today have eternal dimensions. It has always been hard to properly combine political goals and war aims in strategy or to combine arms on the battlefield to greatest effect. It has always been hard to take possession of fortified territory or hold possession of unfortified territory, particularly when it is close to an adversary and far away from the homeland. It has always been hard to cross a body of water to take possession of an island, as British history has shown on repeated occasions. And, as some have found to their dismay, landing with an army intact does not mean victory in all cases. The motivations and internal machinations of adversaries have always been difficult to discern, anticipate, and prevent. Determined and capable adversaries who seek to revisit past historical high-water marks, trials to the existing global order, the challenges of geographical distance, the factors of time and speed, the hesitation or over-eagerness of allies—all of these have posed persistent operational challenges.[169]

New capabilities in today's age of technological advancement have promised to solve these persistent challenges, with decidedly mixed results in their ability to deliver on these promises. But historical perspective shows that the operational

168 For more on how Russia and China have approached the challenge of multi-domain complexity, see Brad Roberts, *On Theories of Victory: Red and Blue*, Livermore Papers on Global Security No. 7 (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2020). https://cgsr.llnl.gov/content/assets/docs/CGSR-LivermorePaper7.pdf. Accessed October 13, 2021.

169 One example of this can be found in Jacek Durkalec et al., "Workshop Summary: Net Assessment and 21st Century Strategic Competition," Center for Global Security Research, Lawrence Livermore National Laboratory (June 29-30 and July 1, 2021). https://cgsr.llnl.gov/content/assets/docs/NetA_Workshop_Summary.pdf. Accessed October 13, 2021.

challenges facing the United States today have been grappled with in other settings, and that rarely is there a single solution or single technology to solve these problems.[170] Articulating a plan for stability in space, defending forward cyber operations, integrating artificial intelligence capabilities—these are not ends in and of themselves, but means to ends to solve hard terrestrial operational problems grounded in time, distance, and an adversary mindset. Most operational problems have been solved by innovation, frequently by applying something new and novel in creative ways. Such innovation requires creative thinkers, an open mindset, and bureaucratic fluidity. What steps can individuals and organizations within the U.S. government take to build capacity?

In his book *Leading Teams: Setting the Stage for Great Performances*, J. Richard Hackman identified the four fundamental questions central to an organization's identity. These must be answered when tackling a new challenge or building capacity. The questions are:

1. **Who decides?** Who has the right to make decisions about how the work is carried out, and to determine how problems that develop are to be resolved?
2. **Who is responsible?** Where do responsibility and accountability for performance outcomes ultimately reside?
3. **Who gains?** How are monetary rewards allocated among the individuals and groups who help generate them?
4. **Who learns?** How are opportunities for learning, growth, and career advancement distributed among organization members?[171]

Hackman went on to note that the answers to these questions help determine the organizational structures: the authority structure (who decides?), the work structure (who is responsible?), the reward structure (who gains?), and the opportunity structure (who learns?).[172] The answers to these questions are beyond the scope of this paper, but they should be in the forefront of leaders' and organizations' minds at they look to build future capacity in multi-domain deterrence. These questions serve as the homework of tomorrow.

A set of six concrete recommendations are designed to aid this thought process:

1. **Create an enduring integrated strategic review process**
2. **Find or mold the long-term human capital necessary to do the thinking**

170 Thomas G. Mahnken, *Forging the Tools of 21st Century Great Power Competition* (Washington, DC: Center for Strategic and Budgetary Assessments, 2020). https://csbaonline.org/uploads/documents/GPC_Final_Report_Web.pdf. Accessed October 13, 2021.

171 J. Richard Hackman, *Leading Teams: Setting the Stage for Great Performances* (Boston: Harvard Business School Press, 2002), p243.

172 Ibid., pp243-244.

3. **Re-examine the existing bureaucracy**
4. **Form analytic testbeds**
5. **Choose the right experiments with the right teams**
6. **Understand the long-term aspects of the multi-domain deterrence challenge**

These recommendations are admittedly disparate in nature. Some are more national or general in character; others are more relevant to specific organizations than others. Much of this is due to the complex nature of the multi-domain deterrence problem. But there are also inherent competitive advantages which some organizations have while others do not. Some organizations can expand on expertise in specific capacities to explore new domains. Others can easily channel their workforce into new areas. For many organizations, breaking down silos and incentivizing multi-domain thinking is the largest near-term priority. Much of these recommendations will depend on an organization's ability to answer the key questions related to authority, work, reward, and opportunity.

1. Create an enduring integrated strategic review posture process

A holistic, integrated strategic posture review is a welcome first step to building institutional and human capacity. The problem has been diagnosed, and a structural solution has been proposed.[173] It should take care, however, to avoid the following process pitfalls to avoid being a disappointment and thus disincentive to future work.

The first pitfall to avoid is to render the solution meaningless by failing to implement it. If it is to be a truly integrated posture review, then it must also have an integrated implementation process that continues to strengthen connections across multiple domains, people, and entities identified in the review, and to translate the report's recommendations into concrete actions and enhanced capabilities.

The second pitfall to avoid is create an integrated review that is equivalent to a piece of plywood, a composite which appears from afar to be a solid whole but one on closer examination that is actually composed of thin separate layers held together with weak glue. If it is simply a standard set of distinct posture reviews layered one on top of the other and coated by an introduction and conclusion, it is of little more value than the separate stovepiped review processes from the past. A more effective metaphor is that of a tapestry comprised of many, small, and distinct threads that have been interwoven together, thereby touching other strands and strengthening the object far beyond that of its separate elements. As a result, the overall product is a larger piece of material with an entirely new purpose.

173 More recommendations on the posture process can be found in Anna Péczeli et al., "Workshop Summary: The 2021 Defense Strategy Review and Modern Strategic Conflict," Center for Global Security Research, Lawrence Livermore National Laboratory (December 15-17, 2020). https://cgsr.llnl.gov/content/assets/docs/The-2021-Defense-Strategy-Review-and-Modern-Strategic-Conflict.pdf. Accessed October 13, 2021.

The final pitfall to avoid is a failure to use the posture process as one of self-examination. A devil's advocate should be designated to question major assumptions; this should be the responsibility of a consciously assigned agent in the room, not the underrepresented agency member allowed to be at the table. Key questions are likely to arise that may not be able to be fully explored given the administration timelines; these should be documented for further exploration. Participants should be constantly on the lookout for people, topics, and organizations that are missing to discover potential myopias and blind spots. Finally, there should be a recognition going in that the first document in a new process is likely the hardest one and could require more time and energy than anticipated. There is no perfect policy process, only varying tradeoffs. The evolution of the Nuclear Posture Review process shows that there are benefits and downsides to differing approaches, but few hard and fast rules.

2. Find or mold the long-term human capital necessary to do the thinking

A posture review is at its heart a collection of people: individuals with different backgrounds and perspectives representing bureaucracies with different equities in a room collaborating and competing within a consensus document. Does the United States have the human capital to do this kind of long-term analytic thinking?

Unfortunately, the consistent answer in many workshops and presentations is no. As one Center for Global Security Research (CGSR) workshop panel titled "Out-Thinking Our Adversaries" noted:

> *There is the need to better prepare leaders for the future. Not only is there a need for buy in from the military education system, there needs to be a stronger focus on teaching concepts such as deterrence, crisis stability, and escalation—all of which are not well understood in the operational sense. Investment in future leaders' education should be prioritized, while ensuring that future military leaders work on real world problems that align with today's most pressing challenges. The persistent challenge is how to educate political leaders about thinking on strategic matters and engage academia to focus more on providing practical recommendations on these issues.*[174]

Several factors have caused this scarcity of analytic depth. One reason is that while some areas have seen expansion, that expansion has tended to be one-dimensional within the domains of space and cyberspace. Two, human capital has been focused elsewhere, allowing the knowledge base to atrophy over the last three decades in several key areas including on Russia and nuclear issues. Three, cross-pollination over a career remains the exception rather than the rule. People tend to be incentivized for promotion within a particular domain or bureaucracy. Rotations outside

174 Jacek Durkalec et al., "Workshop Summary: Multi-Domain Strategic Competition: Rewards and Risks," Center for Global Security Research, Lawrence Livermore National Laboratory (December 2018). https://cgsr.llnl.gov/content/assets/docs/Deterrence_Workshop_Summary_Final2018.pdf. Accessed October 13, 2021.

an organization are challenged both in finding the right person to go off and do a new challenge as well as find a use for their increased talents when they return home. Collaboration between many offices, even when under the same Deputy Assistant Secretary or Assistant Secretary, is far less common than it should be. Rare is the person who moves between functional and regional offices, intelligence and policy, studying Red and Blue or several different Reds, or various domains. Rarer still is that the movement occurs in an organized and intentional fashion aimed at better training an individual or team to tackle a particularly hard operational problem. Four, those designated by an organization to be integrators—those who are responsible for seeing the big picture over many areas–are typically too senior (and thus too busy) to focus on the strategic landscape. Their days are at the mercy of their inbox and meeting schedules, with the immediate fires dominating the time to sit and plan longer-term.

The level of human capital required cannot be created overnight. It requires a particular amount of exposure for someone to develop and gain the necessary new perspectives and skills over the course of their career. Moreover, it takes the right position with enough time away from the demands of the inbox to think about hard operational problems. Finally, it takes the right organizations and mentors to guide people on next steps of their development.

Two immediate steps stand out as ways to improve human capital. The first is the need to create dedicated groups of cross-pollinators at lower levels throughout the U.S. government, people sprinkled throughout agencies and organizations who can speak at some level of competency about other organizations, domains, and mindsets. The initial exposure in a person's career to bigger-picture perspectives should not occur only when they get promoted to a senior level position, nor should it take place when they work in the outside expert community after leaving government. It needs to be done consciously over a person's career as a normal part of professional development, and this experience should be constantly utilized in their day-to-day mission functions within an organization.

Key to developing these lower-level cross pollinators is the second step: creating a well-functioning rotation system that moves employees out and back into home organizations. So much depends on a well-developed rotation framework to develop this talent, yet far too much of the rotation system is encumbered by bureaucracy. It is difficult to leave (or, more accurately, to be allowed by an organization or management to leave), and it is difficult to return. Opportunities become available on a chaotic ad hoc basis. Organizations are reluctant to let talent, particularly young and promising talent, leave on rotation. With an eye on narrow short-term results, leadership often fails to see the value in sending people to work and grow outside of their narrow field. Coming back to a home organization, newly developed skills are frequently left to wither upon re-entry to the organization. People have broader perspectives and bigger questions, only to be left unhappy upon being asked to stay confined to their former position.

If organizations want to attract and develop the people to tackle these hard operational problems, time and effort is required to put an efficient rotation system in

place. The integrated review process will create a new set of people across the United States bureaucracy exposed to this challenge as well as the need for more thinking about multi-domain deterrence. This provides an opportunity to be seized. How can we best use those who have participated in an integrated, multi-domain process to build expertise and understanding in their home organizations?

3. Re-examine the existing bureaucracy

The next step looks beyond the process and the people to the larger bureaucracies: does the United States have the organizations and the organizational structure to do this kind of long-term analytic thinking on multi-domain deterrence? Again, the answer from senior leadership in workshops is a resounding no. Current organizational structures are not designed for this level of scope and complexity. As a recent CGSR workshop summary from a panel titled "Towards a Better Result in 2021" documented:

> *What is needed is a coordinated approach across the U.S. government (DOD, State, Treasury, Commerce, and possibly others as well). This seems to be a huge challenge for the United States because the agencies have been Balkanized, and they do not coordinate well on these kinds of challenging issues [as they] involve hard trade-offs. In principle, it should be the National Security Council that brings these together, but they are mostly consumed by short-term problems and immediate responses. Instead, the United States and its allies need a sustained, long-term interest and effort to think through how they can coordinate response to Russian and Chinese challenges.*[175]

In fact, there are even more silos now than 10 years ago, with the creation of separate stovepipes for cyber and space issues.

The list of hard questions for organizations is growing longer. What organization or individual is the integrator? Who at the upper levels is looking in all these silos for biases and blindspots? Which manager is encouraging their cyber experts to work on nuclear issues, or sending their U.S. nuclear capabilities analyst to go work in intelligence on China? The "Who sits at the head table?" or "Who gets in the room for the meeting?" questions also present major challenges in Washington the broader and more complex the topic. With fewer people who can represent larger issues, conference rooms fill up quickly as more and more people representing narrow, discrete organizational equities demand a seat at the table. Lowering that number requires going up the organizational pipeline to busier senior officials, with the resulting loss of detailed knowledge at the discussion table.

In recent discussions on multi-domain deterrence and comparing the United States and its potential adversaries, major structural changes have been discussed

175 Ibid., p19.

but ultimately discarded.[176] One has been the creation of a Russian General Staff-like entity designed to do this kind of integrative, longer-term analytic function, an organizational conception which runs counter to the historic role of the Joint Staff. Another has been an update of the 1986 Goldwater-Nichols Act, which was an attempt to resolve problems related to interservice rivalries and challenges related to coordinating interservice cooperation on needed concepts such as Air-Land Battle. There are questions whether Goldwater-Nichols—now 35 years old—is still relevant or whether there is a need for major structural reforms in light of the changed security and technology environment. All of these are ideas are worthy of further exploration in other venues.

Within this chapter however, a few recommendations emerge on what do within bureaucracies. The first pertains to silos, specifically identifying silos and a conscious decision taken by leadership to detonate entirely or blow holes in the sides of these bureaucratic silos. The second is identifying how to integrate offices at key junctures or nodes. Senior officials are not an effective substitute for teams specifically tasked with creating and maintaining the connective tissue needed to tackle hard problems. These cells should be identified, created, and empowered where they do not exist already. They need to be seen as representing senior leadership. The third is determining where and how to best place the cross-pollinators within an organization, as well as ensuring that they have a seat at the table and are encouraged to fully participate and contribute substantively in meetings. As with the human capital recommendations, much of the focus here is on fluidity—the rejection of large scale, difficult to evolve reorganizations in favor of the rapid creation of small, dynamic teams to explore difficult issues. The final recommendation is openness. Interesting analysis is meaningless if it cannot be seen by anyone other than the writers and the sponsors. If work is being done in this area, it needs to be shared. If some of it is classified, then it should be downgraded or declassified as appropriate.

4. Form analytic testbeds

The challenge then becomes with what mindset should an organization approach such a large and daunting problem set as multi-domain deterrence. What role can and should the organization play in accelerating progress toward these capabilities and thinking? Simply put, the advice would be to approach its work much as scientists do in a laboratory. These are hard challenges for any organization to tackle immediately or plan for tackling over the long term, so some degree of experimentation is likely required. The overall organizational goal should be to serve as a model for others to follow, with a focus on being flexible, agile, responsive, and innovative. Some organizations will have a better personnel model or organizational culture than others to quickly and easily create interdisciplinary teams, particularly those where people can work portions of their time on specific projects and those where the organization

176 Ibid.

has a history of rapid personnel movements in response to big challenges. All of this requires pulling experts from a lot of different backgrounds or departments quickly when the need arises. It also requires an understanding of the level of effort required. There will be a need to explore hard operational challenges, take some risks, pursue some false leads, and try things that may not necessarily work. This kind of calculated risk taking should be baked into the DNA of organizations working on these issues. Both positive and negative lessons learned should be shared across organizations to work in this area further.[177]

5. Choose the right experiments with the right teams:

As discussed in the opening of this chapter, a key decision is where to begin, resisting the emotional poles that lead to intellectual theorizing overexhaustion or overcaution. Several concrete recommendations would be to:

- Resist the temptation to tackle the whole field at once
- Do not assume every hard operational problem has a multi-domain solution
- Choose a select group of smaller problems to analyze in a multi-domain fashion
- Bound the problem by setting an appropriate scope and scale for the project

The topic of multi-domain deterrence is an immense one, and the only approach likely to succeed is to break it down into smaller composite pieces and then begin reassembling the pieces through the discovery of important interconnections. Attempts to tackle everything at once will likely result in a long process and a set of findings outlining how difficult the problem is, without much in the way of recommendations and results. What furtherance of the multi-domain deterrence problem desperately needs are analytic experiments that show how analysis is done well. Such discrete projects brought to completion with interesting conclusions would serve as models for future work, testbeds for building multi-domain expertise, and pieces of a larger multi-domain deterrence architecture.

These testbed explorations require the right interdisciplinary teams, formed with an eye for both short-term project success as well as longer-term human capital development. Teams should integrate policy and technical experts, Blue and Red specialists, and discussion-specific positions such as devil's advocates, moderators, and notetaker. Experts from other domains should be brought in to provide fresh, comparative perspectives. Bringing together the right mix of expertise at the table is important—strategic thinkers, technical experts, representatives from multiple domains, people willing to challenge the process and lead, guide, and report back to others what was accomplished. Recording the lessons learned from the process is

177 An excellent book on innovative culture can be found in Adam Bryant, *Quick and Nimble: Lessons from Leading CEOs on How to Create a Culture of Innovation* (New York: St. Martin's Press, 2014).

critical, both to teach other people how to do it and improve it for the next iteration. Everyone who goes through such a project should be an apostle—someone who can go out, convince others of the value added in doing these kinds of projects right, and potentially lead their own multi-domain research project. With such a team, people can be provided with a hard problem, a collaborative environment, and time to think.

6. Understand the long-term aspects of the multi-domain deterrence challenge

The underlying analysis requires a focus on long-term sustainment: building the human capital, the organizational capacity, and a track record of experiments and results. All this builds muscle memory, both in individuals and in the organization. An analogy can be drawn with learning how to play a musical instrument, where standard best practices can be applied just as well to this endeavor:

- Practice makes perfect
- Learning slow helps you forget slow
- Smaller shorter sessions than longer sessions
- Muscles remember technique, whether good or bad
- Break songs into smaller pieces
- Memory resides in the brain, not the muscles
- Be patient—the faster you go, the worse your habits will be, and the more you get frustrated

Multi-domain deterrence requires both a long-term mindset and a focus on building something new from the ground up. It is a deliberate process of conceptualizing the work in small pieces, doing the work well, learning the process, reporting the results, aggregating the findings, improving the process, and repeating the process. Giving individuals and teams a model of how to do this well, along with the ability to teach others how to analyze and collaborate to be most effective, will be enormously helpful in the next 10 years as the United States attempts to try and build the human and organizational capacity needed to tackle the problem of multi-domain deterrence.

Seizing the Moment: Integrated Strategic Deterrence, Long-Term Competition, and the National Laboratories

Kim Budil

While the end of the Cold War lowered tensions and fostered a sense of optimism about international cooperation, the international security order over the past several decades has become increasingly complex and contested. Over this same period, technological progress has been accelerating across a wide range of domains. Moreover, the barriers to accessing advanced technologies, once the domain of nation states, have been dramatically lowered. This convergence of forces—increased global competition across security and economic spheres, an accelerating pace of innovation, and a highly democratized science and technology (S&T) ecosystem—has brought leaders across the political spectrum to a common conclusion: Speed and agility are essential, and our ability to out-innovate our rivals will be central to strengthening deterrence and stability.

At Lawrence Livermore National Laboratory (LLNL), we have a special responsibility in this regard. We are a federally funded research and development center (FFRDC), mandated to "operate in the public interest with objectivity and independence"[178] and chartered to help the nation address the most significant challenges of the day. LLNL also has a rich legacy of science and technology innovation, driven by our spirit of technical ambition, team-oriented approach, and willingness to embrace new thinking at critical moments. To ensure the laboratory is bringing the full range of its capabilities and expertise to best address these significant challenges, LLNL has conducted a broad review of its mission and ongoing work to identify opportunities to "up our game." In summer 2021 Lab leadership identified four specific mission focus areas that represent today's most significant national security challenges—areas where we have the opportunity to have a much larger impact by bringing the whole of our capabilities to bear to address these critical national needs. While our core mission focus area continues to be the future of nuclear deterrence, this is also a cornerstone of an emerging mission focus on integrated deterrence and competition (IDC). The other two are climate resilience (adapting to and mitigating the effects of a changing climate) and biosecurity (ensuring earlier detection and more rapid response to emerging pathogens, either natural or manmade).

To better understand how we got to this point and where we are headed, this chapter proceeds as follows. It begins with a review of where we as a nation and we as a laboratory have been in the IDC mission focus area, and proceeds with a discussion of key trends. It then sets out a vision of what the national laboratories

178 Federal Acquisition Regulation 35.017(a)(2).

and other partners can contribute at the national level, with a review of key building blocks. It closes with a discussion of our pathway forward.

Where We've Been

In recent years, a number of trends have come into focus that, cumulatively, have compelled a new national approach to deterrence. One trend is geopolitical: the clear and dramatic erosion in the security environment. The cautious optimism about trend lines in the security environment that marked the national security strategies of the first three post-Cold War presidential administrations has given way to rising alarm. Today, the United States and its allies face two revanchist and nuclear-armed major power rivals, a regional challenger in North Korea that is nuclear arming, and an Iran whose strategic intentions toward nuclear weapons remain unclear. These rivals also see an opportunity in growing doubts about the credibility of U.S. security guarantees and the effectiveness of extended nuclear deterrence.

A second trend is technological: All of these challengers are applying emerging and disruptive technologies, such as advanced sensors and artificial intelligence, in pursuit of military advantage and decision superiority. Moreover, ready access to and exploitation of the space and cyber domains have added significantly to the complexity of this competition. Russia and China have led the way in integrating these new technologies into multi-domain strategies and postures aimed at negating U.S. military superiority. Competition for advantage is intensifying.

The third trend is in leadership focus. Leaders at the Department of Defense (DOD) first articulated a high-level approach to the new technology environment in its first Quadrennial Defense Review of 1997, with the commitment to pursue "full spectrum dominance." The discussion of cyberspace and outer space as domains of military competition blossomed in the Obama period, when the term "cross-domain deterrence" came into vogue as a way to drive thinking about the diversifying strategic toolkit. During the Trump administration, emphasis shifted to multi-domain deterrence operations and the particular new requirements of long-term rivalry and competition for strategic advantage. In 2021, this focus has evolved to integrated deterrence. As Secretary of Defense Lloyd Austin has argued, the United States needs "a new vision for deterrence in this century. We call this vision integrated deterrence. I'll have more to say about this in the weeks to come, but basically, integrated deterrence is about using the right mix of technology, operational concepts, and capabilities—all woven together in a networked way that is so credible, and flexible, and formidable that it will give any adversary pause."[179]

179 C. Todd Lopez, "Defense Secretary Says 'Integrated Deterrence' is Cornerstone of U.S. Defense," DOD News (April 30, 2021). https://www.defense.gov/News/News-Stories/Article/Article/2592149/defense-secretary-says-integrated-deterrence-is-cornerstone-of-us-defense/. Accessed November 24, 2021.

Where We Are Going: the IDC Vision

These are ambitious goals, but they are what is necessary to meet this moment. Successfully deterring our adversaries in the 21st century requires several things: preeminent deployed capabilities, effective integration of operations across domains, coordinated strategic messaging, a rapid and continuous innovation cycle, and enhanced competitiveness, especially in the development and military application of emerging and disruptive technologies.

What can Livermore bring to this project? More broadly, what can the NNSA national laboratories contribute? What are their differentiating capabilities? IDC requires a wide array of capabilities and expertise—building blocks if you will—that will enable a new approach to this strategic competition. The national laboratories house many of these building blocks and are well positioned to build partnerships with stakeholders in government, academia, and the private sector to create a comprehensive approach. When combined for a common purpose, these building blocks can make a unique and formidable contribution to IDC objectives.

Building Block #1: The Foundational Role of Nuclear Weapons Expertise

As the United States seeks to integrate a multi-domain perspective into its deterrence strategies, it must begin with a solid grasp of the existing fundamentals of deterrence. This means beginning with the foundational role of nuclear weapons in deterrence strategy. Nuclear weapons expertise is the first building block—one for which the labs have no peers.

Since their inception, the NNSA labs have designed, developed, sustained, and modernized the nation's nuclear weapons across the traditional military triad of air, land, and sea platforms. This requires deep expertise in nuclear weapons design and engineering and the underpinning S&T disciplines. It is built on world-class technical expertise in unique disciplines. These include high-energy density science (the study of the most extreme states of matter in the universe), actinide materials science (critical to understanding the performance and longevity of nuclear materials), chemistry (designing, synthesizing, and predicting the performance of energetic materials), and nuclear and isotopic science (key to understanding nuclear weapon performance and effects). It also requires world-class capabilities in advanced technology areas including lasers and optical science (to develop advanced experimental facilities and diagnostic tools); advanced materials and manufacturing (to translate design concepts into manufacturable, robust, and long-lived weapons); and high-performance computing, simulation, and data science (the tool that enables integration of understanding and new and legacy data to create predictive models of nuclear weapon performance). A range of scientific facilities and capabilities are also required to enable this work. At LLNL, the National Ignition Facility—the world's largest and most energetic laser system—creates the extreme temperatures and pressures required to explore the regimes accessed by nuclear weapons in the absence of underground nuclear testing. In 2023 the first exascale computing platform dedicated

to national security, El Capitan, will come online, greatly expanding our ability to simulate and predict the complex physical behavior of matter under the extreme conditions associated with nuclear detonations.

In addition to significant scientific capabilities and expertise in specialized areas, the NNSA labs have close ties to the operational planning of the U.S. military to ensure the weapons meet requirements in relevant military scenarios. LLNL also provides detailed modeling and simulation of operational engagement scenarios, along with technical studies of critical operational issues such as the ability of U.S. missiles to penetrate adversary missile defense systems. As part of this enduring mission the laboratories have stewarded this capability through a long period of national strategic atrophy and loss of focus on nuclear deterrence.

In sum, the labs bring a foundational understanding of the nuclear "domain" to the emerging discussion of multi-domain deterrence as well as knowledge of both strategic conflict and the strategies of the United States for deterring such conflict (and, if necessary, prevailing in war). This robust foundation is essential to the further development and integration of military strategies and applications across the new domains.

Building Block #2: Deep Knowledge of Conventional Defense Technologies

Evolving deterrence strategy beyond the nuclear domain requires an understanding of the potential role of non-nuclear capabilities in that strategy, to include conventional strike capabilities and ballistic missile defense. Here too the labs have deep and unique domain knowledge and design expertise.

The labs have long experience in the design and development of conventional weapon systems that have served the nation in a variety of ways, from pathfinders and prototypes to deployed military capability. An exemplar at LLNL is the BLU-129/B 500-pound bomb, a conventional munition. In partnership with the U.S. Air Force, the Lab designed and fielded this munition in 18 months in response to a Joint Urgent Operational Need calling for enhanced lethality on targets while providing highly circumscribed effects that protect nearby noncombatants and friendly forces. Novel high explosive formulations, specialized testing capabilities at the LLNL High Explosive Applications Facility (HEAF) and our remote Site 300, and extensive use of advanced modeling and simulation to speed the innovation cycle enabled this accomplishment.

Similarly in missile defense, LLNL has been engaged for decades in support of counter-missile protection. A current high priority is exploring options that will enable the use of directed energy for this purpose. The highly synergistic nature of this broader application space provides opportunities to stretch our capabilities and our people, greatly enhancing the benefits to both the nuclear and conventional missions.

Building Block #3: Domain Expertise in Space and Cyber

For much of the last decade, pursuing cross-domain deterrence was largely about incorporating cyberspace and outer space into existing deterrence strategy

and moving toward integrated planning for multi-domain operations. Looking to the future, further integration will require both improved lines of authority in DOD and an enhanced focus on operational resilience and lethality.

The national labs have many decades of experience with satellite systems, starting with the space segment of the global nuclear detonation detection system. Over the last decade, a body of new laboratory work on space and counter-space capabilities has taken shape. For example, LLNL has worked with the National Aeronautics and Space Administration (NASA) on nanosatellites, or CubeSats, which can be deployed quickly and add to the resilience of our space infrastructure. This work also significantly leverages our capabilities in advanced sensors and optics, again enhancing capabilities needed to support the nuclear stockpile. In a recent article in *Foreign Affairs*, LLNL policy researchers argue that a global satellite noninterference treaty might be the best chance for saving the collapsing arms control regime.[180]

Over the last decade at LLNL, a body of new work on cyberspace has also taken shape. The Lab's expertise in cyber covers a wide range of applications, from the defense-in-depth tools and expertise developed to protect our own systems and networks from attack, to world-class modeling and simulation tools used to investigate cyber vulnerabilities, to offensive persistent engagement tools, and most importantly to cyber resilience strategies for complex systems such as the U.S. electric grid and the nuclear command and control system.

Building Block #4: Biological and Chemical Weapons Expertise

A comprehensive view of the multi-domain threat space must give some attention to the threats emanating from chemical and biological warfare (CBW) agents and the traditional and potentially non-traditional applications. The erosion of the anti-CBW norm over the last decade is especially troubling. Here too, the national labs have some unique national capabilities for detection, defense, forensics, resilience, and attribution.

The Forensic Science Center at LLNL, one of only two labs in the United States certified by the Organization for the Prohibition of Chemical Weapons (OPCW), provides technical support for verifying compliance with the Chemical Weapons Convention. The Lab's biosciences and bioengineering research laboratories and experts have decades of experience in biosecurity ranging from the assessment of threats to novel detection systems to the development of countermeasures and therapeutics. The national laboratories contributed extensively to the response to the COVID-19 pandemic, from artificial intelligence (AI)-enabled predictive modeling of potential vaccines and treatments, to the design and prototype of portable ventilators. Today our biosecurity mission focus area is aimed at creating a quantum leap forward in our resilience to future pandemics, either natural or manmade.

180 Michael Markey, Jonathan Pearl, and Benjamin Bahney, "How Satellites Can Save Arms Control," *Foreign Affairs* (August 5, 2020). https://www.foreignaffairs.com/articles/asia/2020-08-05/how-satellites-can-save-arms-control. Accessed November 24, 2021.

Building Block #5: Intelligence-based Adversary Assessments

One of the new concepts in the emerging deterrence debate is "think Red." That is, the United States needs to better understand what its adversaries have learned from going to school on the American way of war as well as their strategies for conflict and confrontation below the lethal threshold. It also needs to understand what new capabilities Red is seeking as a result of its learning and what their deployment implies for future Red behaviors. Toward these ends, IDC strategy requires a superior understanding of the adversary.

Here too the national labs have superior capability and capacity—and few peers. Long-standing and highly classified programs at the labs are used to characterize and assess the relevant capabilities of our adversaries, including both peer nation states and rogue actors. Historically, these programs have been focused on characterizing adversary nuclear capabilities as well as assessing the performance characteristics of traditional adversary means for challenging the effectiveness of the U.S. nuclear deterrent, including air and missile defense systems, mobile launchers, as well as hardened and deeply buried military systems. Today LLNL also performs intelligence-based assessments of the cyber and space assets and capabilities of our adversaries. LLNL is also helping our national leaders improve their understanding of the evolving military doctrines and strategies of our adversaries, including their approaches to integrated deterrence and operations.

Building Block #6: Frontier Research on Emerging and Disruptive Technologies (EDTs)

Any project to "think Red" will quickly focus on the progress of U.S. adversaries in developing disruptive military applications of emerging technologies. In turn, any U.S. response must achieve the same, while also seeking common ground to reduce the unwanted risks and dangers of competition wherever possible.

In recent years, as EDTs have become a top concern of U.S. national leaders, LLNL has responded with new programmatic activity. It has used Laboratory Directed Research and Development (LDRD) resources more strategically and worked with sponsors to advance its research in key areas of strategic competition with our adversaries.

Failure of the United States to lead in these areas of emerging and disruptive technology present potentially dire consequences. To both prevent technology surprise by our adversaries and provide the opportunity to create strategic surprise and advantage for the United States, we need to ensure that our research is on the cutting edge of this arena. AI and machine learning, quantum computing, directed energy, and advanced manufacturing are some of the key areas to which LLNL brings highly sophisticated and differentiated capabilities to bear at the frontiers of science.

Building Block #7: Arms Control and Nonproliferation

Any strategy for long-term deterrence and competition must include a component aimed at stabilizing deterrence relationships through political understandings and

reducing risks where shared interests and perceptions make that possible. Such measures require a sound understanding of those deterrence relationships, the dynamics within them, and the political and technical verification tools that might be applied when pursuing stabilization and risk reduction goals. Here too, the national labs have deep knowledge, many decades of experience, and few peers.

The nuclear design expertise at the NNSA labs has supported national leaders for decades in developing treaties and agreements. It has also provided the necessary technical means for monitoring and verification. As the global security environment grows more complex and challenging, new techniques and approaches will be critical to developing the next generation of arms control and nonproliferation regimes. Furthermore, scientific engagement with adversaries and allies alike can help advance these goals and provide essential confidence-building opportunities.

Building Block #8: Strong Partnerships with Academia and the Private Sector

The 2017 U.S. National Defense Strategy rightly argued that any successful long-term strategy to out-compete other major powers requires us to out-think and out-innovate them, both of which require the ability to out-partner. The United States has many natural strengths in this regard—strong alliances, a vibrant private sector with exceptional technical capabilities and capacities, and academic institutions that are drivers. Here too the national labs have something important to contribute.

The national labs are well situated to create partnerships across the larger research and development (R&D) ecosystems. They operate in a space bridging academia and industry, with their multidisciplinary applied science focus and long-term commitment to addressing significant challenges. Numerous mechanisms encourage and facilitate partnerships at many levels, from technical collaborations between researchers to higher-level memorandums of agreement and strategic cooperation across institutions. Extensive collaborations with academia ensure that the labs have access to the best thinking across the broadest range of ideas and remain firmly on the cutting edge, while also building the pipeline of future national security researchers. Relationships with industry are often motivated by the imperative of transferring technology from the labs to the private sector. However, they also give us opportunities to understand and leverage research investments the private sector is making in dual-use technologies such as additive manufacturing, computing, sensors, and diagnostics. This is especially important today as the high-technology private sector is often ahead of government-funded research in key areas. LLNL's unique physical proximity to Silicon Valley, world-class research universities, and other national labs give us a distinct competitive edge in this regard.

Building Block #9: Extensive Analytical Tools and Methods

True multi-domain integration requires much more than bringing together insight into individual domains. It also requires an understanding of the ways in which these domains are interdependent and how military actions in them impact U.S. interests

in peacetime, crisis, and war. It requires the capacity to perform a net assessment of the ways in which portfolios of capabilities balanced differently for each specific purpose can support and advance U.S. objectives over time. Toward these ends, IDC needs some analytical "connective tissue"—analytical tools that can systematically explore and resolve multi-domain challenges. For example, these include technical war gaming, strategic net assessments, and advanced systems analysis.

In these and related areas, LLNL has a solid foundation of expertise and experience. Particularly in the area of modeling and simulation, it is creating pathbreaking new capabilities in AI and decision superiority with the advent of exascale computing.

Building Block #10: Policy Expertise

While the Labs do not make policy, they are often called upon to provide sound technical perspectives to the policymaking and policy implementation processes. Furthermore, they cannot be effective in their mission space without understanding what policymakers seek to accomplish and the role of "best military advice" in helping to shape the policy process. As policy and military leaders have sought to understand the new challenges of modern strategic warfare and the long-term requirements of deterrence and competition, they have turned to LLNL for just such inputs. Here again the national labs have unique assets.

Chief among these assets at LLNL is the Center for Global Security Research (CGSR). A center of excellence on deterrence, assurance, and strategic stability, it has been focused on the problems of integrated strategic deterrence and long-term competition as two of its five areas of concentration since 2015. CGSR has provided significant thought leadership on these issues and is well known to anyone in the U.S. defense community working on these issues. It benefits from its ability to convene leading thinkers from government, academia, think tanks, and elsewhere, bringing them alongside laboratory technical experts to probe topics at the intersection of S&T and policy. In turn, LLNL researchers are given a much greater appreciation of the context for their work and the perspectives of policymakers who shape government priorities. CGSR's impact is felt across the Lab, as its programs and activities reach into every major program and mission area.

Building Block #11: Independence, Objectivity, and National Service

Delivering analytical insights and technical capability to government entities can only be done by "trusted agents." Given the profusion of IDC-relevant policy analyses by advocacy organizations of many different stripes, such trusted agents can have a particular influence at this time. But that reputation is borne of a track record of consistently delivering independent and objective analysis. Here again, the national labs have something valuable to contribute.

As FFRDCs, the labs maintain a strong focus on providing technical advice and assessments that are independent and objective. The national labs were

created to work in long-term partnership with the government to steward essential capabilities that serve the national need. This has uniquely positioned the labs to act as integrators. Along with convening diverse communities of public and private stakeholders, they use their unique role and knowledge to serve as honest brokers of diverse views and interests on topics within their mission space. Due to these long-term relationships, FFRDCs develop deep familiarity with the needs of government stakeholders and ensure continuity of programs, which helps to ensure success in attracting and retaining highly qualified personnel. This accumulated set of expertise and capabilities ensures that the government can rely on the laboratories for quick response capabilities in times of crisis.

Building Block #12: A Workforce with Unique Skills and Long-term Commitment

This last point is also perhaps the most obvious: If this block is missing, none of the other building blocks can make an impact. Excellent people make all the difference. LLNL has just such an exceptional workforce, deeply committed to translating innovation into impact. To date, the Lab has been very successful in attracting and retaining well-trained individuals who are highly motivated to support national security in these new mission focus areas.

From Building Blocks to Integrated Solutions

Having settled on IDC as a new mission focus area in summer 2021, LLNL leadership has only just turned to putting this vision into practice. As of autumn 2021, we are developing a five-year plan to "up our game," shifting from a central focus on developing domain-specific capabilities to working to understand the interdependencies and interplay between and across domains. This will require a multi-faceted approach including development of an analytical framework encompassing relevant domains, analysis of select scenarios that present challenging IDC problems, modernizing our analytical tools to identify and assess strategies to achieve advantage, and advancing our research into emerging and disruptive technologies and their potential applications.

We find ourselves highly motivated by this vision. There is an urgent need to adapt our national strategies and posture to the requirements of long-term competition and deterrence in a security environment that is much more dangerous than before, with technologies advancing at a breakneck pace—and where the risks of catastrophic multi-domain conflict are real. Accepting this reality, a fresh assessment of what we bring to these new challenges leaves us encouraged. We have the building blocks we need to tackle the problems in front of us—to strengthen deterrence, improve competitiveness, and enhance American strategic advantage. And we have no time to lose.

Conclusions and Lessons Learned

Brad Roberts

This effort to take stock of the multi-domain deterrence enterprise began with a set of questions, elaborated in the introduction, about the progress of the United States and allied defense community in coming to terms—conceptually and otherwise—with the challenges of multi-domain deterrence. It also posed some basic questions about the metrics by which we should judge our progress. The intervening chapters have offered different perspectives on the challenge, our progress, and metrics. This closing chapter sets out the main lessons I have drawn from the effort to take stock.

First, the policy context has changed but the basic challenge has not. When CGSR began its exploration of integrated strategic deterrence in 2014, DOD's focus was on understanding the characteristics of cyberspace and outer space as military domains and on how exploring how cross-domain deterrence strategies might compensate for vulnerabilities in one domain with strengths in another. DOD's focus then shifted to multi-domain operations and how to achieve deterrence benefits by simultaneously orchestrating effects in multiple domains. The Biden administration has again shifted the focus—this time onto the requirements of integrating deterrence effects across multiple domains as one dimension of an integrated deterrence strategy. Despite this shifting policy focus, the underlying challenge is enduring: adapting our concepts and approaches to account for the more multi-domain character of modern warfare and for cyberspace and outer space in our military strategies.

Second, cyberspace and outer space both have something valuable to contribute to U.S. efforts to shape the adversary's decision calculus—that is, the calculus of the benefits, costs, and risks of alternative courses of action. In each domain, it is possible to impose new costs on the adversary. It is also possible in each domain to reduce the expected benefits of attack with defensive measures that enhance resilience. The combined effect of such measures may contribute to an erosion of the adversary's confidence in its ability to calibrate and accept the risks of confrontation. A particular value of these domains for these purposes is the low attendant "audience costs" of compellance; that is, as most actions in these domains to coerce an adversary are largely invisible to the public, the adversary need not lose face when choosing to turn away from confrontation.

Third, these values also come with some challenges. Deterrence requires that an adversary have some understanding of the capabilities that an opponent could use in war to impose costs. However, the peacetime display of U.S. capabilities in cyberspace and outer space could potentially compromise their effectiveness in crisis and war. Thus, adversaries may form a misplaced faith in their ability to gain decisive advantage with such means—which could greatly increase the risk of escalatory

behavior early in a crisis that destabilizes the confrontation and drives it in directions neither side intended. Moreover, the exploitation of cyberspace and outer space in crisis and war could add greatly to the fog of war at the strategic level, complicating the already difficult business of sending clear and specific messages of resolve and restraint as a way to shape the adversary's decision calculus. Political leaders may also be reluctant to embrace such tools in crisis and war, judging them more risky than other means, given uncertainties about the possible effects of use and the lack of historical experience.

Fourth, in considering the possible contributions of multi-domain capabilities to deterrence, it is necessary to be mindful of the twin meanings of deterrence. One is a narrow meaning and focuses on the effort to shape an intention that has formed (as above, the intention to step onto the road to war with the United States and its allies). This definition relates to the willingness of adversaries to enter into crises with the United States in the first place. The other is broader and also encompasses (1) restoring deterrence if it has failed, (2) setting the conditions for termination of the war on political terms acceptable to the United States, and (3) guiding the national approach to long-term strategic competition. The multi-domain character of modern strategic conflict poses challenges across the full spectrum of the concept introduced in the 2018 National Defense Strategy to "compete, deter, and win."[181] For these broader purposes, the contributions of cyberspace and outer space are less clear. They may be helpful in restoring deterrence if it has failed, especially if a campaign focused on revealing a few concealed capabilities shakes an adversary's risk calculus; on the other hand, the capacity to engage in extended campaigns in either domain is limited. As a means of disincentivizing cyber or space attacks below the lethal threshold, the threat of offensive action in either domain is not robust. For dealing with attacks below the lethal threshold, deterrence is not a particularly useful organizing concept. Hence, "persistent engagement" is being used as a way to align defensive and offensive activities with U.S. strategy objectives.

Fifth, competition with Russia and China for the disruptive benefits of dominance in these new military domains introduces significant new risks. The central risk is that leaders will perceive a use-or-lose circumstance at the brink of war, while tempted to try to exploit what they might misperceive as decisive advantages through early use. These risks would not be reduced by a U.S. decision not to compete, as such a decision would likely reinforce perceptions in Russia and China of first-mover advantage. Risk reduction needs to be achieved through improved political relations and efforts to reduce or eliminate military flashpoints.

Sixth, Russia and China have well-developed strategies for competing for strategic advantage in cyberspace and outer space. Having first set out new strategies and concepts, they then turned to capability development and to exercising all three.

181 Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (2018). https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf. Accessed November 24, 2021.

These countries also reorganized to promote multi-domain integration as central to their broader military reform efforts. In their centralized planning and operational constructs, integration is readily achieved—unlike in the U.S. system, where such responsibilities are diffused.

Seventh, effectively integrating multi-domain capabilities requires a clear statement of the new military problem. That problem follows from the more multipolar security environment and the revisionist ambitions of leaders in Moscow and Beijing opposed to U.S.-backed regional security orders, the erosion of the conventional military balance in both Europe and the Indo-Pacific, and the competition for military applications of emerging and potentially disruptive technologies. The problem is multi-dimensional. In crisis and war, the United States must be able to deter and, if necessary, defeat a nuclear-armed near-peer in a regional conflict over limited objectives without generating catastrophic multi-domain escalation—while also disincentivizing opportunistic aggression by the other near-peer and assuring U.S. allies worldwide. In circumstances short of war, the United States must be able to prevail in sub-lethal conflict and win at information confrontation—while also out-competing adversaries in setting the conditions for success in future war.

Eighth, effective multi-domain integration requires a clear statement of integrated deterrence strategy. Our preferred definition: integrated deterrence is a strategy for coherently using all instruments of national power in peacetime, crisis, and war in order to deter adversaries, assure allies, and protect strategic stability. It is not a substitute for all of the many things that have to be done well to meet the new military problem. For sublethal conflict, integrated deterrence involves the coherent use of all of the instruments of national and allied power (military, diplomatic, economic, and informational) to deny the adversary confidence in its ability to reset the geopolitical and military competition over regional order on favorable terms.

Ninth, further progress in multi-domain integration requires a clear statement of objectives. These should include:

- Continuing the process of adapting deterrence to the changing geopolitical and technical context
- Strengthening deterrence by reaping synergies wherever possible among the different means of deterrence and by covering gaps where necessary
- Reassuring allies that their revisionist major power neighbors will not succeed in their ambition to remake regional orders and that the United States has the will and capability to honor its commitment to their security
- Ensuring that the role of nuclear weapons in U.S. defense strategy is rightly tailored—that is, that the United States does not rely on nuclear means for circumstances in which the threat to employ them is not necessary and credible and also does not rely on non-nuclear means for circumstances in which the threat to employ its nuclear means is both necessary and credible

- Developing a theory of victory in modern war that addresses its multi-domain, multidimensional, and transregional characteristics in a sound, effective manner

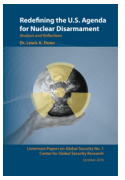
Tenth, new U.S. capabilities in cyberspace and outer space are useful supplements to nuclear weapons in the deterrence toolkit, but they cannot replace nuclear weapons. Their contributions to deterrence are potentially significant but are qualitatively different from the contributions of nuclear weapons. Cyberspace and outer space hold promise as significant deterrents because these are domains where the United States can credibly threaten to upon costs asymmetrically, assuming that its own postures here have the necessary resilience. The qualitative difference stems from the fact that no non-nuclear capability holds out the possibility of consequences that are both devastating and immediate in the way that nuclear weapons do.

Eleventh, the basis for comparing the progress of the United States and its allies to the progress of Russia and China in coming to terms with the multi-domain challenge is not well established. Some analysts take a domain-centric approach, comparing fielded capabilities. Others take a broader net assessment approach, comparing the development of capabilities, military thought, and organization. U.S. understanding of the competitiveness of its multi-domain posture is constrained by many factors, including the secrecy governing the new domains, the inherent complexity of the multi-domain challenge, a net assessment methodology underdeveloped for this purpose, confidence in the ability to improvise in crisis and dominate in war, the absence of a plausible theory of victory in modern strategic war, and a lack of understanding of the theories of victory of U.S. adversaries.

Twelfth, the 2021 National Defense Strategy can be expected to lay down some important new markers in this story. Seen in retrospect five or 10 years hence, its value will likely be judged on the additional work it sets in motion so that U.S. progress in coming to terms with multi-domain challenges continues to accelerate and becomes better informed by a sound understanding of context and metrics.

CGSR Publications

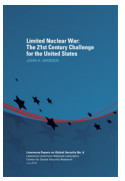
Livermore Papers on Global Security



#1 Lewis A. Dunn
Redefining the U.S. Agenda for Nuclear Disarmament (2016)

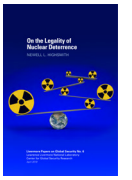
#2 Yukio Satoh
U.S. Extended Deterrence and Japan's Security (2017)

#3 Dave Johnson
Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds (2018)



#4 John K. Warden
Limited Nuclear War: The 21st Century Challenge for the United States (2018)

#5 Michael Nacht, Sarah Laderman, and Julie Beeston
Strategic Competition in China-U.S. Relations (2018)



#6 Newell L. Highsmith
On the Legality of Nuclear Deterrence (2019)

#7 Brad Roberts
On Theories of Victory, Red and Blue (2020)

#8 Toby Dalton & George Perkovich
Thinking the Other Unthinkable: Disarmament in North Korea and Beyond (2020)

#9 Michael Albertson
Negotiating Putin's Russia: Lessons Learned from a Lost Decade of Bilateral Arms Control (2021)

Publications available for download at cgsr.llnl.gov

CGSR Publications

Occasional Papers

Jacek Durkalec
The 2018 U.S. Nuclear Posture Review, NATO's Brussels Summit and Beyond (2018)

Zachary S. Davis
Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise (2019)

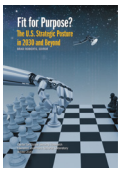
Mona Dreicer, Editor
Getting Innovation Right (2019)

Bruce T. Goodwin
Additive Manufacturing and Nuclear Security: Calibrating Rewards and Risks (2019)

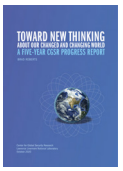
Benjamin Bahney, Editor
Space Strategy at a Crossroads: Opportunities and Challenges for 21st Century Competition (2020)

Brad Roberts, Editor
Major Power Rivalry and Nuclear Risk Reduction: Perspectives from Russia, China, and the United States (2020)

Anna Péczeli and Bruce Goodwin
Technical Issues in the Comprehensive Nuclear Test Ban Treaty (CTBT) Ratification Debate: A 20-Year Retrospective (2020)



Brad Roberts
Fit for Purpose? The U.S. Strategic Posture in 2030 and Beyond (2020)



Brad Roberts
Toward New Thinking About Our Changed and Changing World: A Five-Year CGSR Progress Report (2020)

Brad Roberts
Taking Stock: U.S.–China Track 1.5 Nuclear Dialogue (2020)

Amelia Morgan and Anna Péczeli
Europe's Evolving Deterrence Discourse (2021)

Bruce T. Goodwin
Nuclear Weapons Technology 101 for Policy Wonks (2021)

Publications available for download at cgsr.llnl.gov

Center for Global Security Research

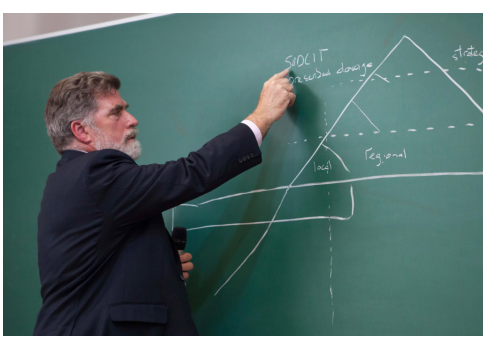
The Center for Global Security Research (CGSR) was established at Lawrence Livermore National Laboratory (LLNL) in 1996 to serve as a bridge between the science, technology, and national security policy communities. It focuses on emerging national security challenges in the areas of deterrence, assurance, and strategic stability.

CGSR's Objectives

- To explore the dynamics of potential 21st century strategic conflicts (i.e., those with a potential nuclear aspect) and to formulate ideas about how to achieve U.S. deterrence and other objectives in such conflicts.

- To explore the sources and characteristics of strategic competition in the emerging security environment and to formulate organizing concepts to enhance the competitive position of the United States and its allies and partners over the long term.

- To identify whether and how technically-based approaches can address new challenges to national and international security.



- To catalyze broader national and international thinking about the requirements of effective deterrence, assurance, and strategic stability in a changed and changing security environment.

- To assist in the development of new generations of experts motivated by a clear view of the changed and changing security environment.

CGSR's Approach

The center has three main lines of effort.

- **Listen and Learn:** the Center convenes seminars with outside speakers to better understand national policy priorities and national and international developments bearing on the lab's missions.
- **Support:** the Center provides analysis and expertise to laboratory leadership in support of strategic planning and to national leadership in policy development and implementation.
- **Intellectual Leadership:** the Center convenes workshops, commissions research, and generates publications aimed at advancing thinking about contemporary and emerging national security challenges related to strategic conflict.

The Center's work is conducted on an entirely unclassified basis. It is also multidisciplinary and entirely nonpartisan in character.

The Center has strong partnerships with many other organizations in the United States and abroad. These help to ensure that its work is informed by a diversity of perspectives and interests. In 2016, CGSR inaugurated a monograph series, the Livermore Papers on Global Security. The series is designed to provide in-depth analysis of major emerging challenges in the security environment and their implications.

“Livermore’s Center for Global Security Research has been a pathbreaker in the development of new thinking about emerging strategic problems. One of the most difficult new problems is the multi-domain complexity of potential future conflicts that spill over into cyberspace and outer space, while also having a profound nuclear dimension. This timely volume provides important new insights into this problem of complexity and the necessary responses from the United States at a time of rising national leadership attention to the requirements of integrated deterrence. In doing so, it addresses a core strategic problem of the 21st century: how to deter, fight, and win limited high intensity theater conflicts against nuclear-armed adversaries without catastrophic escalation that poses an existential threat to the U.S. homeland.”

Gregory J. Weaver
Deputy Director for Strategic Stability
Strategic Plans and Policy Directorate
The Joint Staff

Lawrence Livermore National Laboratory

ISBN-978-1-952565-12-0