Cross-Domain Deterrence

Strategy in an Era of Complexity

EDITED BY JON R. LINDSAY
and
ERIK GARTZKE

OXFORD
UNIVERSITY PRESS

CONTENTS

4

Simplicity and Complexity in the Nth Nuclear Era

RON LEHMAN

Because separate expert organizations with distinct cultures inform nuclear, cyber, space, and other special operations, perspectives often differ on strategy, capabilities, threats, and priorities. Thus, a comparative approach can provide interesting insights, analogies, and lessons learned, highlighting relative strengths and weaknesses. When confronted with the most challenging scenarios, however, an important defense policy goal is synergism between cross-domain and nuclear deterrence—a total deterrent greater than the sum of the parts. Unfortunately, new capabilities, notably in cyberspace and space, could instead undermine deterrence by adding complexity, reducing reaction times, and creating common failure modes, potentially eroding even the nuclear components of deterrence.

In discussions of CDD, imprecise language frequently multiplies the uncertainty. The confusion is built in. The word "domain" has several relevant definitions. It may refer to an area, region, or place, usually demarcated by a particular environment or governance. At the same time, "domain" may denote a "specified sphere of activity or knowledge."[1] Accordingly, "domain" often refers to the places where activities take place, the associated activities themselves, and more. For example, space operations take place in the "space domain" but also in the other domains, such as land, sea, and air. Cyber is especially confusing. In a sense, the entire physical "cyber domain" is located in all the other domains. Nevertheless, the emergent power of "cyber warfare" has prompted wide acceptance today of a formally designated cyber domain. The "electromagnetic spectrum," however, has not been officially delineated

[1] See: "Domain," *Oxford English Dictionary*, accessed 30 January 2018, https://en.oxforddictionaries.com/definition/domain; "Domain," *Merriam-Webster Dictionary*, accessed 30 January 2018, https://www.merriam-webster.com/dictionary/domain.

as a domain, and its overlap with cyberspace is unclear. Yet electromagnetic warfare long preceded "cyber" and still has a profound impact on all the domains.[2]

Nuclear weapons, and to a degree other weapons of mass destruction (WMD), are also historically "multidomain." Where nuclear weapons might explode is of the greatest importance. The over 2,000 recorded nuclear weapon detonations have taken place on the ground, underground, at sea, underwater, in the air, and in outer space.[3] Nuclear weapons also have cross-domain effects. For example, electromagnetic pulse effects from the 1962 Starfish Prime nuclear test in outer space impacted satellites in low-earth orbit, radios on aircraft, and electrical equipment on the ground in distant Hawaii.[4] Again, the distinctly destructive potential of nuclear war, however, has not resulted in the official designation of a "nuclear domain."

Delineation of military domains continues to morph, and where humanity enters a domain, warfare follows. War was initially confined to the land, but greater movement over larger bodies of water inevitably led to the advance of naval warfare. For each of these early domains of warfare—land and sea—strategies were developed, organizations created, and weapons procured—each increasingly tailored to the domain. As illustrated in history from the ancient Greek and Persian wars to modern times, however, each domain impacts the others even when strategy or tactics result in an emphasis on capabilities for one particular domain. Getting the balance right and coordinating operations is a challenge.[5]

The military forces of the United States were managed by two separate departments, War and Navy, until after World War II. The two domains overlapped and interacted, as illustrated by the emergence of an amphibious Marine Corps. Military matters continue to become ever more complex. The portent of new military domains could be seen in the Army Air Corps, the Artillery Branch, and the Signal Corps. Today we speak of land, sea, air, outer space, and cyber as the

[2] See: Mark Pomerleau, "What Would It Take to Declare the Electromagnetic Spectrum a Domain of Warfare?," *C4ISRNET*, 30 November 2016, accessed 30 January 2018, https://www.c4isrnet.com/c2-comms/2016/11/30/what-would-it-take-to-declare-the-electromagnetic-spectrum-a-domain-of-warfare/.

[3] Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organization, "World Overview," *CTBTO.org*, accessed 30 January 2018, https://www.ctbto.org/nuclear-testing/history-of-nuclear-testing/world-overview/.

[4] Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organization, "9 July 1962 'Starfish Prime', Outer Space," *CTBTO.org*, accessed 30 January 2018, https://www.ctbto.org/specials/testing-times/9-july-1962starfish-prime-outer-space.

[5] See, for example, such classics as Herodotus, *The History of Herodotus* [440 BCE], trans. George Rawlinson, http://classics.mit.edu/Herodotus/history.html; Thucydides, *The History of the Peloponnesian War* [431 BCE], trans. Richard Crawley, http://classics.mit.edu/Thucydides/pelopwar.html; Alfred Thayer Mahan, *The Influence of Sea Power upon History, 1660–1783* (1890), http://www.gutenberg.org/ebooks/13529; and H. J. Mackinder, "The Geographical Pivot of History," *Geographical Journal* 23, no. 4 (April 1904): 421–437, https://www.jstor.org/stable/1775498.

fundamental domains of conflict. Some would add unconventional warfare/special operations, undersea, and even underground as military domains. In the future, if warfare develops advanced means to target the internal mental and/or physical state of human combatants or autonomous machines, existing organizations that now focus on psychological/information operations, biosecurity, or artificial intelligence might point the way to designation of additional domains. We might then speak of the "noosphere"[6] or "genomic/proteomic warfare" or a "singularity battlefield" as additional military domains.[7]

Adapting organizations to integrate cross-domain operations continues. From 1879 to 1921, the Departments of State, War, and the Navy were collocated in a single building next to the White House that is now known as the Eisenhower Executive Office Building.[8] For a more complex world, the National Security Act of 1947 created the consolidated Department of Defense with a secretary of defense and the Joint Chiefs of Staff, the Central Intelligence Agency, and the National Security Council to integrate across domains and added the Air Force to give greater attention to a domain made highly strategic by the invention of the atomic bomb.[9] The launch of Sputnik I in 1957 highlighted the fact that outer space would become a vital domain, leading to the Air Force Space Command, then a unified command, and now a proposal for a Space Force as a sixth branch of the armed services.[10] In August 2017 the president ordered creation of a unified U.S. Cyber Command independent of STRATCOM, which became a reality in May 2018.[11] Some of the

[6] Per the *Oxford English Dictionary*, a noosphere is "a postulated sphere or stage of evolutionary development dominated by consciousness, the mind, and interpersonal relationships." See: "Noosphere," *Oxford English Dictionary*, accessed 30 January 2018, https://en.oxforddictionaries.com/definition/noosphere.

[7] Various concepts of a "singularity" invoke the specter that at some time in the future humanity will be overwhelmed and threatened by an exponential advance of technology, particularly if artificial intelligence could comprehend what humans could never comprehend. For a short guide to definitions and the literature, see: "17 Definitions of the Technological Singularity," *Singularity Weblog*, 18 April 2012, accessed 30 January 2018, https://www.singularityweblog.com/17-definitions-of-the-technological-singularity/; Peter Rejcek, "Can Futurists Predict the Singularity?," *SingularityHub*, 31 March 2017, accessed 30 January 2018, https://singularityhub.com/2017/03/31/can-futurists-predict-the-year-of-the-singularity/.

[8] See: Office of the Historian, "State, War, and Navy Building July 1875–April 1947," U.S. Department of State, accessed 30 January 2018, https://history.state.gov/departmenthistory/buildings/section27.

[9] See: Office of the Historian, "National Security Act of 1947," U.S. Department of State, accessed 30 January 2018, https://history.state.gov/milestones/1945-1952/national-security-act.

[10] See: "Chronology," U.S. Air Force Space Command, accessed 30 January 2018, http://www.afspc.af.mil/About-Us/Heritage/chronology/.

[11] See: Jim Garamone and Lisa Ferdinando, "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command," Department of Defense, 18 August 2017, accessed 30 January 2018, https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/.

most important cross-domain questions involve cyber. Are cyberattacks commensurate with kinetic attacks or something different? Can cyber itself be a significant deterrent capability, or is cyber warfare's impact on deterrence primarily through an ability to degrade or enhance traditional deterrent forces? Integrating cyber and space operations continues to be highlighted in the National Security Strategy of the United States.[12]

Integration and optimization of operations across multiple domains remains vital in classic nuclear deterrence, but the emergence of "hybrid warfare" has also moved cross-domain operations to the center of conflicts at lower levels. Hybrid warfare is commonly defined today as the use of unconventional, irregular, or proxy forces supported by cyber and information warfare, often with external sanctuary support for logistics, air defense, and firepower, perhaps also accompanied by threats of vertical or horizontal escalation. This might include, in the case of the Russian Federation, threats of nuclear use at levels of escalation well below what the West would countenance as appropriate. Russian military operations in Ukraine (often described as "frozen conflicts") are the most visible examples of hybrid warfare cited today, but U.S. operations in Afghanistan in 2001 and certain operations by antagonists in the Vietnam War might also be examined as historical variations.

Exploring the theory and practice of classical deterrence provides insight into CDD. At the same time, examining space, cyber, and unconventional warfare across domains such as land, sea, air, or outer space highlights what may persist and what will change in traditional deterrence thinking, including its nuclear dimension. All components of deterrence—nuclear and conventional, offensive and defensive—are more closely linked to space, cyber, and unconventional operations than is widely recognized. All are becoming more salient, interactive, and intense at lower levels of the escalatory ladder. As the United States encounters more potential adversaries who think differently about these matters, all deterrence increases in complexity.

Challenges to deterrence created by diverse military operations across various domains by multiple players should be explored in the context of recent political and technological transformations, the renewed importance of regional deterrence, and an increasing diversity among adversaries and allies. Rapid change suggests a steep learning curve about deterrence under the new conditions. Meanwhile, decades of disinterest in nuclear matters have created a significant "forgetting curve" that is relevant to all deterrence in all domains.

Issues that we would call "cross-domain" predate even the Revolution in Military Affairs, but they seem more leveraging today as we enter yet another nuclear era.

[12] See: "National Security Strategy of the United States of America," White House, December 2017, accessed 30 January 2018, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

The United States is not alone in revisiting the diverse, WMD/cross-domain/hybrid components of deterrence. Facing emerging, often asymmetrical threats, the United States needs innovation in strategy and capabilities to provide its own asymmetrical leverage.

Simplicity and Complexity

Is truth to be found more in simplicity or in complexity? This heuristic question shapes thinking in deterrence strategy just as it does in philosophy, science, public policy, and art. We define an "idea" but struggle with its many forms. We develop explanatory theories but trust them only with confirming data. We paint with a "minimalist" broad brush but explain from a "pointillist" perspective. We pursue uniform laws but then fear unwanted outcomes when particular circumstances change.

Nuclear deterrence also struggles with this simplicity/complexity dichotomy.[13] Doctrines are promulgated through simple ideas—superiority, sufficiency, flexible response, assured destruction, minimum deterrence, countervailing force, reduced reliance. Implementation, however, is more complex. In analytical studies, the implications of these fundamental concepts are tested against complicated simulations, gaming, and "big data" analysis, often looking for the unexpected, such as chaotic effects or emergent behavior. And in political-military operations, concise guidance is actualized through highly diverse forces deployed on land, at sea, through the air, under the oceans, underground, in outer space, and throughout the electromagnetic/cybersphere.

The difficulty of understanding the significance of the "simple" versus the "complex" still beleaguers decisionmaking two millennia after Archilochus of Paros famously said: "the fox knows many things, but the hedgehog knows one big thing."[14]

[13] For a recent compilation of essays exploring broad versus narrow approaches to deterrence theory, see: Elbridge A. Colby and Michael S. Gerson, eds., *Strategic Stability: Contending Interpretations* (Carlisle, PA: U.S. Army War College, 2013). The book cover design is drawn from Kazimir Malevich's *Black Cross*, an early twentieth-century painting in the Russian Museum in St. Petersburg expressing a bold, simple geometric pattern in black and white.

[14] Among those who have built on Archilochus's distinction is Isaiah Berlin, *The Hedgehog and the Fox: An Essay on Tolstoy's View of History*, 2nd. ed. (1953; reprint, Princeton, NJ: Princeton University Press, 2003). Berlin's work is often cited for its discussion of the strengths and weaknesses of hedgehogs and foxes and the potential for merging both. Earlier thinkers, such as Erasmus in 1500, favored the firm principle of the hedgehog; see: Desiderius Erasmus, *The Adages of Erasmus*, ed. William Watson Barker (Toronto: University of Toronto Press, 2001), 87. Others have continued the effort to integrate hedgehog and fox; see, for example, Steven Jay Gould, *The Hedgehog, the Fox, and the Magister's Pox: Mending the Gap between Science and the Humanities* (New York: Harmony Books, 2003). Others favor the fox; see, for example, Philip Tetlock, "Why Foxes Are Better Forecasters Than Hedgehogs," lecture at Long Now Foundation, 26 January 2007, http://longnow.org/seminars/02007/jan/26/why-foxes-are-better-forecasters-than-hedgehogs/.

Even in the twenty-first century, experts invoke "foxes" and "hedgehogs" to anchor nuclear strategy. The hedgehog understands the terrifying power of nuclear weapons. The fox knows that many other important matters may ultimately determine whether nuclear weapons are ever used again. In a world being transformed rapidly by politics and technology and increasingly "cross-domain," should we look more to the fox or to the hedgehog?

Deterrence, like disarmament, leans heavily on one big idea—fear should stimulate restraint. A credible approach to deterrence and arms restraint, however, requires attention to many ideas—different values, alternative priorities, conflicting interests, uneven strengths, unequal vulnerabilities, competing histories, diverse cultures, divergent norms, anomalous psychologies, asymmetrical strategies, and countervailing technologies. Geopolitical and technological changes continuously alter these factors.

We see this complexity expanding in today's discussions of CDD. National security operations using diverse capabilities at different levels of conflict across multiple domains are not new. Nevertheless, interconnected societies, global economies, and even advanced military forces feel increasingly vulnerable to loss of communications, data, transportation, infrastructure, energy, and even lives from attacks that can come in many forms from multiple sources. A common thread in all domains is fear of the destruction, denial, or abuse of information technology for strategic leverage. When defenses against such attacks prove weak, interest in deterrence grows.

Applying lessons from classical nuclear deterrence theory to cyber, space, and other cross-domain operations can be useful, especially if care is taken to consider what is different. Deterrent effects of diverse military capabilities across different domains vary greatly. Few are as stark as WMD, especially nuclear. Greater intellectual insight, however, might actually flow in the other direction, in that analysis of space, cyber, and hybrid warfare might improve our understanding of classical deterrence and its nuclear component. This additional insight might be gained partly by use of analogies but, more important, grows out of understanding how these factors interact. Again, sustaining deterrence while exploring restraint in this more complex nuclear era requires transforming decisionmaking to balance a wider range of considerations.

Changing Circumstances across the Strategic Landscape

In the immediate future, all aspects of deterrence face expanding challenges and complexity, developments that certainly tighten the linkage of nuclear deterrence to space, cyber, and even unconventional warfare. Each of these deserves some elaboration.

The Accelerated Advance and Spread of Latent, Strategic Dual Use Technologies

Advanced simulations, "big data," and artificial intelligence are so powerfully enabling theory and experimentation—the two traditional pillars of science—that experts have difficulty tracking real-world applications. This accelerates the rapid advance and spread of dual use technology, thus complicating deterrence calculations as more states and nonstate actors acquire latent or actualized WMD. Space, cyber, and advanced conventional technology have joined nuclear, chemical, biological, and radiological weapons in posing dangers to societies, economies, and militaries. Given that preventing their spread is problematic, greater emphasis is now being placed on ways to deter or defend against weapons that might result from latent capabilities in untrustworthy hands.

A New Nuclear Normal

At the end of the Cold War, nonproliferation seemed almost a consensus international norm. Wide agreement about nonproliferation was reflected at the first UN Security Council Summit in 1992;[15] and was embodied in the decisions by South Africa, Ukraine, Belarus, and Kazakhstan to give up their nuclear weapons and in the short-lived 1991 North-South Korean Denuclearization Agreement, in which both Seoul and Pyongyang gave up enrichment and reprocessing.

Today, the growing nuclear arsenals of North Korea, India, and Pakistan and the militantly latent nuclear program of Iran—each a different case—will test the impact of nuclear deterrence on stability. This "new normal" impacts other governments or blocs seeking greater security, status, or influence. Most governments will forgo the nuclear option, but many are already looking for other military enhancements with strategic impact, including various cross-domain capabilities. Hackers from Russia, China, North Korea, and Iran have already demonstrated considerable offensive cyber capability. The talent and interest to copy these cross-domain military capabilities exists in many troubled regions. A fresh look at deterrence in South Asia, for example, might help analysts escape perceptual bias, such as stereotyping or mirror imaging left over from the Cold War, not only for classical deterrence but also for cross-domain and hybrid approaches.

[15] On 31 January 1992, speaking as president of the UN Security Council Summit, then British prime minister John Major declared, on behalf of the Summit heads of State and governments: "the proliferation of all weapons of mass destruction constitutes a threat to international peace and security"—traditionally powerful UN language used when strong action, including possible military force, is to be endorsed. See: 1962 John Major, "United Nations: Security Council Summit Statement Concerning the Council's Responsibility in the Maintenance of International Peace and Security," *International Legal Materials* 31, no. 3 (May 1992): 762, http://www.jstor.org/stable/20693700.

Levers for Regime Interests and Survival

In many countries, latent or actualized weapons programs can increase a government's public support at home and political prestige abroad. Iran's latent weapons capability provided leverage in negotiations to remove sanctions and reduce isolation. North Korea has shown how a failing, pariah regime can buy decades of survival by manipulating its transition from latent to actualized nuclear weapons. Ukraine used nuclear weapons in its possession as bargaining chips in part for security assurances under the U.S.-Russia-Ukraine Trilateral Statement of January 1994. Belarus and Kazakhstan had already begun denuclearizing, but both states also insisted on security assurances under the Budapest Memorandum of 1994.[16]

With several former Soviet republics under pressure from a nuclear-armed Russia and with Russian troops occupying Crimea, opinion leaders in several countries are questioning the wisdom of forgoing nuclear options. The fall of Muammar Gaddafi, after Libya gave up its WMD programs, is often contrasted with the resilience of those regimes that have acquired WMD or kept the option near at hand. Indeed, Syria gave up its declared chemical weapons only in a context in which the survival of the regime of Bashar al-Assad might be prolonged. Space, cyber, and unconventional operations might increasingly become important elements of strategies to secure regime objectives. Cyber, in particular, is a tool for domestic control in authoritarian regimes that can readily become an international lever.

A Rising China and a Provocative Russia

Both Russia and China are now more provocative in asserting territory disputed with neighbors. Russia has occupied Crimea, inserted troops into eastern Ukraine, expanded its presence and expectations in the Arctic, and escalated its intervention in Syria. "Oil and gas" diplomacy and an extractive economy reinforce this behavior.

The interests of China and Russia often diverge. Their styles of rhetoric and diplomacy have important differences. Nevertheless, military and geopolitical cooperation between these two nuclear-armed, authoritarian regimes is increasing. Each has important asymmetrical military capabilities, including in space, cyber, and unconventional operations that are of concern to their neighbors, including U.S. allies. They are setting examples of cross-domain/hybrid operations that others might copy.

[16] United Nations General Assembly Security Council, "Letter dated 7 December 1994 from the Permanent Representatives of the Russian Federation, Ukraine, the United Kingdom of Great Britain and Northern Ireland and the United States of America to the United Nations addressed to the Secretary-General," S/1994/1399, 19 December 1994, accessed 15 September 2018, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_1994_1399.pdf

The Backlash against "Western Values"

Renewed interest in nuclear geopolitics among countries in troubled regions coincides with their growing skepticism and even animosity toward Western values as reflected in openness, transparency, market economies, free trade, the rule of law, the sanctity of boundaries, nongovernmental organizations, and human rights. These political developments have important security implications. For example, confidence in military restraint, stability measures, arms reductions, and disarmament is based on norms creating open access and transparent behavior. Instead, these values and norms, associated with verifiable arms control and confidence-building, are increasingly a source of tension between states, especially as authoritarian regimes invoke nationalism and make ethnic or cultural identity a rationale for the control of information and travel.

Both the norms of restraint and the conditions for restraint are weakening. Does this portend more aggressive behavior? Consider, for example, that the pushback against libertarian approaches to the Internet coincides with wider exploitation of cyber operations. As more governments look to these means to deal with terrorism or political opposition, the capacity for cyber warfare will grow and with it the prospect for more cross-domain operations among many states, nonstate entities, and even individuals.

Strategic Effects at Lower Levels of Arms

At lower levels of deterrent forces, small changes in numbers or capabilities might have greater significance. This increases the importance of situational awareness. Many of the technologies that provide the necessary transparency for warning or verification, however, are also associated with cross-domain/multicapability military and intelligence operations and targeting. These can produce further challenges to confidence and stability.

Reductions in nuclear weapons are generally welcomed, but fear of vulnerability at low numbers might make some states providing nuclear umbrellas less willing or able to make credible commitments. This, in turn, could encourage other states to seek their own, independent deterrents through WMD or space, cyber, and unconventional capabilities.

Cross-Domain Asymmetrical Responses

For some governments, nuclear programs are asymmetric responses to deter larger military powers. Interest in cross-domain operations as asymmetrical responses is also growing and coincides with the recognition that advanced conventional munitions, cyberattacks, space warfare, and covert military operations might have strategic, even dramatic impact. This complicates escalation control measures, such

as signaling and demonstrations of restraint, and becomes even more worrisome with the invocation by countries such as Russia and North Korea of nuclear threats in small, regional confrontations.

The fuzzy relationship between cross-domain operations and military escalation creates ambiguous thresholds, perhaps undermining strategic stability. A decision to employ nonkinetic, cross-domain capabilities, such as cyber operations, is easier than a decision to use conventional or nuclear weapons, in part because it might be more legally ambiguous.[17] Cyber operations begun in peacetime, however, might be viewed differently once conflict begins. If the consequences of soft-kill, cross-domain attacks rise, adversaries might respond with kinetic weapons.

More and Different Possibilities

Just as the "N-body problem" in celestial mechanics complicates predictability, so adding more powerful cross-domain capabilities to the quivers of an increasing number of diverse antagonists complicates risk assessment. For example, cyber warfare is not confined to the military. Cyber operations have already empowered state security affiliated organizations, criminal syndicates, and even malicious individuals to threaten harm to the financial and social health of great powers and to their military forces, including potentially early warning and command and control. Similar dependencies and vulnerabilities are increasing with respect to satellites and space operations.

The diversity of those who could exploit these different weapons may also be increasing. The intellectual history of deterrence is, in many ways, a history of logic trees and game theory. Still, a strict and common rationality does not explain all behavior. Differences in culture, personality, and training can alter outcomes. The growing, diverse pool of possible decisionmakers with tools applicable to many domains complicates understanding of what is already complex psychology. The social sciences, like the physical sciences, have developed many techniques to analyze complexity, but few of these have found their way into real-world decisionmaking.

"Learning Curves" and "Forgetting Curves"

During the Cold War, many of the finest military leaders, diplomats, technologists, and academics were steeped in the theory, policy, and operations related to nuclear deterrence, including air and missile defense, antisubmarine warfare, electronic countermeasures, space operations, and covert actions. A vast literature of analysis

[17] John Norton Moore, Guy B. Roberts, and Robert F. Turner, eds., *National Security Law*, 3rd ed. (Durham, NC: Carolina Academic Press, 2015). See especially: Paul Rosenzweig, "Law and Warfare in the Cyber Domain," in *National Security Law & Policy*, 3rd ed., edited by John Norton Moore, Guy B. Roberts, and Robert F. Turner (Durham, North Carolina: Carolina Academic Press, 2015), 537–562.

and lessons learned was produced. With the end of the Cold War, interest and understanding of deterrence declined.

As deterrence again rises in importance, new generations face both "learning curves" and "forgetting curves" as traditional deterrence language morphs into somewhat different meanings. What does "deterrence" mean when the source of an attack is difficult to attribute and may not be a government? What does "warfighting" mean when war is not declared and weapons are not kinetic? What is "unacceptable damage" when cyber "shrinkage" and the cost of prevention involves billions of dollars? How do we understand "escalation" when the next step is a soft, "functional kill" that might, or might not, have devastating secondary effects well into the range associated with kinetic or even nuclear weapons?

Yet Another Nuclear Era

From the perspective of the hedgehog and his one big idea, we live in a single, continuous nuclear age. The nuclear weapons age has a beginning. We do not know how or if it will end. Given widespread nuclear "know-how," we will live under the shadow of this big idea well into the future. From the perspective of the fox, however, with his many ideas, several nuclear ages, or perhaps eras, can be delineated. These eras may be defined by changes in potential adversaries, the military balance, opposing strategies, probabilities of conflict, the weapons involved, and the possible consequences of war. One could, for example, divide the nuclear age into approximate eras this way:

- U.S. Nuclear Monopoly (c. 1945–1949)
- U.S. Nuclear Superiority (c. 1950–1960)
- Bilateral Nuclear Balance (c. 1961–1991)
- U.S. Military Superiority (c. 1992–2008)
- Strategic Regional Complexity (c. 2009–2013)
- Peer and Pariah Asymmetrical Challenges (c. 2014–?)

Each such attempt to delineate different nuclear eras will have flaws, but clearly there has been a significant phase change in nuclear-related geopolitics.

Our world is disappointingly more dangerous now than was anticipated early in the post–Cold War years. The improving missile capabilities of North Korea to strike South Korea are being extended to reach Japan and the United States. The intense centrality of tactical nuclear forces for countries like Russia and Pakistan, especially in smaller, regional contexts, challenges assumptions about what is existential. The evolution of the basic nuclear forces of China, India, and Pakistan toward diversification on land, at sea, and in the air, reopens questions of sufficiency as diversity becomes more important to maintain stability. At the same time, the energetic renewal of Cold War symbols of first strike, such as the large, liquid-fueled, Russian

intercontental ballistic missiles (ICBMs) with large numbers of multiple independently targetable reentry vehicles (MIRVs), which were prohibited in the Strategic Arms Reduction Treaty II, underscores different views of "strategic stability."

Potential adversaries explicitly acquire space, cyberspace, advanced conventional weapons, and "hybrid" capabilities to counter conventional U.S. force projection. The ultimate asymmetrical response, however, is the threat to use nuclear weapons even in those scenarios that the United States has sought to denuclearize. Russia, in particular, sees nuclear weapons as escalatory top cover for its cross-domain and hybrid operations. Both allies and potential adversaries of the United States are watching these developments closely. The interaction of all of these developments may not result in a disastrous "perfect storm," but major storm clouds are appearing that require new risk assessments and an update to U.S. strategic thinking.

Simplifying the Complex in a Cross-Domain Nuclear Age

"Thinking about the unthinkable," as the enterprise of deterrence was described during the Cold War, became unfashionable in the two decades after its end. Thinking deeply about the unthinkable, sadly, has again become a necessity. To help simplify the complex, three subjects deserve a deeper analysis: CDD, varieties of escalation, and the morphing of doctrinal deterrence concepts as the next nuclear age comes to fruition.

Cross-Domain Deterrence as a Priority

In the preface to a recent National Research Council study, the cochairs noted: "*nuclear* deterrence is not synonymous with *strategic* deterrence"; "all Air Force capabilities, including space, cyber, and conventional capabilities play a role in effective deterrence and provide options for decision makers"; "there does appear to be agreement within DoD [Department of Defense] and within the Air Force that *strategic* deterrence is *cross-domain* deterrence"; and there is "an emphasis on how the concept of *tailored* deterrence is evolving, the different mindsets of regional aggressors, controlling escalation in regional crises, the growing importance of missile defenses, and new dynamics for a concept that in the Cold War was called *extended* deterrence."[18]

[18] Gerald F. Perryman, Jr., and Allison Astorino-Courtois, preface to Committee on U.S. Air Force Strategic Deterrence Military Capabilities in the 21st Century Security Environment, Air Force Studies Board, Division on Engineering and Physical Sciences, *U.S. Air Force Strategic Deterrence Analytic Capabilities: An Assessment of Tools, Methods, and Approaches for the 21st Century Security Environment*

This clear statement that nuclear, space, cyber, and conventional capabilities are elements of both CDD and strategic deterrence is not new. Nor is the emphasis on tailoring deterrence to regional settings. What is new is the sense of urgency in dealing with these complex interactions with nuclear deterrence even at lower levels of escalation. Nuclear weapons are meant to be different from other weapons. They scream "Don't Tread on Me!" They delineate "bright-lines" not to be violated at higher levels of conflict,[19] even if they inevitably cast weaker shadows of warning that escalation is dangerous around redlines well below the nuclear threshold.

A clear line between nuclear and conventional strikes has important utility in escalation control—a goal potentially undermined by the emerging, fuzzy cross-domain environment. Space, cyber, and some nonconventional warfare operations might substitute for nuclear and conventional attacks but might be evaluated differently by diverse decisionmakers. This might make signaling more difficult and actions more dangerous.

Comparing, contrasting, and synthesizing these deterrence issues related to nuclear, conventional, unconventional, air and missile defense, electromagnetic, cyber, and space operations is an excellent exercise for promoting new thinking about deterrence in all its dimensions. Consider some of the following classic challenges.

Attribution and Accountability

During the bipolar Cold War, strategists worried that third parties might provoke catalytic war by conducting an anonymous nuclear strike that one superpower might think was perpetrated by the other. Today, space, cyber, and hybrid operations are presenting new difficulties, both technical and political, for attribution and the resulting inability to hold accountable those responsible. More cross-domain players, each with different escalatory dynamics, increase the prospects for such confusion. At lower levels of conflict or crime, this might be tolerable, but sudden, great violence, combined with confusion over responsibility, could result in a dangerously wrong response.

Asymmetrical Responses and Blowback Effects

Blowback against the advantages of one adversary often motivates others to exploit asymmetric responses, such as terrorism, guerrilla warfare, improvised explosives, landmines, and chemical weapons. Russian hybrid warfare, as conducted in Eastern

(Washington, DC: National Research Council, 2014), xii–xiii, https://www.nap.edu/read/18622/chapter/1. The author was a member of the committee.

[19] For the use of "bright-line" rules in jurisprudence to influence behavior, see: "Bright-Line Rule," Legal Information Institute, accessed 30 January 2018, https://www.law.cornell.edu/wex/bright-line_rule.

Europe and the Caucasus, involves an asymmetrical strategy that integrates cyber operations, covert deployments, proxy insurgents, and information warfare but adds threatening nuclear rhetoric. For countries like Russia and Pakistan, tactical nuclear weapons are asymmetrical responses to superior conventional power.

Russian success at cross-domain operations in local settings, including nuclear saber-rattling in the face of strong Western opposition, has not been lost on other countries. Iran, for example, has demonstrated extensive cyber, information, drone, and proxy warfare prowess while it sustains a latent nuclear capability and develops missile and space launch systems. The low cost of entry and different vulnerabilities make cyber operations a powerful equalizer. Low-earth orbit, with so many vital satellites, may yet be another realm where asymmetric dependencies invite asymmetric strategies.

The United States may be said to have its own asymmetrical strategy—one that emphasizes the "soft power" of political, cultural, and economic influence. Its asymmetrical "hard power" preferences have been conventional cruise missiles, no-fly zones, and fast-moving ground units supported by the "shock and awe" of high-technology weapons. For example, U.S. Special Forces deployed in small numbers with the Northern Alliance in Afghanistan conducted a U.S. form of hybrid warfare from horseback, supported by reconnaissance satellites, drones, and B-52 strategic bombers armed with conventional joint direct attack munitions. As more potential state or nonstate adversaries of the United States and its allies turn to space, cyber, information, and hybrid operations, the West will need to explore more asymmetrical options of its own, whether high-tech or otherwise and involving both hard and soft power.

Collateral Damage and Proportionality

United States policy and law requires that any use of force, from nonlethal to nuclear, must be targeted only against legitimate military objectives and proportionate to the military necessity. Civilian casualties and property damage inflicted incidentally to otherwise legal military operations, often termed "collateral damage," might be war crimes if they are excessive under the circumstances.[20]

Recent history suggests a disturbing trend: a greater proportion of civilian to military casualties even in small, local wars, particularly those involving nonstate actors and failed states. This derives primarily from the intense ethnic, religious, and linguistic divides that characterize those wars. Often this involves the explicit use of terror as a tool of influence and of civilians as both shields and

[20] Office of General Counsel of the Department of Defense, *Department of Defense Law of War Manual* (Washington, DC: Department of Defense, June 2015), 393–395, accessed 30 January 2018, http://www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf.

targets—developments increasing the risk of collateral damage when outsiders intervene.

Cross-domain technology plays a role also—in some cases improving the ability to distinguish civilians from combatants but in other cases placing them at risk. Greater urbanization has made populations more vulnerable to loss of power, water, sanitation, and other vital infrastructure. The prospect that space, cyber, and other cross-domain actions could result in great collateral damage by indirect means on urban populations has important implications for both deterrence and the laws of warfare.

Counterforce, Countervalue, Escalation, Deescalation

Cross-domain operations, such as space and cyber, can be aimed at military or industrial targets. These operations, however, face difficulties similar to those that kinetic weapons face in identifying or avoiding civilians. Escalation might make this even more difficult. Cyber warfare, for example, might be able to attack with great precision the control systems—known specifically as supervisory control and data acquisition (SCADA) systems—that manage electrical grids, gas pipelines, communications, water supplies, transportation, and industrial processes. Such nonkinetic attacks might or might not produce immediate casualties yet ultimately could result in massive loss of life. A major disconnect between what was intended and the resulting consequences could easily erase signals meant to show restraint.

Damage Assessment, Certainty, Uncertainty, and Sufficiency

In the kinetic world, both nuclear and conventional, many models exist for approximating expected damage to targets. Plans can then be designed to ensure that critical targets are destroyed and collateral damage reduced. In the actual fog of combat, however, implementation of attack plans and subsequent damage assessment are challenges at all levels of warfare. For example, tanks on a battlefield are often struck many times again after they were originally neutralized and their operators killed because the next forces to encounter them do not recognize that they had already been destroyed.

Nonkinetic cross-domain attacks have many of the same targeting and damage assessment challenges. In particular, "functional kill" can amplify uncertainties about the success of the attack or unintended effects. Likewise, determining requirements for force structures and capabilities is often linked to the confidence cobelligerents have in their estimates of the damage they can inflict or might suffer. Thus, uncertain effects might complicate calculating sufficiency, just as they complicate the psychological dynamics of escalation.

Decision Cycles, Response Times, and the "Fait Accompli"

Fear of the "fait accompli" has long been a preoccupation in deterrence theory. If one side believes that it faces ready and relevant responses, it might be deterred. If that party believes, however, that a delayed response will mean a weak response or none at all, it might strike. Thus, inadequate options, insufficient clarity, and unwieldy decisionmaking are weaknesses in deterrence that could be exacerbated and exploited by an effective cross-domain adversary. Space, cyber, and hybrid warfare can, as in the case of carefully orchestrated kinetic attacks, negate retaliatory capabilities, create uncertainty, and delay decisionmaking by destroying forces, denying communications and analysis, or altering the perceived context for a decision.

Like the "frog in the pot" phenomenon, living with extensive, unattributed cyber operations during a lengthy, preconflict phase could reduce responsiveness if an attack occurs later. Creation of such a mental fog about where on the escalatory ladder things stand could be destabilizing.

Measure/Countermeasure Dynamics and Defenses

In deterrence theory, the relationship of offensive forces to defensive forces in stability calculations is hotly debated. Would a party with confidence in its own missile defense, for example, be more likely to strike first, believing that its defenses would be even more effective against a depleted retaliation? On the other hand would an attacker risk a first strike if the missile defenses of the other side might prevent a disarming first strike or if overcoming those defenses requires such a massive attack that unacceptable countervalue retaliation would be an inevitable consequence?

The offense-defense relationship in strategy is but one example of measure/countermeasure dynamics, a process that is very intense in space, cyber, and other cross-domain endeavors. Significant instabilities seem to be associated with dependence on vulnerable assets without providing diverse and redundant backup. Modern military forces and societies have become dependent on space satellites and other vulnerable interconnected information technology. Deterrence has been the strategy of choice to prevent nation-state attacks on these assets, but the return of outlaw states and the rise of cyber hackers has shown the importance of also developing countermeasures and defenses. The ingenuity of cybercrime, however, illustrates how volatile confidence in countermeasures can be.

More work is needed to understand CDD and its implications for classical deterrence. A larger number of parameters must be considered as the complexity of all deterrence calculations increases due to various factors: linkage to economic and political sanctions, information warfare and propaganda, messaging and the "signal to noise" problem, nonnuclear WMD, "gray area" weapons that are difficult to categorize, and others.

Geometries of Escalation

Exploration of escalation dynamics can illuminate uncertainties in deterrence theory and might offer more integrated perspectives for deterrence decisionmaking in a world in which cross-domain operations interact more intensely with the totality of deterrence, including its nuclear dimensions.

Escalation as a Singularity

Crossing the nuclear threshold means generating a phase change in destructive potential. All calculations expand fundamentally at the point of nuclear use. The danger at this singularity is so great that many believe that a "taboo" militates strongly against the possibility of any "rational" nuclear first use. Fear of an all-or-nothing certainty of destruction is expected to reinforce the nuclear taboo and the logic of disarmament.

Unfortunately, the idea of a shared norm against any and all nuclear use faces real challenges. Nuclear saber-rattling from Pyongyang and Moscow intimidates by implying that these states are prepared to ignore the nuclear taboo in situations in which Western norms would not permit making nuclear threats. These states' rhetorical "nuclear brinksmanship" in contemporary crises suggests that they have some ideas about when actual nuclear use might serve their national interests.

The persistence of real-world nuclear-threat-mongering is a challenge to the single-point, zero-dimensional perspective that asserts that any nuclear use could only be all-or-nothing. Cross-domain operations continue the assault. Fundamentally, the history of space, cyber, and advanced conventional and unconventional warfare demonstrates that such operations are not at all confined to a single decision or circumstance. They escalate and deescalate continuously from the innocuous and preconflict phases all the way to total war, either in support roles or as weapons themselves. The danger is that nonkinetic and unconventional operations might inadvertently constitute an unacceptable escalation leading to major kinetic or even nuclear responses.

Escalation as Linear

The deterrence policies of most nuclear weapons states do not assume that all nuclear use is inevitably out of control. To be seen as "credible" by adversaries, by allies, and in their own minds, nuclear powers want options that can be limited. Traditionally, they speak of an "escalatory ladder," which is a linear, one-dimensional concept. The "ladder" links higher and lower levels of conflict with "rungs" or "steps," suggesting that escalation can be turned up, modulated, paused, even deescalated. Cross-domain operations are relevant to the one-dimensional nuclear escalatory

ladder, both in support of the diverse nuclear forces that are required during movement up or down an escalatory ladder and because such operations themselves are often described as "tunable," opening up more dimensions for escalation response and control. Whether more tools and more data will ease or complicate escalation control remains uncertain, but more cross-domain tools and data are emerging in any case.

Escalation as Planar

In recent years, analysts have increasingly replaced the concept of the nuclear "escalatory ladder" with a cross-domain "escalatory lattice." Such two-dimensional, "planar" concepts reflect a view that cross-domain operations can themselves be powerful weapons, sometimes substituting for nuclear or conventional weapons. Cross-domain options have long been available. The prospect that operations in the space or cyber domains, to some degree, could impact other domains, inflicting high levels of counterforce or countervalue damage, compels consideration of this wider dimension. Escalation is not just from conventional to nuclear or to more of both. What has changed is the perception now that cross-domain operations can have highly leveraging or damaging effects on a scale once associated only with major escalation in kinetic conflict or even with limited nuclear strikes.

Escalation as Cubic

"Cross-domain" strategy also highlights a third dimension, "escalatory depth." Operations around the Earth, through the atmosphere, and in outer space involve allies, friends, and potential adversaries dispersed around the globe. The phrase "horizontal escalation," meaning escalation in a different geographical region, as opposed to "vertical escalation," meaning a higher level of violence, has always underscored the spatial aspects of deterrence. Such geographical strategies are again being seen, in part amplified by the inherent mobility of cross-domain operations. Cyber operations, for example, can move from one area to another quickly or can act globally, constantly keeping one antagonist or another off balance. In the age of modern cross-domain capabilities, confining conflict geographically will be problematic.

Escalation as Temporal

This agility of cross-domain warfare to move great distances reminds us also of yet another important dimension of escalation; namely, the temporal. Different elements of the nuclear triad operate and interact on different timelines. Likewise, cross-domain warfare can be inserted into the middle of timelines for decisionmaking concerning other military deployments. Such timely intervention

provides considerable leverage. Timing gives us a fourth dimension in escalatory calculations, one that becomes even more important because military operations in the electromagnetic/cyber spectrum can take place at the speed of light.

Escalation as Nth-Dimensional

How many dimensions of escalation are there? Many, undoubtedly, but not all are equal or even significant. Where do we draw the line? At least a fifth dimension seems necessary; namely, the role of human variety as reflected in different histories, cultures, and psychologies. We know enough about classical deterrence to suspect that rules-based logic is not sufficient to explain important strategic behavior.

In some ways, cross-domain operations make this human behavioral consideration even more important. The rules and logic of CDD are less well understood and universalized than those of classical nuclear deterrence, making decisions even more complicated by diverse cultures and psychologies. For example, the exploitation of information technology by criminals and terrorists points the way for nation-states both before and after conflict.

The Morphing of Deterrence Language

A major goal of deterrence is war prevention. This is frequently contrasted with warfighting or defense, options for when prevention presumably has failed. The language of deterrence relies heavily on such contrasting frames of reference to evaluate strategies, promulgate guidance, and set force requirements. These concepts, however, may not be so distant from each other. More often, the meanings change with circumstances and relocate along a continuum of possibilities that make them less distinct. The rise of cross-domain capabilities in the context of deterrence may reinforce tendencies for seemingly antagonistic categories in analysis or policy to converge, diverge, or overlap. An examination of key concepts is illuminating.

"Conflict" versus "Crisis"

International law has long recognized that absence of a formal declaration of war does not mean that there is no war. The laws of warfare apply under a wide range of conflicts. Likewise, nation-states find the boundary between preconflict and conflict fuzzy, given the historical use of espionage, agents of influence, propaganda, sanctions, demonstrations of force, and proxies. Cross-domain operations, such as cyber, might lie dormant or be active in this fuzzy region only to blow up into full-scale warfare. Even then, some confusion might exist as to whether a war is under way and how serious it is.

Cross-domain operations and even conventional strikes, however, might not "let slip the dogs of war." Conceivably, an electromagnetic pulse attack might fall in this category. Both the attacker and the attacked in a crisis might not want to escalate. Tactics like hybrid warfare might permit a very hot, simmering condition that avoids flame or an explosion. However, the risk of conflagration under such "nonwar" circumstances can be high, particularly when the adversaries have different thresholds of tolerance and might initiate actions that are misunderstood or have greater consequences than anticipated.

Space, cyber, and hybrid operations run particular risks because their potentially intense cross-domain activities range both well below and well above the fuzzy conceptual and physical boundaries that now define conflict or war. Unlike the demilitarized zone that divides the Korean peninsula, designed to keep major combatants clearly apart, cyber operations can extend the zone of confrontation to great distances inside sovereign boundaries even in times of peace. As long as the antagonists find these provocations tolerable, many acts that might constitute a casus belli might not lead to war. Attitudes can change quickly, however, perhaps triggered by a perceived change in the quality or quantity of cross-domain damage being inflicted or suffered. This volatile subjectivity complicates the managing of stability on the basis of rule-based logic.

"Deterrence" versus "Warfighting"

The contrast between deterrence and warfighting may be more theoretical than practical. For example, some ethicists argue that use of nuclear weapons could never be moral, legal, or rational. Ironically, a number of these same ethicists also argue that nuclear weapons should be retained during dangerous times, but only for their cautionary influence. At the far opposite end of the spectrum from this view was the expectation after World War II that nuclear weapons would routinely replace other weapons for combat use whenever they were more effective or affordable. Neither of these views is that of the U.S. government. For clear policy reasons, the United States long ago mandated that nuclear weaponry should not be regarded or treated as just another, cheaper version of bombs or bullets. If in dire circumstances no acceptable alternative exists, however, nuclear weapons could be used.[21]

A stark conceptual contrast between pure "deterrence" and pure "warfighting" provides a useful shorthand for discussion of policy and strategy. In the physical world, the distinction is less absolute. Indeed, major doubts exist about the wisdom of either policy in its purest form. Strategies of deterrence and of warfighting appear

[21] The view in Moscow, which is defended by nuclear-armed antiballistic missile systems, may be less clear. The Russian military seems interested in retaining nuclear warheads for several types of military missions that the United States has converted to conventional warheads. Part of the rationale seems to be greater cost-effectiveness.

more credible toward the middle of the continuum that runs between the two extremes. Along that continuum, there is considerable overlap. Deterrence is about preventing a war, not fighting one. Yet the credibility of deterrence rests on the prospect that proportionate retaliatory action can and will be taken.

To be proportionate, both in the just war tradition and in the practical military tradition of Clausewitz, such retaliation and any escalation must be purposeful, rational, and measured. Forces maintained for deterrence must impact military capabilities. Thus, for legal and military reasons, deterrence requires something like warfighting. Attempting to limit destruction though escalation control suggests a similar conclusion: nuclear weapons are too dangerous to be used except when absolutely necessary, but to reserve potential use only for massive retribution after all is lost might make that worst outcome more likely.

How do new cross-domain capabilities impact the distinction between "deterrence" and "warfighting"? Given that cyber operations in particular are used every day, one might assume that cross-domain operations would be little more than warfighting, even in circumstances other than war. On the other hand the ability of cyber and space warfare to damage or disrupt nuclear forces and their associated C4ISR,[22] in whatever domain in which forces have been deployed, places cross-domain operations at the heart of deterrence calculations because of the implications for strategic stability. Equally significant is the prospect that cross-domain strikes could inflict significant damage on civil infrastructure, resulting in massive indirect casualties. "Fuzzy deterrence" and "fuzzy warfighting" could become largely indistinguishable, increasing the importance of understanding what damage is being done.

"Countervalue" versus "Counterforce"

If deterrence is thought of as influence through the generation of fear, then which is feared more, destruction or defeat? Undoubtedly the answer depends on how the audience assesses the probabilities of either of these consequences. Still, this simple question defines the public debate between "countervalue" and "counterforce" targeting.

Countervalue targeting, such as strikes on civil infrastructure, is broader than its most extreme, illegal form, which would be deliberate attacks designed to maximize civilian casualties. Likewise, counterforce is broader than its most intuitive focus, defeat of uniformed military formations. Countervalue and counterforce overlap considerably when strikes are aimed at defense industries, communications nodes, power grids, and transportation systems. In theory, for both counterforce and

[22] The acronym C4ISR stands for command, control, communications, computers, intelligence, surveillance, and reconnaissance.

countervalue strategies, as escalation increases, the countervalue destruction grows, as does "collateral damage," such as civilian casualties. Do cross-domain operations follow the same escalatory path? Not necessarily. Several aspects of cross-domain escalation may be nonlinear in consequences and could increase uncertainty and danger.

First, space, cyber, and hybrid attacks might overlap conventional and nuclear weapons in functional effects and collateral damage. Consider, for example, how different cobelligerents might perceive attacks by various means that produce the same massive destruction or disruption to their electrical generation and distribution systems. The analysis of aerial bombing in World War II performed by the United States Strategic Bombing Survey suggested that the destruction of electrical power capacity would have significantly reduced German weapons production and concluded that electrical power was not effectively targeted.[23]

In the early days of the Cold War, experts wondered if a key element of deterrence should be the threat of massive nuclear explosive strikes along the Soviet electrical grid and on power plants. Years later, in 1962, the Starfish Prime nuclear weapons test demonstrated that the electromagnetic pulse from nuclear weapons could damage electrical and electronic systems without such weapons' heat, blast, or ionizing radiation extending near the surface of the Earth.[24]

During Operation Desert Storm, nonnuclear means were found to destroy electrical power generation and distribution through conventional air strikes and even nonexplosive means. In recent years, the Department of Homeland Security has expressed concern that cyber hackers might be able to bring down large segments of the U.S. electrical power grid. More recently, a well-planned sniper attack on a Pacific Gas and Electric transformer station near San Jose, California, reminded everyone that in an age of global terror, advanced societies have vulnerabilities to unconventional forces, insurgencies, criminals, and even inspired "lone wolves."[25] Exploring such common targets of cross-domain threats reminds us that weapons we perceive as very different—nuclear, electromagnetic pulse, conventional, cyber, "little green men"—can have similar functional effects operating across the domains.

Second, if various cobelligerents perceive the degree of escalation associated with these alternative means of warfare differently, then cross-domain escalation

[23] *The United States Strategic Bombing Survey Summary Report (European War)*, (Washington, DC: Government Printing Office, 1945).

[24] Office of the Deputy Assistant Secretary of Defense, "Appendix C: Basic Nuclear Physics and Weapons Effects," *Nuclear Matters Handbook 2016* (Washington, DC: Department of Defense, 2016), accessed 15 September 2018, https://www.acq.osd.mil/ncbdp/nm/NMHB/chapters/Appendix_C.htm.

[25] Matthew L. Wald, "California Power Substation Attacked in 2013 Is Struck Again," *New York Times*, 28 August 2014, accessed 30 January 2018, http://www.nytimes.com/2014/08/29/us/california-power-substation-attacked-in-2013-is-hit-again.html.

might further undermine predictability and stability. For example, consider a simple matrix of cyber, conventional, and nuclear attacks against cyber, conventional, and nuclear targets. One might easily expect a roughly linear progression in escalation logic from cyber-on-cyber attacks through conventional-on-conventional attacks to nuclear-on-nuclear attacks. Yet a cyberattack on cyber assets perceived by one antagonist as restrained might result in damage that another antagonist associates with major kinetic strikes or even electromagnetic pulse or nuclear. This might be worse when what is intended as a limited counterforce measure, such as an attack on electrical power, nevertheless is perceived as a major countervalue escalation because of the consequences for civilians.

Space and cyber operations might not be kinetic, or immediately lethal, yet their counterforce and/or countervalue impacts could be large and significant. Consider, for example, the "Manichaean" dilemma we face in our interconnected, all-seeing world: the once inconceivable "light" shed on everything by our digitally interconnected world could quickly become disastrously "dark." The same microelectronics revolution that permits global sharing of immense data for business, personal, and military applications can also be used to destroy or disrupt the ability to know what is happening and to communicate about it. Perhaps even worse is the advanced capability in the information age to deceive, distort, or mislead. Expectation of nearly total awareness might be comforting. Loss of C4ISR would be very stressing. Being confused might be deadly.

"Homeland Security" versus "Over There"

Extending a "nuclear umbrella" to allies has long been the ultimate sign that the security shared should be considered inseparable—that what happens in foreign lands matters at home. An attack on one is an attack on all. The problem, of course, is that the national security interests of states are no more identical than their economic and political interests are. Deterring an "existential" threat to the homeland might be the most universally agreed-on role for nuclear deterrence. But what is "existential" and whose "homeland"? At what intensity in the conflict should nuclear use be considered? In the nuclear realm, allies may differ on whether the escalatory ladder should be steep or flat. Views may change; states may even switch sides.

Differences among allies over where the nuclear threshold should be located are often managed by ambiguity about thresholds. In the case of cross-domain cyber and space operations, the ambiguity is less in the use than in the effects. Preconflict operations may seem small and local but can easily lead to large or global effects. The regional application of space assets involves exposing global operations to threats based far from the homeland. Similarly, cyber warfare not only blurs the boundary between nonconflict and conflict but also does not always require a regional presence or local logistics to attack. In short, cross-domain operations tend

to link the fortunes of distant regions, even as their actual use might be less controversial among allies. Obviously, extended deterrence will remain a key element as CDD matures. Indeed, threats against the very space and cyber assets that many states vitally depend on might offer strong coupling effects in deterrence terms.

As we transition into a more intensely cross-domain view of deterrence, our concepts will likely morph to reflect further blurring of distinctions. Western policymakers continue to emphasize that nuclear weapons are different from other weapons, but more attention will have to be paid to what we mean and what others mean when they say those words. We will continue to find useful such shorthand as "counterforce," "countervalue," "warfighting," and "extended deterrence," but these will be even less exclusive categories than they are today. As conceptual categories of classical deterrence theory increasingly overlap with their opposites in this new multidisciplinary, cross-domain world, our living language must capture subtle but important changes in the meaning of our words. Yet our age will remain nuclear. And, as before, the nuclear specter does not mean the end of conflict, including wars that could escalate to use of nuclear weapons.

Along the way, Russia and China have demonstrated new asymmetrical and cross-domain capabilities for area denial and escalation dominance. The Russian invasion of Crimea, its hybrid warfare in Eastern Ukraine, and Moscow's invocation of nuclear weapons in smaller, regional crises spotlight the dangers. This new cross-domain/nuclear era will become even more dangerous if other players in troubled regions borrow from the Russian playbook.

Multidisciplinary Perspectives on Deterrence Today

Rethinking deterrence in our new nuclear/cross-domain era is vital. The timing is fortuitous. Multidisciplinary analysis of the complexities of recent developments may actually generate important new thinking. Our topic here, cross-domain and nuclear deterrence and the morphing of strategic concepts, confronts us with a steep "learning curve" even as we are likely to discover that we have been on a sizeable "forgetting curve." Hopefully, new thinkers looking at old data and old thinkers looking at new data can generate the deeper understandings that we now need.

Geopolitically, a quarter of a century after the end of the Cold War, we may feel like the protagonists in the motion picture *The Big Chill*.[26] We have left behind our youth and are discovering that we have not accomplished all that we had hoped. Our sense of vulnerability is great. We are in an age of angst. What do current political and technological changes portend? With deep reductions in nuclear weapons,

[26] *The Big Chill*, directed by Lawrence Kasdan (Columbia Pictures, 1983).

is the "unthinkable" becoming more "thinkable," and to whom? Do others think differently about goals, strategy, values? How can objective logic influence what appears to be highly subjective behavior? Is real deterrence local or global or an interaction of both?

We must be careful not to prejudge the outcomes of a fresh look at deterrence today. Undoubtedly, some fundamental truths will reassert themselves. Not all WMD are alike. Nothing is as comprehensively and instantaneously destructive as the blast, heat, and direct radiation of nuclear weapons. Biological weapons pose another plausible threat of mass destruction. Chemical, conventional, space, and even cyber warfare may nevertheless pose great threats to military operations and civilian lives. Recognition of these potential horrors should cast a shadow of caution. Fear alone, however, has not prevented wars from beginning and escalating.

For the United States, a major challenge to deterrence occurs when escalation takes place at levels well short of an immediate, existential threat to the American homeland. Given an expectation that Washington cares less about the Russian "Near Abroad" than does Moscow, the Kremlin may be sounding the nuclear klaxon in smaller, local conflicts such as Georgia or Ukraine precisely because the Russian leadership believes that Western powers would conclude that their interests do not warrant any nuclear risk. Certainly keeping local conflicts from becoming global or nuclear must be a main focus for the United States, but care must be taken not to create power vacuums into which others gain dangerous leverage for conventional, space, cyber, or unconventional operations precisely by threatening to go nuclear.

A number of hypotheses about contemporary deterrence are warranted. Basic deterrence principles seem enduring, but cross-domain developments such as cyber and space complicate deterrence calculations. This occurs at time when many assumptions about deterrence are already being challenged by changes in weapons, targets, geography, and players. At low nuclear weapons numbers and especially in the context of regional escalation dynamics, not only does the unthinkable require more thinking, but the entanglement and overlap of nuclear and nonnuclear may be very serious.

Like WMD, nonWMD cross-domain activities can be seen as asymmetric responses to the strengths of an adversary. Space, cyber, and unconventional operations blur boundaries such as those between conflict and crisis or between countervalue and countermilitary consequences by confusing attack assessments. Indeed, they may create gaps and creases to be exploited in escalation logic and behavior.

Cross-domain operations have important symbolic and operational linkages to nuclear deterrence. They may play more heavily as the unthinkable becomes more thinkable at lower levels of nuclear arms and with more nuclear and cross-domain antagonists. Intense space, cyber, and hybrid operations are here to stay,

are increasingly "go-to" asymmetrical options for adversaries, allies, and ourselves, and have vital implications for deterrence. Across all domains, the United States should exploit more sophisticated technology, simulations, and gaming in support of analysis, training, planning, and evaluation of tactics, forces, weapons, networks, and systems.

5

Deterrence in and through Cyberspace

JACQUELYN G. SCHNEIDER

"Cyber deterrence" has become a buzzword for U.S. policymakers. Whether it is the use of cyber operations to deter actions within other domains or the deterrence of adversary cyberspace operations within the cyber domain, U.S. policymakers are increasingly concerned with deterrence and cyberspace. The 2015 U.S. Department of Defense (DoD) Cyberspace Strategy advocates a "comprehensive cyber deterrence strategy to deter key state and nonstate actors from conducting cyberattacks against U.S. interests";[1] initiative 10 of the U.S. "Comprehensive National Cybersecurity Initiative" directs the U.S. government to "define and develop enduring deterrence strategies and programs";[2] and the 2017 Executive Order on strengthening cybersecurity calls for "the Nation's strategic options for deterring adversaries."[3] Even the Department of State is preoccupied with deterrence in cyberspace, arguing that norms must be developed "in support of deterrence and de-escalation of cyberattacks."[4] These calls for cyber deterrence also clamor from outside of the executive branch, with increasingly vehement calls for cyber deterrence from Senate leaders and domestic constituencies.[5] Despite the resounding calls win U.S. policy

[1] U.S. Department of Defense, "DoD Cyber Strategy," April 2015, 10, accessed 25 January 2018, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[2] White House, "Comprehensive National Cybersecurity Initiative," 2009, 5, accessed 25 January 2018, https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf.

[3] White House, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," 2017, accessed 25 January 2018, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[4] U.S. State Department, "Final Report of the International Security Advisory Board (ISAB) on a Framework for International Cyber Stability," 2 July 2014, 5, accessed 25 January 2018, http://www.state.gov/documents/organization/229235.pdf.

[5] Scott Maucione, "McCain Presses Obama Administration on Cyber Deterrence," *Federal News Radio*, 20 November 2015, accessed 25 January 2018, http://federalnewsradio.com/defense/2015/11/mccain-presses-obama-administration-cyber-deterrence.

formerly an Analyst at the RAND Corporation and received an MA in International Affairs from University of California, San Diego.

Brendan Rittenhouse Green is Assistant Professor of Political Science at the University of Cincinnati.

Kelly M. Greenhill is Associate Professor at Tufts University and Research Fellow at Harvard University's Kennedy School. Greenhill is author of *Weapons of Mass Migration: Forced Displacement, Coercion and Foreign Policy*, winner of the 2011 International Studies Association's Best Book of the Year Award. She is coauthor and coeditor of *Coercion: The Power to Hurt in International Politics; Sex, Drugs and Body Counts: The Politics of Numbers in Global Crime and Conflict*; and *The Use of Force: Military Power and International Politics* (8th ed.). Greenhill has served as an analyst for the Department of Defense.

Phil Haun is Professor and Dean of Academics at the U.S. Naval War College. He is author of *Coercion, Survival and War: Why Weak States Resist the United States* (Stanford University Press, 2015) and *A-10s over Kosovo*, (Air University Press, 2003). His next book, *The Book of ACTS: The Lectures of the Air Corps Tactical School and American Strategic Bombing in World War II*, is forthcoming from the University Press of Kentucky.

Chin-Hao Huang is Assistant Professor of Political Science at Yale-NUS College. His research focuses on international relations of East Asia. He is the recipient of the American Political Science Association Foreign Policy Section Best Paper Award for his research on China's compliance behavior in multilateral security institutions. He was previously a researcher at the Stockholm International Peace Research Institute and the Center for Strategic and International Studies. He received his PhD in Political Science from the University of Southern California and BS (Hons) from Georgetown University.

David C. Kang is Professor of International Relations and Business, Director of USC Korean Studies Institute, and Director of USC Center for International Studies at the University of Southern California. Kang's latest book is *American Grand Strategy and East Asian Security in the 21st Century* (Cambridge University Press, 2017).

Ron Lehman chairs the Department of Defense Threat Reduction Advisory Committee and the Board of the International Science and Technology Center and is the Counselor at Lawrence Livermore National Laboratory. Lehman was Director of the U.S. Arms Control and Disarmament Agency, Assistant Secretary of Defense (International Security Policy), Ambassador and Chief Negotiator for START I, and Deputy Assistant to the President for National Security Affairs, and served on the Staff of the Senate Armed Services Committee and with the U.S. Army in Vietnam. Lehman was Postdoctoral Fellow at the Hoover Institution at Stanford University and Adjunct Professor at Georgetown University.

Austin G. Long is a Senior Political Scientist at the RAND Corporation. He was an analyst and adviser to the U.S. military in Iraq (2007–8) and Afghanistan (2011 and 2013). In 2014–15, Long was a Council on Foreign Relations International Affairs Fellow in Nuclear Security, serving in the Joint Staff J5 (Strategic Plans and Policy) Strategic Deterrence and Nuclear Policy Division. Long received a BS from the Sam Nunn School of International Affairs at the Georgia Institute of Technology and his PhD in Political Science from the Massachusetts Institute of Technology.

Michael Markey is a Political Scientist at Lawrence Livermore National Laboratory. He previously worked for several years in the U.S. government studying national security issues, with an emphasis on arms control monitoring. Markey's current research interests include extended deterrence and strategic stability with an emphasis on emerging domains of competition. Markey holds an MA in International Affairs from the University of California, San Diego.

Rupal N. Mehta is Assistant Professor in the Department of Political Science at the University of Nebraska-Lincoln. Previously, Mehta was Stanton Nuclear Security Postdoctoral Fellow in the Belfer Center's International Security Program and Project on Managing the Atom. Mehta's book, *The Politics of Nuclear Reversal*, explores conditions under which states that have started nuclear weapons programs stop their pursuit. Her work has appeared in the *Journal of Conflict Resolution*, *International Studies Quarterly*, and *Washington Quarterly*. Mehta received a PhD and MA in Political Science from the University of California, San Diego.

James D. Morrow is A. F. K. Organski Collegiate Professor of World Politics and Research Professor at the Center for Political Studies at the University of Michigan. He is the author of *Order within Anarchy, Game Theory for Political Scientists*, coauthor of *The Logic of Political Survival*, and author of over thirty articles in refereed journals and another thirty other publications. Morrow is a member of the American Academy of Arts and Sciences. He received the Karl Deutsch Award from the International Studies Association in 1994. He was President of the Peace Science Society in 2008–9.

Patrick M. Morgan is Professor Emeritus with the Political Science Department at the University of California, Irvine. He has published a number of books and many articles, primarily dealing with American foreign policy, national security affairs, and international politics. He has been an occasional consultant with RAND, Sandia Labs, the U.S. State Department, and the U.S. Air Force. He is a board member and recording secretary for the Council on U.S.-Korean Security Studies annual conference. He has held several Fulbright fellowships and two fellowships at the Woodrow Wilson Center.

Michael Nacht is Thomas and Alison Schneider Professor of Public Policy at the University of California, Berkeley. He served as Dean of the University's Goldman School of Public Policy (1998–2008). His most recent book is *Strategic Latency: Red,*