Falcon 9 Starlink L24 rocket successfully launches from SLC-40 at Cape Canaveral Space Force Station, Florida, April 28, 2021 (U.S. Space Force/Joshua Conti)

Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence

By Mark Montgomery and Erica Borghard

Mark Montgomery is Executive Director of the U.S. Cyberspace Solarium Commission and Senior Director of the Foundation for Defense of Democracies' Center on Cyber and Technology Innovation. Dr. Erica Borghard is a Resident Senior Fellow in the New American Engagement Initiative, Scowcroft Center for Strategy and Security, at the Atlantic Council.

Scholars and practitioners in the area of cyber strategy and conflict focus on two key strategic imperatives for the United States: first, to maintain and strengthen the current deterrence of cyberattacks of significant consequence; and second, to reverse the tide of malicious behavior that may not rise to a level of armed attack but nevertheless has cumulative strategic implications as part of adversary campaigns. The Department of Defense (DOD) strategic concept of defend forward and U.S. Cyber Command's concept of persistent engagement are largely directed toward this latter challenge. While the United States has ostensibly deterred strategic cyberattacks above the threshold of armed conflict, it has failed to create sufficient costs for adversaries below that threshold in a way that would shape adversary behavior in a desired direction.[1] Effectively, this tide of malicious behavior represents a deterrence failure for strategic cyber campaigns below the use-of-force threshold; threat actors have not been dissuaded from these types of campaigns because they have not perceived that the costs or risks of conducting them outweigh the benefits.[2] This breakdown has led to systemic and pervasive efforts by adversaries to leverage U.S. vulnerabilities and its large attack surface in cyberspace to conduct intellectual property theft—including critical national security intellectual property—at scale, use cyberspace in support of information operations that undermine America's democratic institutions, and hold at risk the critical infrastructure that sustains the U.S. economy, national security, and way of life.

U.S. strategy has simultaneously focused on the longstanding challenge of deterring significant cyberattacks that would cause loss of life, sustained disruption of essential functions and services, or critical economic impacts—those activities that may cross the threshold constituting a use of force or armed attack. Indeed, Congress chartered the U.S. Cyberspace Solarium Commission in the 2019 National Defense Authorization Act to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences."[3] There is also a general acknowledgment of the link between U.S. cyber strategy below and above the threshold of armed conflict in cyberspace. Specifically, efforts to defend forward below the level of war—to observe and pursue adversaries as they maneuver in "gray" and "red" space, and to counter adversary operations, capabilities, and infrastructure when authorized—could yield positive cascading effects that support deterrence of strategic cyberattacks.[4]

Less attention, however, has been devoted to the cross-domain nexus between adversary cyber campaigns below the level of war and the implications for conventional or nuclear deterrence and warfighting capabilities.[5] The most critical comparative warfighting advantage the United States enjoys relative to its adversaries is its technological edge in the conventional weapons realm—even as its hold may be weakening.[6] Indeed, this is why adversaries prefer to contest the United States below the level of war, in the gray zone, and largely avoid direct military confrontation where they perceive a significant U.S. advantage. At the same time, adversaries are making substantial investments in technology and innovation to directly erode that edge, while also shielding themselves from it by developing offset, antiaccess/area-denial capabilities.[7] Moreover, adversaries are engaging in cyber espionage to discern where key U.S. military capabilities and systems may be vulnerable and to potentially blind and paralyze the United States with cyber effects in a time of crisis or conflict.[8]

Therefore, while technologically advanced U.S. military capabilities form the bedrock of its military advantage, they also create cyber vulnerabilities that adversaries can and will undoubtedly use to their strategic advantage. To support a strategy of full-spectrum deterrence, the United States must maintain credible and capable conventional and nuclear capabilities. However, adversaries could hold these at risk in cyberspace, potentially undermining deterrence. If deterrence fails in times of crisis and conflict, the United States must be able to defend and surge conventional capabilities when adversaries utilize cyber capabilities to attack American military systems and functions. In this way, cyber vulnerabilities that adversaries exploit in routine competition below the level of war have dangerous implications for the U.S. ability to deter and prevail in conflict above that threshold—even in a noncyber context. The strategic consequences of the weakening of U.S. warfighting capabilities that support conventional—and, even more so, nuclear—deterrence are acute. Additionally, the scope and challenge in securing critical military networks and systems in cyberspace is immense. Therefore, urgent policy action is needed to address the cyber vulnerabilities of key weapons systems and functions.

Deterrence in U.S. Strategy

Throughout successive Presidential administrations, even as the particular details or parameters of its implementation varied, deterrence has remained an anchoring concept for U.S. strategy.[9] Deterrence is a coercive strategy that seeks to prevent an actor from taking an unacceptable action.[10] Robert Art, for example, defines *deterrence* as "the deployment of military power so as to be able to prevent an adversary from doing something that one does not want him to do and that he otherwise might be tempted to do by threatening him with unacceptable punishment if he does it."[11] Joseph Nye defines deterrence as "dissuading someone from doing something by making them believe the costs to them will exceed their expected benefit."[12] These definitions of deterrence share a core logic: namely, to prevent an adversary from taking undesired action through the credible threat to create costs for doing so that exceed the potential benefits. However, one notable distinction is Art's focus on the military instrument of power (chiefly nuclear weapons) as a tool of deterrence, whereas Nye's concept of deterrence implies a broader set of capabilities that could be marshalled to prevent unwanted behavior. Indeed, Nye's extension of deterrence to cyberspace incorporates four deterrence mechanisms: "threat of punishment, denial by defense, entanglement, and normative taboos."[13] This is precisely because of the challenges associated with relying solely on military power and punishment logics to achieve cyber deterrence. Our working definition of deterrence is therefore consistent with how Nye approaches the concept.

Credibility lies at the crux of successful deterrence. The target must believe that the deterring state has both the capabilities to inflict the threatening costs and the resolve to carry out a threat.[14] A deterring state must therefore develop mechanisms for signaling credibility to the target.[15] Much of the Cold War deterrence literature focused on the question of how to convey resolve, primarily because the threat to use

Company fire support officer assigned to 2nd Battalion, 3rd Field Artillery Regiment, 1st Armored Brigade Combat Team, 1st Armored Division, monitors computer system showing target locations at Dona Ana Range Complex, New Mexico, March 8, 2021 (U.S. Army/Elijah Ingram)

nuclear weapons—particularly in support of extended deterrence guarantees to allies—lacks inherent credibility given the extraordinarily high consequences of nuclear weapons employment in comparison to any political objective.[16] This raises questions about decisionmakers' willingness to follow through on a nuclear threat. However, the credibility conundrum manifests itself differently today. Specifically, the potential for cyber operations to distort or degrade the ability of conventional or even nuclear capabilities to work as intended could undermine the credibility of deterrence due to a reduced capability rather than political will.[17] Moreover, given the secret nature of cyber operations, there is likely to be information asymmetry between the deterring state and the ostensible target of deterrence if that target has undermined or holds at risk the deterring state's capabilities without its knowledge.

U.S. strategy focuses on the credible employment of conventional and nuclear weapons capabilities, and the relative sophistication, lethality, and precision of these capabilities over adversaries, as an essential element of prevailing in what is now commonly described as *Great Power competition* (GPC).[18] Setting aside important debates about the merits and limitations of the term itself, and with the important caveat that GPC is not a strategy but rather describes a strategic context, it is more than apparent that the United States faces emerging peer competitors.[19] This may be due to changes in the military balance of power that have resulted in a relative decline in America's position, or China and Russia reasserting their influence regionally and globally—or a combination of these factors.[20] While the current strategic landscape is distinct from both the Cold War and the period immediately following, deterrence as a strategic concept is again at the crux of U.S. strategy but with new applications and challenges. As the 2017 National Security Strategy notes, "deterrence today is significantly more complex to achieve than during the Cold War. Adversaries studied the American way of war and began investing in capabilities that targeted our strengths and sought to exploit perceived weaknesses."[21] In this new environment, cyberspace is a decisive arena in broader GPC, with significant implications for cross-domain deterrence.[22]

The literature on the feasibility of deterrence in cyberspace largely focuses on within-domain deterrence—in other words, the utility and feasibility of using (or threatening) cyber means to deter cyber behavior.[23] Scholars have identified a number of important impediments to this form of cyber deterrence.[24] For instance, the challenges of discerning timely

Chief Information Security Officer for Acquisitions Katie Arrington discusses Cybersecurity Maturity Model Certification with Norwegian National Defense and Security Industries Association, from the Pentagon, Washington, DC, January 13, 2021 (DOD/Brittany A. Chase)

and accurate attribution could weaken cyber deterrence through generating doubt about the identity of the perpetrator of a cyberattack, which undermines the credibility of response options.[25] Uncertainty about the effects of cyber capabilities—both anticipating them ex ante and measuring them ex post—may impede battle damage assessments that are essential for any deterrence calculus.[26] This uncertainty is further complicated by limitations in the ability to hold targets at risk or deliver effects repeatedly over time.[27] A deterring state may avoid revealing capabilities (which enhances the credibility of deterrence) because the act of revealing them renders the capabilities impotent.[28] Finally, the target may simply not perceive the threatened cyber costs to be sufficiently high to affect its calculus, or the target may be willing to gamble that a threatened action may not produce the effect intended by the deterring state due to the often unpredictable and fleeting nature of cyber operations and effects.[29] Others offer a more sanguine take. For instance, deterrence may have more favorable prospects when it focuses on deterring specific types of behavior or specific adversaries rather than general cyber deterrence.[30]

Notably, there has been some important work on the feasibility of cross-domain deterrence as it pertains to the threat of employing noncyber kinetic capabilities to deter unwanted behavior in cyberspace. As Jacquelyn Schneider notes, this type of deterrence "involves the use of punishment or denial across domains of warfighting and foreign policy to deter adversaries from utilizing cyber operations to create physical or virtual effects."[31] The literature has also examined the inverse aspect of cross-domain deterrence—namely, how threats in the cyber domain can generate instability and risk for deterrence across other domains. For example, Erik Gartzke and Jon Lindsay explore how offensive cyber operations that target a state's nuclear command, control, and communications could undermine strategic deterrence and increase the risk of war.[32] Similarly, Austin Long notes potential pathways from offensive cyber operations to inadvertent escalation (which is by definition a failure of deterrence) if "attacks on even nonmilitary critical systems (for example, power supplies) could impact military capabilities or stoke fears that military networks had likewise been compromised."[33]

Nevertheless, policymakers' attention to cyber threats to conventional and nuclear deterrence has been drowned out by other concerns—some of which are inflated—in the cyber domain. For instance, the typical feared scenario is the equivalent of a "cyber Pearl Harbor" or a "cyber 9/11" event—a large-scale cyberattack against critical U.S. infrastructure that causes significant harm to life or property.[34] This line of thinking, however, risks missing the ostensibly more significant threat posed by stealthy cyberspace activities that could undermine the stability of conventional or nuclear deterrence.

Cyber Risks to Conventional and Nuclear Deterrence

The cyber vulnerabilities that exist across conventional and nuclear weapons platforms pose meaningful risks to deterrence.[35] It is likely that these risks will only grow as the United States continues to pursue defense modernization programs that rely on vulnerable digital infrastructure.[36] These vulnerabilities present across four categories, each of which poses unique concerns: technical vulnerabilities in weapons programs already under development as well as fielded systems, technical vulnerabilities at the systemic level across networked platforms ("system-of-systems" vulnerabilities), supply chain vulnerabilities and the acquisitions process, and nontechnical vulnerabilities stemming from information operations.

Connectivity, automation, exquisite situational awareness, and precision are core components of DOD military capabilities; however, they also present numerous vulnerabilities and access points for cyber intrusions and attacks. Innovations in technology and weaponry have produced highly complex weapons systems, such as those in the F-35 Joint Strike Fighter, which possesses unparalleled technology, sensors, and situational awareness—some of which rely on vulnerable Internet of Things devices.[37] In a pithy depiction, Air Force Chief of Staff General David Goldfein describes the F-35 as "a computer that happens to fly."[38] However, the increasingly computerized and networked nature of these weapons systems makes it exponentially more difficult to secure them. Moreover, the use of commercial off-the-shelf (COTS) technology in modern weapons systems presents an additional set of vulnerability considerations.[39] Indeed, a 2019 DOD Inspector General report found that DOD purchases and uses COTS technologies with known cybersecurity vulnerabilities and that, because of this, "adversaries could exploit known cybersecurity vulnerabilities that exist in COTS items."[40]

Therefore, a fundamental issue is that both individual weapons programs already under development and fielded systems in the sustainment phase of the acquisition life cycle are beset by vulnerabilities. Prior to 2014, many of DOD's cybersecurity efforts were devoted to protecting networks and information technology (IT) systems, rather than the cybersecurity of the weapons themselves.[41] Protecting IT systems is important in its own right. Federal and private contractor systems have been the targets of widespread and sophisticated cyber intrusions. For instance, former Secretary of the Navy Richard Spencer described naval and industry partner systems as being "under cyber siege" by Chinese hackers.[42] Yet of most concern is that the integrity and credibility of deterrence will be compromised by the cybersecurity vulnerabilities of weapons systems.

In recent years, while DOD has undertaken efforts to assess the cyber vulnerabilities of individual weapons platforms, critical gaps in the infrastructure remain. For example, there is no permanent process to periodically assess the vulnerability of fielded systems, despite the fact that the threat environment is dynamic and vulnerabilities are not constant. This means that a singular static assessment is unlikely to capture how vulnerabilities may evolve and change over time.[43] Relatedly, a 2018 Government Accountability Office report found pervasive and significant mission-critical vulnerabilities across most weapons systems already under development.[44] Between 2012 and 2017, DOD penetration testers—individuals who evaluate the cybersecurity of computer systems and uncover vulnerabilities—discovered "mission-critical cyber vulnerabilities in nearly all weapon systems under development."[45] Penetration testing teams were able to overcome weapons systems cybersecurity controls designed to prevent determined adversaries from gaining access to these platforms and to maneuver within compromised systems while successfully evading detection.

Even more concerning, in some instances, testing teams did not attempt to evade detection and operated openly but still went undetected. Moreover, some DOD operators did not even know the system had been compromised: "[U]nexplained crashes were normal for the system," and even when intrusion detection systems issued alerts, "[this] did not improve users' awareness of test team activities because . . . warnings were so common that operators were desensitized to them."[46] Existing testing programs are simply too limited to enable DOD to have a complete understanding of weapons system vulnerabilities, which is compounded by a shortage of skilled penetration testers.[47]

Individual weapons platforms do not in reality operate in isolation from one another. Rather, most modern weapons systems comprise a complex set of systems—systems of systems that entail "operat[ing] multiple platforms and systems in a collaborate manner to perform military missions."[48] An example is the Aegis weapon system, which contains a variety of integrated subsystems, including detection, command and control, targeting, and kinetic capabilities.[49] Therefore, vulnerability assessments that focus on individual platforms are unable to identify potential vulnerabilities that may arise when these capabilities interact or work together as part of a broader, networked platform. The challenge of securing these complex systems is compounded by the interaction of legacy and newer weapons systems—and most DOD weapons platforms are legacy platforms. Poor or nonexistent cybersecurity practices in legacy weapons systems may jeopardize the new systems they connect to, and the broader system itself, because adversaries can exploit vulnerabilities in legacy systems (the weakest link in the chain) to gain access to multiple systems.[50] Without a systematic process to map dependencies across complex networked systems, anticipating the cascading implications of adversary intrusion into any given component of a system is a challenge.

Another pathway through which adversaries can exploit vulnerabilities in weapons systems is the security of the DOD supply chain—the global constellation of components and processes that form the production of DOD capabilities—which is shaped by DOD's acquisitions strategy, regulations, and requirements. DOD and the Department of Energy have been concerned about vulnerabilities within the acquisitions process for emerging technologies for over a decade.[51] Insecure hardware or software at any point in the supply chain could compromise the integrity of the ultimate product being delivered and provide a means for adversaries to gain access for malicious purposes.

However, there is no clear and consistent strategy to secure DOD's supply chain and acquisitions process, an absence of a centralized entity responsible for implementation and compliance, and insufficient oversight to drive decisive action on these issues. There is instead decentralized responsibility across DOD, coupled with a number of reactive and ad hoc measures that leave DOD without a complete picture of its supply chain, dynamic understanding of the scope and scale of its vulnerabilities, and consistent mechanisms to rapidly remediate these vulnerabilities.

Until recently, DOD's main acquisitions requirements policy did not systematically address cybersecurity concerns. For instance, it did not call for programs to include cyberattack survivability as a key performance parameter.[52] These types of requirements are typically established early in the acquisitions process and drive subsequent system design decisionmaking. If cybersecurity requirements are tacked on late in the process, or after a weapons system has already been deployed, the requirements are far more difficult and costly to address and much less likely to succeed.[53] In 2016, DOD updated the Defense Federal Acquisition Regulations Supplement (DFARS), establishing cybersecurity requirements for defense contractors based on standards set by the National Institute of Standards and Technology. Then, in part due to inconsistencies in compliance, verification, and enforcement in the cybersecurity standards established in DFARS, in 2019 DOD issued the Cybersecurity Maturity Model Certification, which created new, tiered cybersecurity standards for defense contractors and was meant to build on the 2016 DFARS requirement.[54] However, this has resulted in confusion about requirements, and the process for independently auditing and verifying compliance remains in nascent stages of development.[55] At the same time, in the 2019 National Defense Authorization Act (NDAA), Congress took legislative action to ban government procurement of or contracting with entities that procure telecommunications technologies from specific Chinese firms, including Huawei and ZTE, and affiliated organizations. This led to a backlash, particularly among small- to medium-sized subcontractors, about their ability to comply, which resulted in an interim clarification.[56]

Moreover, ownership of this procurement issue remains decentralized, with different offices both within and without DOD playing important roles. Significant stakeholders within DOD include the Under Secretary of Defense for Acquisition and Sustainment, the Under Secretary of Defense for Intelligence and Security, the Defense Counterintelligence and Security Agency, the Cybersecurity Directorate within the National Security Agency, the DOD Cyber Crime Center, and the Defense Industrial Base Cybersecurity Program, among others. Within the Intelligence Community, the National Counterintelligence and Security Center within the Office of the Director of National Intelligence also plays a role in supply chain security through its counterintelligence mission, which includes the defense industrial base. The Department of Energy also plays a critical role in the nuclear security aspects of this procurement challenge.[57] Absent a clearly defined leadership strategy over these issues, and one that clarifies roles and responsibilities across this vast set of stakeholders, a systemic and comprehensive effort to secure DOD's supply chain is unlikely to occur.[58]

Risks stemming from nontechnical vulnerabilities are entirely overlooked in strategies and policies for identifying and remediating cyber vulnerabilities in DOD weapons systems. However, adversaries could compromise the integrity of command and control systems—most concerningly for nuclear weapons—without exploiting technical vulnerabilities in the digital infrastructure on which these systems rely. Instead, malicious actors could conduct cyber-enabled information operations with the aim of manipulating or distorting the perceived integrity of command and control. This could take place in positive or negative forms—in other words, perpetrating information as a means to induce operations to erroneously make a decision to employ a capability or to refrain from carrying out a lawful order. The consequences are significant, particularly in the nuclear command and control realm, because not employing a capability could undermine positive and negative control over nuclear weapons and inevitably the stability of nuclear deterrence.

Policy Recommendations

Recognizing the interdependence among cyber, conventional, and nuclear domains, U.S. policymakers must prioritize efforts to reduce the cyber vulnerabilities of conventional and nuclear capabilities and ensure they are resilient to adversary action in cyberspace. Cyber threats to these systems could distort or undermine their intended uses, creating risks that these capabilities may not be reliably employable at critical junctures. Additionally, cyber-enabled espionage conducted against these systems could allow adversaries to replicate cutting-edge U.S. defense technology without comparable investments in research and development and could inform the development of adversary offset capabilities. Vulnerabilities such as these have important implications for deterrence and warfighting. Deterrence postures that rely on the credible, reliable, and effective threat to employ conventional or nuclear capabilities could be undermined through adversary cyber operations. And, if deterrence fails, cyber operations to disrupt or degrade the functioning of kinetic weapons systems could compromise mission assurance during crises and conflicts.

More than 100 players from around the Nation participate in Defend Forward: 2019 Critical Infrastructure War Game, at U.S. Naval War College, July 25, 2019, in Newport, Rhode Island (U.S. Navy/Tyler D. John)

As adversaries' cyber threats become more sophisticated, addressing the cybersecurity of DOD's increasingly advanced and networked weapons systems should be prioritized. The Cyberspace Solarium Commission's March 2020 report details a number of policy recommendations to address this challenge.[59] We now unpack a number of specific measures put forth by the Cyberspace Solarium Commission that Congress, acting in its oversight role, along with the executive branch could take to address some of the most pressing concerns regarding the cyber vulnerabilities of conventional and nuclear weapons systems. We also describe the important progress made in the fiscal year (FY) 2021 NDAA, which builds on the commission's recommendations.

In terms of legislative remedies, the Cyberspace Solarium Commission report recommends Congress update its recent legislative measures to assess the cyber vulnerabilities of weapons systems to account for a number of important gaps. The ultimate objective is to enable DOD to develop a more complete picture of the scope, scale, and implications of cyber vulnerabilities to critical weapons systems and functions. Past congressional action has spurred some important progress on this issue. Specifically, in Section 1647 of the FY16 NDAA, which was subsequently updated in Section 1633 of the FY20 NDAA, Congress directed DOD to assess the cyber vulnerabilities of each major weapons system.[60] Although this process has commenced, gaps remain that must be remediated. For example, there is no permanent process to periodically assess the cybersecurity of fielded systems. Additionally, the current requirement is to assess the vulnerabilities of *individual* weapons platforms. But given the interdependent and networked nature of multiple independent weapons systems, merely assessing individual platforms misses crucial potential vulnerabilities that may arise when platforms interact with one another. Therefore, DOD must also evaluate how a cyber intrusion or attack on one system could affect the entire mission—in other words, DOD must assess vulnerabilities at a systemic level.

Given that Congress has already set a foundation for assessing cyber vulnerabilities in weapons systems, there is an opportunity to legislatively build on this progress. The commission proposed Congress amend Section 1647 of the FY16 NDAA (which, as noted, was amended in the FY20 NDAA) to include a requirement for DOD to annually assess major weapons systems vulnerabilities. In the FY21 NDAA, Congress incorporated elements of this recommendation,

Colonial Pipeline halted operation of its 5,500 miles of pipeline, stretching from Texas to New York, after being hit by randsomware cyber attack, on May 7, 2021 (Photo courtesy J.B.)

directing the Secretary of Defense to institutionalize a recurring process for cybersecurity vulnerability assessments that "take[s] into account upgrades or other modifications to systems and changes in the threat landscape."[61] Importantly, Congress recommended that DOD assign a senior official responsibilities for overseeing and managing this process—a critical step given the decentralization of oversight detailed herein—thus clarifying the National Security Agency's Cybersecurity Directorate's role in supporting this program.[62] In a different section of the FY21 NDAA, Congress updated language describing the Principal Cyber Advisor's role within DOD as the coordinating authority for "cybersecurity issues relating to the defense industrial base," with specific responsibility to "synchronize, harmonize, de-conflict, and coordinate all policies and programs germane to defense industrial base cybersecurity," including acquisitions and contract enforcement on matters pertaining to cybersecurity.[63]

Work remains to be done. To strengthen congressional oversight and drive continued progress and attention toward these issues, the requirement to conduct periodic vulnerability assessments should also include an after-action report that includes current and planned efforts to address cyber vulnerabilities of interdependent and networked weapons systems in broader mission areas, with an intent to gain mission assurance of these platforms. Moreover, the process of identifying interdependent vulnerabilities should go beyond assessing technical vulnerabilities to take a risk management approach to drive prioritization given the scope and scale of networked systems. The objective would be to improve the overall resilience of the systems as well as to identify secondary and tertiary dependencies, with a focus on rapid remediation of identified vulnerabilities. In addition to assessing fielded systems vulnerabilities, DOD should enforce cybersecurity requirements for systems that are in development early in the acquisition life cycle, ensuring they remain an essential part of the front end of this process and are not "bolted on" later.[64] Doing so would essentially create a requirement for DOD to institutionalize a continuous assessment process of weapons systems' cyber vulnerabilities and annually report on these vulnerabilities, thereby sustaining its momentum in implementing key initiatives.

Additionally, in light of the potentially acute and devastating consequences posed by the possibility of cyber threats to nuclear deterrence and command and control, coupled with ongoing nuclear modernization programs that may create unintended cyber risks, the cybersecurity of nuclear command, control, and communications (NC3) and National Leadership Command Capabilities (NLCC) should be given specific attention.[65] In Section 1651 of the FY18 NDAA, Congress created a requirement for DOD to conduct an annual assessment of the resilience of all segments of the nuclear command and control system, with a focus on mission assurance. The FY21 NDAA makes important progress on this front. Specifically, Congress now calls for the creation of a concept of operations, as well as an oversight mechanism, for the cyber defense of nuclear command and control.[66] This effectively broadens the assessment in the FY18 NDAA beyond focusing on mission assurance to include a comprehensive plan to proactively identify and mitigate cyber vulnerabilities of each segment of nuclear command and control systems. Establishing an explicit oversight function mechanism will also hopefully create mechanisms to ensure that DOD routinely assesses every segment of the NC3 and NLCC enterprise for adherence to cybersecurity best practices, vulnerabilities, and evidence of compromise.

Inevitably, there is an inherent tension between Congress's efforts to act in an oversight capacity and create additional requirements for DOD, and the latter's desire for greater autonomy. Nevertheless, the stakes remain high to preserve the integrity of core conventional and nuclear deterrence and warfighting capabilities, and efforts thus far, while important, have not been sufficiently comprehensive.

In addition to congressional action through the NDAA, DOD could take a number of steps to reinforce legislative efforts to improve the cybersecurity of key weapons systems and functions. For example, as a complement to institutionalizing a continuous process for DOD to assess the cyber vulnerabilities of weapons systems, the department could formalize a capacity for continuously seeking out and remediating cyber threats across the entire enterprise. This is why the commission recommends that DOD develop and designate a force structure element to serve as a threat-hunting capability across the entire DOD Information Network (DODIN), thus covering the full range of nonnuclear to nuclear force employment. Threat-hunting entails proactively searching for cyber threats on assets and networks. Specifically, DOD could develop a campaign plan for a threat-hunting capability that takes a risk-based approach to analyzing threat intelligence and assessing likely U.S. and allied targets of adversary interest. Based on this analysis, this capability could proactively conduct threat-hunting against those identified networks and assets to seek evidence of compromise, identify vulnerabilities, and deploy countermeasures to enable early warning and thwart adversary action. Given the potentially high consequences of cyber threats to NC3 and NLCC, priority should be assigned to identifying threats to these networks and systems, and threat-hunting should recur with a frequency commensurate with the risk and consequences of compromise.

A potential impediment to implementing this recommendation is the fact that many cyber threats will traverse the boundaries of combatant commands, including U.S. Cyber Command, U.S. Strategic Command, and the geographic combatant commands. In order for a force structure element for threat-hunting across DODIN to have more seamless and flexible maneuver, DOD should consider developing a process to reconcile the authorities and permissions to enable threat-hunting across all DODIN networks, systems, and programs.

Given the extraordinarily high consequence of a successful adversary cyber-enabled information operation against nuclear command and control decisionmaking processes, DOD should consider developing a comprehensive training and educational requirement for relevant personnel to identify and report potential activity. DOD must additionally consider incorporating these considerations into preexisting table-top exercises and scenarios around nuclear force employment while incorporating lessons learned into future training.[67] Implementing these recommendations would enhance existing DOD efforts and have a decisive impact on enhancing the security and resilience of the entire DOD enterprise and the critical weapons systems and functions that buttress U.S. deterrence and warfighting capabilities.

Much of the focus within academic and practitioner communities in the area of cyber deterrence has been on within-domain deterrence, and even studies of cross-domain deterrence have been largely concerned with the employment of noncyber instruments of power to deter cyberattacks. This has led to a critical gap in strategic thinking—namely, the cross-domain implications of cyber vulnerabilities and adversary cyber operations in day-to-day competition for deterrence and warfighting above the level of armed conflict. Failure to proactively and systematically address cyber threats and vulnerabilities to critical weapons systems, and to the DOD enterprise, has deleterious implications for the U.S. ability to deter war, or fight and win if deterrence fails. Implementing the Cyberspace Solarium Commission's recommendations would go a long way toward restoring confidence in the security and resilience of the U.S. military capabilities that are the foundation of the Nation's deterrent. **JFQ**

Notes

[1] *Summary: Department of Defense Cyber Strategy 2018* (Washington, DC: Department of Defense [DOD], 2018), available at <https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF>; *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Washington, DC: U.S. Cyber Command, 2018), available at <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>; "An Interview with Paul M. Nakasone," *Joint Force Quarterly* 92 (1st Quarter 2019), 6–7.

[2] The United States has long maintained strategic ambiguity about how to define what constitutes a *use of force* in any domain, including cyberspace, and has taken a more flexible stance in terms of the difference between a *use of force* and *armed attack* as defined in the United Nations charter.

[3] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232—August 13, 2018, 132 Stat. 1636, available at <https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf>.

[4] As defined in Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, June 8, 2018), "The term 'blue cyberspace' denotes areas in cyberspace protected by [the United States], its mission partners, and other areas DOD may be ordered to protect," while "'red cyberspace' refers to those portions of cyberspace owned or controlled by an adversary or enemy." Finally, "all cyberspace that does not meet the description of either 'blue' or 'red' is referred to as 'gray' cyberspace" (I-4, I-5). Prior to the 2018 strategy, defending its networks had been DOD's primary focus; see *The DOD Cyber Strategy* (Washington, DC: DOD, April 2015), available at <https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf>.

[5] For a notable exception, see Erik Gartzke and Jon R. Lindsay, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity* (Oxford: Oxford University Press, 2019).

[6] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2020* (Washington, DC: DOD, 2020).

[7] The spread of advanced air defenses, antisatellite, and cyberwarfare capabilities has given weaker actors the ability to threaten the

United States and its allies. For example, China is the second-largest spender on research and development (R&D) after the United States, accounting for 21 percent of the world's total R&D spending in 2015. Also, improvements in Russia's military over the past decade have reduced the qualitative and technological gaps between Russia and the North Atlantic Treaty Organization. See National Science Board, "Overview of the State of the U.S. S&E Enterprise in a Global Context," in *Science and Engineering Indicators 2018* (Alexandria, VA: National Science Foundation, 2018), O-1; Scott Boston et al., *Assessing the Conventional Force Imbalance in Europe: Implications for Countering Russian Local Superiority* (Santa Monica, CA: RAND, 2018).

[8] Gordon Lubold and Dustin Volz, "Navy, Industry Partners Are 'Under Cyber Siege' by Chinese Hackers, Review Asserts," *Wall Street Journal*, March 2019, available at <https://www.wsj.com/articles/navy-industry-partners-are-under-cyber-siege-review-asserts-11552415553>; Zak Doffman, "Cyber Warfare: U.S. Military Admits Immediate Danger Is 'Keeping Us Up at Night,'" *Forbes*, July 21, 2019, available at <https://www.forbes.com/sites/zakdoffman/2019/07/21/cyber-warfare-u-s-military-admits-immediate-danger-is-keeping-us-up-at-night/#7f48cd941061>.

[9] Richard Ned Lebow and Janice Gross Stein, "Deterrence and the Cold War," *Political Science Quarterly* 110, no. 2 (Summer 1995), 157–181.

[10] Lawrence Freedman, *Deterrence* (Cambridge, UK: Polity, 2004), 26.

[11] Robert J. Art, "To What Ends Military Power?" *International Security* 4, no. 4 (Spring 1980), 6.

[12] Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (January 2017), 45. For additional definitions of deterrence, see Glenn H. Snyder, *Deterrence and Defense* (Princeton: Princeton University Press, 1961); Robert Jervis, "Deterrence Theory Revisited," *World Politics* 31, no. 2 (January 1979), 289–324; Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1980); and Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966).

[13] Nye, "Deterrence and Dissuasion," 54–55.

[14] Schelling, *Arms and Influence*; Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017), 454–455. See also Alexander L. George, William E. Simons, and David I. Hall, eds., *The Limits of Coercive Diplomacy* (Boulder, CO: Westview Press, 1994), for a more extensive list of success criteria.

[15] See James D. Fearon, "Signaling Foreign Policy Interests: Tying Hands Versus Sinking Costs," *Journal of Conflict Resolution* 41, no. 1 (February 1997), 68–90; Robert Jervis, "Signaling and Perception: Drawing Inferences and Projecting Images," in *Political Psychology*, ed. Kristen Renwick Monroe (Mahwah, NJ: Lawrence Erlbaum Associates Publishers, 2002), 293–312.

[16] The literature on nuclear deterrence theory is extensive. Some key works include Kenneth N. Waltz, *The Spread of Nuclear Weapons: More May Be Better*, Adelphi Papers 171 (London: International Institute for Strategic Studies, 1981); Lawrence D. Freedman and Jeffrey Michaels, *The Evolution of Nuclear Strategy* (London: Macmillan, 1989); Robert Powell, *Nuclear Deterrence Theory: The Search for Credibility* (Cambridge: Cambridge University Press, 1990); Richard K. Betts, *Nuclear Blackmail and Nuclear Balance* (Washington, DC: Brookings Institution Press, 1987); Bernard Brodie, *Strategy in the Missile Age* (Princeton: Princeton University Press, 2015); Schelling, *Arms and Influence.*

[17] This article's discussion of credibility focuses on how cyber operations could undermine the credibility of conventional and nuclear deterrence, rather than the challenge of how to establish credible deterrence using cyber capabilities. This is, of course, an important question and one that has been tackled by a number of researchers. See, for example, Martin C. Libicki, *Brandishing Cyberattack Capabilities* (Santa Monica, CA: RAND, 2013); Brendan Rittenhouse Green and Austin Long, "Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition," *International Security* 44, no. 3 (January 2020), 48–83.

[18] *Summary: DOD Cyber Strategy.*

[19] For one take on the *Great Power competition* terminology, see Zack Cooper, "Bad Idea: 'Great Power Competition' Terminology" (Washington, DC: Center for Strategic and International Studies, December 1, 2020), available at <https://defense360.csis.org/bad-idea-great-power-competition-terminology/>.

[20] See, for example, Eric Heginbotham et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017* (Santa Monica, CA: RAND, 2015); Michèle A. Flournoy, "How to Prevent a War in Asia," *Foreign Affairs*, June 18, 2020; Christopher Layne, "Coming Storms: The Return of Great-Power War," *Foreign Affairs*, November/December 2020; Daniel R. Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, February 13, 2018), available at https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[21] *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 27, available at <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

[22] Daniel R. Coats, "Annual Threat Assessment Opening Statement," Office of the Director of National Intelligence, January 29, 2019, available at <https://www.dni.gov/files/documents/Newsroom/Testimonies/2019-01-29-ATA-Opening-Statement_Final.pdf>. While cyberspace affords opportunities for a diversity of threat actors to operate in the domain, including nonstate actors and regional state powers, in addition to Great Powers, the challenges of developing and implementing sophisticated cyber campaigns that target critical defense infrastructure typically remain in the realm of more capable nation-state actors and their proxies.

[23] For some illustrative examples, see Robert Jervis, "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare* 15, no. 2 (2016), 66–73; Nye, "Deterrence and Dissuasion," 44–71; Martin C. Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016); Aaron F. Brantly, "The Cyber Deterrence Problem," in *2018 10th International Conference on Cyber Conflict*, ed. Tomas Minarik, Raik Jakschis, and Lauri Lindstrom (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2018), available at <https://ccdcoe.org/uploads/2018/10/Art-02-The-Cyber-Deterrence-Problem.pdf>; Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).

[24] Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017), 381–393.

[25] Libicki, *Cyberspace in Peace and War*, 41–42; Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack," *Journal of Cybersecurity* 1, no. 1 (2015), 53–67; Nye, "Deterrence and Dissuasion," 49–52.

[26] Lindsay, "Tipping the Scales," 52.

[27] Ibid., 56.

[28] Brantly, "The Cyber Deterrence Problem"; Borghard and Lonergan, "The Logic of Coercion."

[29] Borghard and Lonergan, "The Logic of Coercion"; Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018); "An Interview with Paul M. Nakasone," 4.

[30] Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly* 77 (2nd Quarter 2015).

[31] Jacquelyn G. Schneider, "Deterrence in and Through Cyberspace," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Erik Gartzke and Jon R. Lindsay (Oxford: Oxford University Press, 2019), 104.

[32] Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3, no. 1 (2017), 37–48.

[33] Austin Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," *Journal of Cybersecurity* 3, no. 1 (2017), 20.

[34] See, for example, Emily O. Goldman and Michael Warner, "Why a Digital Pearl Harbor Makes Sense . . . and Is Possible," in *Understand-*

ing Cyber Conflict: 14 Analogies, ed. George Perkovich and Ariel E. Levite (Washington, DC: Georgetown University Press, 2017), 147–157; and Justin Sherman, "How the U.S. Can Prevent the Next 'Cyber 9/11,'" *Wired*, August 6, 2020, available at <https://www.wired.com/story/how-the-us-can-prevent-the-next-cyber-911/>.

[35] Relatedly, adversary campaigns to conduct cyber-enabled intellectual property theft against the U.S. military and the defense industrial base are also a concern because they continue to cause staggering losses of national security information and intellectual property.

[36] Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: DOD, January 2013), available at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf>.

[37] DOD Office of Inspector General, *Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of the Commercial Off-the-Shelf Items*, Report No. DODIG-2019-106 (Washington, DC: DOD, July 26, 2019), 2, available at <https://www.oversight.gov/sites/default/files/oig-reports/DODIG-2019-106.pdf>.

[38] Valerie Insinna, "Inside America's Dysfunctional Trillion-Dollar Fighter-Jet Program," *The New York Times Magazine*, August 21, 2019, available at <https://www.nytimes.com/2019/08/21/magazine/f35-joint-strike-fighter-program.html>.

[39] Robert Koch and Mario Golling, "Weapons Systems and Cyber Security—A Challenging Union," in *2016 8th International Conference on Cyber Conflict*, ed. Nikolaos Pissanidis, Henry Roigas, and Matthijs Veenendaal (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016), 194, available at <https://www.ccdcoe.org/uploads/2018/10/Art-12-Weapons-Systems-and-Cyber-Security-A-Challenging-Union.pdf>.

[40] DOD Office of Inspector General, *Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of the Commercial Off-the-Shelf Items*, i.

[41] *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, DC: Government Accountability Office, 2018), available at <https://www.gao.gov/assets/gao-19-128.pdf>.

[42] Lubold and Volz, "Navy, Industry Partners Are 'Under Cyber Siege.'"

[43] *Weapon Systems Cybersecurity*, 31–32.

[44] Ibid., 21.

[45] Ibid.

[46] Ibid., 24.

[47] Ibid., 25. See also Martin C. Libicki, David Senty, and Julia Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (Santa Monica, CA: RAND, 2014), x; Julian Jang-Jaccard and Surya Nepal, "A Survey of Emerging Threats in Cybersecurity," *Journal of Computer and System Sciences* 80, no. 5 (2014), 977.

[48] Assistant Secretary of the Navy for Research, Development, and Acquisition, Chief Systems Engineer, *Naval "Systems of Systems" Systems Engineering Guidebook, Volume II*, Version 2.0 (Washington, DC: Headquarters Department of the Navy, November 6, 2006), 3.

[49] *Leading Edge: Combat Systems Engineering & Integration* (Dahlgren, VA: NAVSEA Warfare Centers, February 2013), 9; "Aegis Weapon System," available at <https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2166739/aegis-weapon-system/>.

[50] Koch and Golling, "Weapons Systems and Cyber Security," 191.

[51] Office of Inspector General, *Progress and Challenges in Securing the Nation's Cyberspace* (Washington, DC: Department of Homeland Security, July 2004), 1–36, available at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-019.pdf>.

[52] *Manual for the Operation of the Joint Capabilities Integration and Development System* (Washington, DC: DOD, August 2018).

[53] *Weapon Systems Cybersecurity*, 9–10.

[54] For gaps in and industry reaction to the Defense Federal Acquisition Regulation Supplement, see, for example, National Defense Industrial Association (NDIA), *Implementing Cybersecurity in DOD Supply Chains White Paper: Manufacturing Division Survey Results* (Arlington, VA: NDIA, July 2018), available at <http://www.ndia.org/-/media/sites/ndia/divisions/manufacturing/documents/cybersecurity-in-dod-supply-chains.ashx?la=en>.

[55] Office of the Under Secretary of Defense for Acquisition and Sustainment, Cybersecurity Maturity Model Certification, available at <https://www.acq.osd.mil/cmmc/>; DOD, "Press Briefing by Under Secretary of Defense for Acquisition and Sustainment Ellen M. Lord, Assistant Secretary of Defense for Acquisition Kevin Fahey, and Chief Information Security Officer for Acquisition Katie Arrington," January 31, 2020, available at <https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2072073/press-briefing-by-under-secretary-of-defense-for-acquisition-sustainment-ellen/>.

[56] "Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment," *Federal Register*, July 14, 2020, available at <https://www.federalregister.gov/documents/2020/07/14/2020-15293/federal-acquisition-regulation-prohibition-on-contracting-with-entities-using-certain>.

[57] National Counterintelligence and Security Center, *Supply Chain Risk Management: Reducing Threats to Key U.S. Supply Chains* (Washington, DC: Office of the Director of National Intelligence, 2020), available at <https://www.dni.gov/files/NCSC/documents/supplychain/20200925-NCSC-Supply-Chain-Risk-Management-tri-fold.pdf>.

[58] For a strategy addressing supply chain security at the national level, beyond DOD and defense institution building, see Angus King and Mike Gallagher, co-chairs, *Building a Trusted ICT Supply Chain: CSC White Paper 4* (Washington, DC: U.S. Cyberspace Solarium Commission, October 2020), available at <https://www.solarium.gov/public-communications/supply-chain-white-paper>.

[59] These include implementing defend forward, which plays an important role in addressing one aspect of this challenge. As stated in the *Summary: DOD Cyber Strategy 2018*, "The Department must defend its own networks, systems, and information from malicious cyber activity and be prepared to defend, when directed, those networks and systems operated by non-DOD-owned Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) entities." Ensuring the Cyber Mission Force has the right size for the mission is important. Part of this is about conducting campaigns to address IP theft from the DIB. See the Cyberspace Solarium Commission's recent report, available at <www.solarium.gov>.

[60] House Armed Services Committee (HASC), *National Defense Authorization Act for Fiscal Year 2016*, H.R. 1735, 114th Cong., Pub. L. No. 114-92, 2015–2016, available at <https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf>.

[61] HASC, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Conference Report to Accompany H.R. 6395*, December 2020, 1796.

[62] Ibid., 1797.

[63] Ibid., 1861–1862.

[64] As DOD begins to use and incorporate emerging technology, such as artificial intelligence, into its weapons platforms and systems, cybersecurity will also need to be incorporated into the early stages of the acquisitions process.

[65] *Nuclear Posture Review* (Washington, DC: DOD, February 2018), available at <https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF>; Jon Lindsay, "Digital Strangelove: The Cyber Dangers of Nuclear Weapons," *Lawfare*, March 12, 2020, available at <https://www.lawfareblog.com/digital-strangelove-cyber-dangers-nuclear-weapons>; Paul Bracken, "The Cyber Threat to Nuclear Stability," *Orbis* 60, no. 2 (February 2016).

[66] HASC, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, H.R. 6395, 116th Cong., 2nd sess., 1940.

[67] Lindsay, "Digital Strangelove."