What is the Future of Cyber Deterrence?

Erica Lonergan, Mark Montgomery

The SAIS Review of International Affairs

Conflict in the Fifth Domain

Johns Hopkins

SAIS Review of International Affairs, Volume 41, Number 2, Summer-Fall 2021, pp. 61-73 (Article)

Published by Johns Hopkins University Press

What is the Future of Cyber Deterrence?

Erica Lonergan and Mark Montgomery

Scholars and practitioners alike have debated the feasibility of applying deterrence models to cyberspace. Advocates of "cyber persistence theory," for instance, posit that deterrence strategies are unlikely to succeed in the cyber domain. In contrast, the Cyberspace Solarium Commission's March 2020 report advocates for updating traditional deterrence concepts to account for the implications of emerging technologies, calling for the United States to implement a strategy of "layered cyber deterrence." In this article, we unpack the concept of cyber deterrence from three perspectives: definitional differences; distinguishing between general and specific deterrence; and the role of thresholds. Based on our analysis, we demonstrate why cyber strategies anchored in persistent engagement and near-constant offensive maneuver are insufficient to address the range of threat actor behavior in cyberspace. Instead, we offer a theoretical framework that articulates the conditions under which deterrence is possible in cyberspace. Finally, we conclude by providing policy recommendations for the United States.

Introduction

The question of the applicability of deterrence frameworks to cyberspace is an enduring debate among scholars and practitioners. Deterrence is a strategy to prevent a target from taking an action that the deterrer finds undesirable through manipulating the target's perception of the costs, benefits, and risks

Dr. Erica Lonergan (née Borghard) is an Assistant Professor in the Army Cyber Institute at the United States Military Academy at West Point. She is also a Research Scholar in the Saltzman Institute of War and Peace Studies at Columbia University. Erica served as the Senior Director and Lead, Task Force One, for the U.S. Cyberspace Solarium Commission. Previously, Erica held Senior Fellow positions at the Carnegie Endowment for International Peace and the Atlantic Council. Prior to that, Erica was a Council on Foreign Relations International Affairs Fellow, with placement at JPMorgan Chase and U.S. Cyber Command. Erica also served as an Assistant Professor and Executive Director of the Rupert H. Johnson Grand Strategy Program in the Department of Social Sciences at West Point. She holds a Ph.D. in Political Science from Columbia University and is a term member of the Council on Foreign Relations. The views expressed are personal and do not reflect the policy or position of any U.S. government entity or organization.

Mark Montgomery serves as the Senior Advisor to the Chairmen of the Cyberspace Solarium Commission and was previously the Executive Director. He is also the Senior Director of the Center on Cyber and Technology Innovation and a Senior Fellow at the Foundation for Defense of Democracies. He previously served as Policy Director for the Senate Armed Services Committee under the leadership of Senator John S. McCain and completed 32 years as a nuclear trained surface warfare officer in the U.S. Navy, retiring as a Rear Admiral in 2017. Mark has graduate degrees from the University of Pennsylvania and Oxford University, and he completed the U.S. Navy's nuclear power training program.

of cooperating versus defecting.[1] Deterrence is often associated with the threat of punishment (e.g., threatening to impose significant costs on a target to dissuade them from acting). US nuclear deterrence strategy during the Cold War is associated with this form of deterrence. However, deterrence could also take other forms, such as denial, by making it more difficult for a target to carry out an action through increasing the military costs of doing so, which is prevalent in conventional deterrence; entanglement in leveraging the interdependence of the deterrer and target; or norms, by creating reputational costs for violating the terms of the threat.[2] Deterrence succeeds when the target perceives that these costs outweigh the expected gains and that the deterring state has both the capability and willingness to carry out the threat.[3] Therefore, possessing a capability, or even demonstrating a capability, is not necessarily sufficient for deterrence to succeed. The deterring state must communicate to the target its expectations about behavior and consequences for defection in a way that is appropriately understood by the target, making signaling an essential element of deterrence.[4]

Early academic work on cyber deterrence, largely drawn from nuclear deterrence literature, expressed skepticism that the logic of deterrence could be extended to cyberspace.[5] According to these scholars, while cyber capabilities may change the nature of conflict, certain characteristics of cyberspace also create vexing challenges for deterrence and signaling.[6] For example, several factors may complicate the effective communication of deterrent threats in cyberspace. These include the preference for operating secretly and maintaining plausible deniability and, by extension, challenges of attribution; the absence of common indices or shared frameworks to help clarify the intent behind observed behavior; and the ways that cyber operations function as ambiguous (rather than clear) signals. Additionally, some purported attributes of cyberspace complicate deterrence capabilities beyond communication, such as the "borderless" nature of cyberspace; the speed with which attacks take place; the low barriers to entry and proliferation of capabilities across numerous actors; and the advantages of offense over defense.[7] And finally, there are credibility issues associated with cyber deterrence, particularly in terms of punishment-based strategies, because the lack of violence in cyber operations and the limitations of obtaining strategic effects—the damage that can be inflicted with cyber capabilities in comparison to other military capabilities—raise questions about whether states would actually follow through on the terms of deterrent threats.[8]

Given these challenges, some academics have extended this line of reasoning to reject the feasibility of cyber deterrence outright, particularly for cyber operations that occur in the competitive space below the level of armed conflict. The emergence of cyber persistence theory, epitomized by Richard Harknett and Michael Fischerkeller's work, reflects the idea that the absence of traditional sovereignty in cyberspace, coupled with a state of "constant contact" between rivals, poses insurmountable hurdles for deterrence strategies.[9] Instead, states should operate continuously in cyberspace to "shape cyberspace *ad infinitum*."[10] Over time, Fischerkeller posits, norms of behavior and stability will emerge in cyberspace through a process of *tacit bargaining*, whereby, through continuously interacting in cyberspace, rivals will come to shared understandings of what is acceptable versus unacceptable behavior, an "agreed competition."[11]

Nevertheless, strategy and policy in the United States continue to be anchored in strategic concepts based on the logic of deterrence. For example, despite articulating a new strategic vision for military cyber operations based on the idea of "defending forward"—actively maneuvering and disrupting adversary capabilities and infrastructure as close as possible to their sources—the 2018 Department of Defense (DoD) Cyber Strategy largely echoes the 2015 DoD Cyber Strategy in its emphasis on deterrence.[12] More recently, the US Cyberspace Solarium Commission, chartered by Congress in 2019 to develop a comprehensive cyber strategy for the United States, emphatically endorsed the idea that cyber deterrence is possible. The Commission's March 2020 report articulates a strategy of "layered cyber deterrence" aimed at "increas[ing] the costs and decreas[ing] the benefits that adversaries anticipate when planning cyber attacks against American interests."[13]

The viability of deterrence frameworks has vital implications for US policymaking. If deterrence is mismatched to the strategic environment in cyberspace, or to the strategies of US adversaries, then US strategies and policies grounded in deterrence are likely to fail. However, we argue that the question of cyber deterrence is not as simple as ascertaining whether or not it works. Rather, we aim to go beyond binary debates about the feasibility of cyber deterrence, and instead explore the conditions under which different forms of deterrence are more or less likely to work in cyberspace. In doing so, we build on Joseph Nye's foundational work on the different forms of deterrence in cyberspace, as well as work by Jacquelyn Schneider, Erik Gartzke, Jon Lindsay, Shawn Lonergan, and other authors that explores the cross-domain aspects of cyber deterrence.[14] Specifically, there are three core conceptual issues that need to be examined to assess the viability of cyber deterrence under various conditions: What do we mean by cyber deterrence? Are there different dynamics between general versus specific deterrence? And what is the role of thresholds in cyber deterrence? Addressing these foundational questions is essential for illuminating the constraints, opportunities, and challenges of implementing a deterrence strategy for cyberspace under different conditions. Below, we explore these issues in greater detail and conclude by providing specific policy recommendations for the United States.

We argue that the question of cyber deterrence is not as simple as ascertaining whether or not it works.

Defining Cyber Deterrence

Cyber deterrence skeptics, such as Harknett and Fischerkeller, make broad claims about the feasibility of cyber deterrence, arguing that "the protection or advancing of national interests cannot rest on deterrence as the central strategy."[15] However, prior to assessing the value of deterrence, clarity around what "cyber deterrence" refers to is essential. There is inconsistency among both academics and practitioners about what precisely the term "cyber deterrence" means. Specifically, use of the term tends to conflate different objects of deterrence, whether a state aims to deter behavior within or outside of cyberspace, and the different means of deterrence including whether the deterrent threat leverages cyber versus non-cyber tools. Typically, when experts use the term "cyber deterrence" they are referring to reciprocal, within-domain deterrence, or the threat of employing cyber capabilities to prevent an adversary from engaging in some unwanted behavior in cyberspace.[16] In practice, however, deterrence in and through cyberspace can take on different combinations across the objective and the means, as illustrated in Table 1.

In practice, however, deterrence in and through cyberspace can take on different combinations across the objective and the means.

Unpacking these different dimensions of cyber deterrence can shed light on which aspects of cyber deterrence are more or less likely to be successful under various conditions and provide leverage in identifying the specific deterrence challenges that may be associated with different forms of cyber deterrence.

Table 1. Unpacking Cyber Deterrence

	Deter behavior in cyberspace	**Deter behavior outside of cyberspace**
Cyber means of deterrence	Within-domain cyber deterrence	The relationship between cyber power and kinetic military capabilities
Non-cyber means of deterrence	Cross-domain cyber deterrence	Traditional deterrence

Within-domain cyber deterrence entails preventing cyberattacks by threatening to employ cyber power and responding with symmetrical capabilities. This could take the form of punishment, such as holding an adversary's power grid at risk through cyber means as a way of preventing a target from conducting some form of cyber behavior with the implied threat to unleash offensive cyber capabilities to disrupt critical infrastructure. However, within-domain cyber deterrence could also take the form of denial, including conducting offensive cyber operations to degrade adversary offensive cyber capabilities and infrastructure to make it harder for them to achieve objectives through cyberspace.[17] Indeed, the language used in the 2018 DoD Cyber Strategy to describe some elements of the implementation of defend forward is largely consistent with this form of cyber deterrence, specifically, those elements of defend forward that involve "disrupt[ing] or halt[ing] malicious cyber activity at its source."[18] An example of this form of deterrence in practice is US Cyber Command's reported cyber campaign in the leadup to the 2018 midterm elections to temporarily disrupt the ability of the Internet Research Agency, a troll farm linked to the Russian government, to carry out cyber-enabled information operations intended to interfere in the elections.[19] These types of operations are aimed at making it more difficult for adversaries to conduct their own offensive cyber operations—a form of denial—rather than threatening to punish adversary populations or economies.

Cross-domain cyber deterrence involves the threat to employ non-cyber capabilities to deter adversaries from conducting malicious behavior in cyberspace. This form of deterrence is typically associated with kinetic military capabilities; that is, the threat to retaliate with conventional force if an adversary conducts a large-scale offensive cyber operation with significant effects. Successive US cyber strategies, with varying degrees of explicitness, relied on this form of deterrence. For example, the 2011 International Strategy for Cyberspace states that the United States "reserve[s] the right to use all necessary means" in response to cyberattacks.[20] Similarly, the 2018 National Cyber Strategy declares that the United States will leverage "all instruments of national power," including "military (both kinetic and cyber)," to respond to cyberattacks.[21] However, cross-domain deterrence could also involve non-military tools, such as issuing indictments and imposing sanctions against individuals or governments conducting malicious cyber activity.[22] Indeed, the bulk of US responses to malicious cyber activity have taken this latter form of cross-domain deterrence.

Less prominent in deterrence debates, but equally important, is the employment of cyber power to achieve deterrence outcomes beyond cyberspace. This application of cyber deterrence could take two forms. First, states could employ cyber operations as a means of deterring the escalation of ongoing international crises—as Benjamin Jensen and Brandon Valeriano have described, operating as an escalatory off-ramp.[23] They argue that the Trump administration's reported decision to conduct a cyberattack against North Korea in 2017 enabled the United States to "demonstrate capability while avoiding escalation."[24] In this sense, demonstrating cyber capabilities during an international crisis as an alternative to other, non-cyber shows of force could act as a cross-domain deterrent signal. This could enable states to manage the delicate dance of conveying resolve while preventing crises from spiraling out of control, but more research is needed to explore the conditions under which this may be more or less risky. The inverse dynamic is also possible, wherein actions that take place in cyberspace could pose a threat to the stability of conventional or nuclear deterrence, given the reliance of technologically advanced militaries on vulnerable digital systems.[25] From a US perspective, there is a real risk that nuclear modernization programs could increase the surface area of attack for malicious cyber activity, and that advanced conventional systems that rely on digital technologies for command and control, precision-targeting, communications, and other core functions could be degraded via cyber means.[26] This could undermine the credibility of conventional and nuclear deterrence postures if there are information asymmetries that lead to a situation in which the cyber-attacker possesses private information about the vulnerabilities of the deterring state's capabilities. It could also, at a more basic level, erode deterrent capabilities by preventing a state from employing a capability at a desired time and with the intended effect.

Therefore, "cyber deterrence" as an umbrella concept in fact contains many different aspects and manifestations of deterrence in practice. And, while the US cyber deterrence posture has appeared across all these forms of deterrence at various times, they are often aggregated to describe US cyber strategy writ large. The reality is that these different permutations of cyber deterrence each pose different types of challenges, limitations, and opportunities. Singular pronouncements of the efficacy (or lack thereof) of deterrence in cyberspace misses these distinctions.

For instance, the primary impediment to successful within-domain cyber deterrence stems from capability limitations, rather than credibility ones. There is abundant evidence that the US government possesses the willingness to use cyber capabilities to respond to adversary cyber capabilities. General Paul Nakasone, Commander of US Cyber Command, testified to Congress in February 2019 on Cyber Command's role in defending the 2018 midterm elections against Russian cyber interference, noting that: "We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts."[27] However, cyber operations lack violent effects. The actual effects are often ephemeral because there are limitations in terms of developing and implementing strategic cyber campaigns at scale and over time. Additionally, offensive cyber operations are characterized by temporal sensitivities, potentially confounding the ability to obtain an intended effect in cyberspace at the desired time. These aspects of offensive cyber operations have prompted scholars to raise doubts about whether even the most capable cyber powers can consistently possess the capability to carry out cyber-based deterrent threats.[28] This is precisely the inverse of the challenge US policymakers faced during the Cold War in the context of nuclear deterrence; the capability to follow through on the threat to employ nuclear weapons was largely uncontested, but the credibility that a decision-maker would actually give such an order was extraordinarily difficult to establish.

This raises the question of whether cyber operations in themselves are sufficient to create costs at a level that would induce an adversary to change its behavior. However, the inherent limitations to the use of cyber power as an independent instrument are not synonymous with pronouncements of deterrence skeptics that it is too difficult to shape behavior in cyberspace.

In a cross-domain context, the threat to respond to cyber incidents with kinetic military force presents the inverse challenge to that of within-domain cyber deterrence: a credibility issue, rather than a capability one. While the US government reserves the right to respond to cyberattacks that cross a key threshold with the full range of retaliatory capabilities, it's unclear whether US adversaries have thus far avoided crossing this threshold because they believe the United States would follow through on this threat, or simply because the geopolitical context has not (yet) given rise to a scenario where this kind of behavior would be relevant.[29] In a relatively stable international system, a crisis has not emerged where the stakes are sufficiently high for states to consider major, large-scale cyberattacks against the United States.

For non-kinetic, cross-domain response measures, the issue is similar to within-domain cyber deterrence. The historical US approach of imposing sanctions, issuing indictments, and conducting other law enforcement actions—let alone the impact of cyber norms initiatives—appears to have had only a marginal effect, if any, on adversary behavior. With respect to international cyber norms, the US government has pursued multilateral norms development efforts through fora such as the United Nations Group of Governmental Experts. While successful on paper, in practice they have been less than effective. The most prominent example of potential success, the 2015 agreement between President Obama and President Xi of China, has been mixed at best and has proven unsustainable over time. The agreement to refrain from conducting cyber-enabled intellectual property theft was made possible by a change in US policy to publicly "name and shame" China for activities in cyberspace as means of bringing China to the bargaining table.[30] However, several years after the agreement was struck, the US government publicly stated that, while there had been a decrease in Chinese-linked cyber-enabled economic espionage, China is "well beyond the bounds today of the agreement that was forged."[31] Similarly, recent efforts by the Biden administration to reign in Russian support of cybercriminal activity, particularly ransomware, by targeting the private sector through leveraging direct diplomatic engagement and other measures, have largely been ineffective.[32]

Taken together, these insights about the limitations of cyber power and other instruments of power leveraged in the absence of a cohesive, integrative national strategy, are precisely what inform the Solarium Commission's strategic concept of layered cyber deterrence. Layered cyber deterrence posits that the synchronization and coordination of different elements of national power—not only cyber power—are essential prerequisites of successful deterrence outcomes.

Layered cyber deterrence posits that the synchronization and coordination of different elements of national power—not only cyber power—are essential prerequisites of successful deterrence outcomes.

Distinguishing Between Specific and General Deterrence

Another complication associated with the use of the term "cyber deterrence" is that it is often used in a general sense to connote preventing all forms of malicious cyber behavior. It is important to distinguish this general form of deterrence, which is quite weak and likely to be ineffective in cyberspace—as it is in most domains—from specific cyber deterrence. Treating deterrence in broad, general terms, agnostic to adversary or strategic context, reflects some of the problems that come with extending the logic of nuclear deterrence to the cyber realm. Given the sheer stakes involved in the use of nuclear weapons—by any actor, under any conditions—promulgating a policy that aims to deter nuclear employment writ large rests on more plausible foundations. General statements about cyber deterrence are common in US strategy documents. For example, the 2018 DoD cyber strategy articulates that the United States will use "all instruments of national power to deter adversaries from conducting malicious cyberspace activity that would threaten US national interests, our allies, or our partners."[33] However, this is not a helpful way of conceptualizing cyber deterrence that should be tailored to the perception and pressure points of a particular adversary, which are almost always likely to vary across targets and over time.

The inherent weakness of vague deterrence statements only serves to confirm the arguments of those who reject cyber deterrence, because it does not help identify the types of levers that could be employed against specific actors to induce their behavior in the desired direction. Moreover, these pressure points may even vary within an adversary state. For instance, in regard to Russia, it's critical to distinguish between Russian-enabled proxy and criminal groups and the actual arms of the Russian state: the Foreign Intelligence Service (SVR), Main Intelligence Directorate (GRU), and Federal Security Service (FSB). These actors vary immensely in terms of capabilities and motivation (particularly distinctions between politically- and profit-motivated groups). Friction among groups within a state could also be exploited for deterrence purposes. For example, Russian security services have ambiguous but symbiotic relationships with criminal organizations, within which the government provides safe haven for cybercriminals as long as they don't turn their capabilities against the state, and sometimes calls on these groups to operate on behalf of the state for the purposes of maintaining plausible deniability.[34] This relationship can sometimes be nebulous and contentious. Hypothetically, the United States could leverage Russia's preference for plausible deniability and its desire to avoid direct confrontation with the United States to take more proactive measures against Russian proxy groups in cyberspace and through other means. The escalation calculus is simply different; in other words, the United States is likely able to take stronger actions with lower escalation risks against Russian proxies than if it were taking direct measures against the Russian government itself. For example, when the Wagner group—a Russian-linked mercenary network—targeted a US outpost in Syria in 2018, the Russian government denied that the attacking forces were linked to Russia and implicitly allowed the United

States to retaliate by calling in air strikes that killed several hundred people, including Russian nationals, without escalating.[35] In other words, Russia has demonstrated that it would rather sacrifice its proxy groups than get drawn into an escalation with the United States.

Therefore, to be effective, cyber deterrence should be made more specific and tailored to the particular target of deterrence. There are a number of parameters to consider: the nature of the target, including its capabilities, motivation, and relationship to adversary governments; the type of target the United States aims to prevent them from attacking, particularly specific elements of critical infrastructure; the specific type of behavior, be it espionage, disruption, or degradation; and temporal factors such as peacetime or crisis. Greater granularity with respect to these will help to illuminate which deterrence levers and combinations of instruments of national power are most likely to be effective.

Therefore, to be effective, cyber deterrence should be made more specific and tailored to the particular target of deterrence.

The Role of Thresholds

Pessimistic pronouncements about the efficacy of cyber deterrence miss the nuances of the empirical record of cyber deterrence at different thresholds. On the one hand, there is a consensus among both cyber deterrence optimists and pessimists that, at the highest thresholds where cyber operations have violent, physical effects, deterrence appears to be holding (noting the caveats discussed above). However, as Harknett and Fischerkeller note, the real deterrence challenge exists below that threshold because most of the damage resulting from cyber operations does not rise to a level of "use of force." In their parlance, "[s]uch damage is of a very different nature and not representative of the significant damage being caused by on-going espionage, sabotage, and subversion."[36]

Pessimistic pronouncements about the efficacy of cyber deterrence miss the nuances of the empirical record of cyber deterrence at different thresholds.

The problem with this approach is that it aggregates the full scope of malicious cyber activity that takes place below a use of force threshold as being analogous and equally un-deterrable. However, as Jacquelyn Schneider has argued, further disaggregating cyber activities below a "use of force" threshold is important for identifying which forms of cyber behavior may be more receptive to a deterrence approach, and which areas are outside of the scope of deterrence frameworks.[37] In particular, with respect to the proliferation of cyber espionage, which Harknett and Fischekeller accurately point to as comprising much of the "malicious" behavior in cyberspace, deterrence is an inappropriate strategic framework. That is why, in part, many experts balked at policymakers' depictions of the SolarWinds breach, discovered in December 2020, as equivalent to an act of war.[38] Given that all states implicitly accept that espionage, whether conducted through cyber or conventional means, is a necessary state practice, it makes little sense to attempt to deter this kind of behavior. Thus, applying deterrence frameworks at very low thresholds like cyber espionage is likely to be counterproductive. Additionally, this distracts from specific types of behavior that do not amount to a use of force but are above the level of espionage where states may be able to shape adversary behavior with deterrence frameworks. Additional policy work needs to be done to define more critical points and distinctions beyond the use of force threshold and to accept those areas where deterrence is in fact not the right framework, such as espionage for national security purposes.

Policy Implications

This analysis gives rise to a number of policy implications for the United States. First, US strategy should be updated to reflect these more nuanced understandings of cyber deterrence at a fundamental level. While deterrence has anchored the US approach to cyberspace for decades, there has not been sufficient progress in moving beyond broad conceptualizations of deterrence and toward more specific and tailored applications of the various combinations of instruments of national power.

First, US strategy should be updated to reflect these more nuanced understandings of cyber deterrence at a fundamental level.

Second, as the Solarium Commission recommended in its March 2020 report, the US government urgently needs to improve how it signals and communicates to adversaries and other audiences about its cyberspace capabilities and intent. While the current (albeit vague) declaratory policy appears to be working with respect to deterring cyber behavior that crosses a use of force threshold, there is room for the United States to more clearly communicate what behavior would cross specific lines and the range of potential responses. Moreover, greater clarity on distinctions between acceptable versus unacceptable behavior below that threshold, and the types of costs that the United States would consider leveraging in response, is essential. The United States cannot assume that simply by way of acting in cyberspace through a process of tacit bargaining that adversaries will understand US intent, particularly since there are mismatches between perceptions of red lines and the meaning behind observed behavior. In other words, there are likely significant differences in how adversaries define what constitutes acceptable behavior even in a context of tacit bargaining.

Additionally, more work needs to be done on the impact of cyber operations on deterrence beyond cyberspace. While there have been some reports in the media about the United States choosing to conduct cyber operations to deter crisis escalation instead of more forceful measures, it's not clear the extent to which this is a systematic strategy. Yet, this use of cyber capabilities may be one of the more fruitful applications of cyber power. With respect to cyber threats to conventional and nuclear deterrence, enhancing the security and resilience of these weapon systems to cyber threats should be a central priority for policymakers given the potential for asymmetric threats to erode full-spectrum deterrence capabilities.

Third, the United States must continue to work to lower the bar to conduct routine cyber operations, as creating speed and agility in execution is a strong signal of willingness to use. The FY2019 National Defense Authorization Act designated cyber reconnaissance and surveillance as a traditional military activity. This designation provided increased authority for the military to use offensive cyber operations in campaign planning and responses to adversary activities. The Trump administration subsequently produced National Security Presidential Memorandum 13, which purportedly created a streamlined process for the development and approval of cyber campaign plans. This was reportedly an essential element of US success in preventing Russian cyber-enabled information operations efforts in both the 2018 and 2020 US elections.[39] Maintaining, or even improving the speed of planning execution—often the most critical element in offensive cyber operations—can also send a strong signal to the adversary.

Maintaining, or even improving the speed of planning execution—often the most critical element in offensive cyber operations—can also send a strong signal to the adversary.

Fourth, the US government should continue to improve the effectiveness and speed of non-military cost imposition tools, such as sanctions and law enforcement options. In particular, the speed of application should be shortened from months and years to days and weeks. By way of example, indicting North Korean officials four and seven years after the Sony hack has no strategic impact.

Finally, these policy recommendations require the involvement of allies and partners. To a much greater degree than any other form of warfare, cyberattacks utilize third party assets, sovereign territory, and even personnel in a way that make unilateral responses inherently more difficult. The United States must consistently identify allies and partners who are willing to work closely with the United States to establish rules of behavior, systems for identifying unacceptable rules of behavior, methods for rapidly sharing that information, and tools for responding. This goal will be challenging, but the deterrent effect of an informed, responsive, and impactful multilateral response to malicious cyber activity will be significant.

Notes

[1] Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security,* (Princeton, NJ: Princeton University Press, 1961), 9; Lawrence Freedman, *Deterrence* (Cambridge, UK: Polity,

2004), 26; Robert J. Art, "To What Ends Military Power?," *International Security* 4, no. 4 (1980): 3–35.

[2] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2016): 44–71: John J. Mearsheimer, *Conventional Deterrence,* (Ithaca, NY: Cornell University Press, 1985): 14–15.

[3] John J. Mearsheimer, "Nuclear Weapons and Deterrence in Europe," *International Security* 9, no. 3 (1984): 21.

[4] In this article, we focus on cyber deterrence between states or their non-state proxies. The challenges of cyber deterrence are compounded when the target of deterrence is a non-state actor, such as a terrorist organization, that is not operating on behalf of a state.

[5] See, for example, Martin Libicki, *Cyberdeterrence and Cyberwar,* (Santa Monica: RAND Corporation, 2009); Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (Washington, D.C.: National Defense University Press, 2009); Emily O. Goldman and John Arquilla, *Cyber Analogies* (Monterey, CA: Naval Postgraduate School, 2014); Ben Buchanan, *The Cybersecuritiy Dilemma: Hacking, Trust, and Fear Between Nations,* (New York, NY: Oxford University Press, 2016).

[6] Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017); John Arquilla and David Ronfeldt, "Cyberwar is Coming," *Comparative Strategy* 12, no. 2 (1993): 141–165; Also see Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (2013): 41–73; Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32; Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*, (New York, NY: Oxford University Press, 2018).

[7] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37; Libicki, *Cyber Deterrence and Cyberwar;* On signaling, see Valeriano et al., *Cyber Strategy*, which discusses cyber operations as ambiguous signals. On offense versus defense, see Rebecca Slayton.

[8] Erica D. Borghard and Shawn Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452–481.

[9] Michael Fischerkeller and Richard Harknett, "Deterrence is Not a Credible Strategy," *Orbis* 61, no. 3 (2017): 382.

[10] Fisherkeller and Harknett, "Deterrence is Not a Credible Strategy," 388.

[11] Michael P. Fischerkeller, "Persistent Engagement and Tacit Bargaining: A Strategic Framework for Norms Development in Cyberspace's Agreed Competition," *Institute for Defense Analysis,* (November 2018).

[12] Department of Defense, *2018 and 2015 Department of Defense Cyber Strategies*, (2015 & 2018)

[13] Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report,* (2020): 24.

[14] Nye, "Deterrence and Dissuasion in Cyberspace;" 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, (New York, NY: Oxford University Press, 2019); Jon Lindsay et al, "Cybersecurity and Cross-Domain Deterrence: The Consequences of Complexity," *Journal of Cybersecurity* 1, no. 1 (2015): 53–67; Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–348; Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies* (2021); Mark Montgomery and Erica Borghard, "Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence," *Joint Force Quarterly* 102 (2021).

[15] Harknett and Fischerkeller, "Deterrence is Not a Credible Strategy," 382.

[16] For further reference, please see Aaron F. Brantly, "The Cyber Deterrence Problem," *2018 10th International Conference on Cyber Conflict (CyCon),* IEEE, (2018): 31–54; and Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Forces Quarterly* 77, no. 2 (2015): 8–15.

[17] Borghard and Lonergan, "Deterrence by Denial in Cyberspace."

[18] Department of Defense, *Cyber Strategy,* (2018): 1.

[19] Michael Wines and Julian E. Barnes, "How the U.S. is Fighting Russian Election Interference," *The New York Times*, August 2, 2018; Patricia Zengerle and Doina Chiacu, "U.S. 2018 Elections 'Under Attack' by Russia: U.S. Intelligence Chief," *Reuters*, February 13, 2018.

[20] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, (May 2011): 14.
[21] The White House, *National Cyber Strategy of the United States of America*, (September 2018): 21.
[22] Tim Maurer and Garrett Hinck, "Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity," *Journal of National Security Law and Policy* 10, no. 3 (January 2020): 525–561.
[23] Benjamin Jensen and Brandon Valeriano, "What Do We Know About Cyber Escalation? Observations from Simulations and Surveys," *The Atlantic Council* (November 2019).
[24] Benjamin Jensen and Brandon Valeriano, "The Myth of the Cyber Offense," Cato Institute Policy Analysis no. 862 (2019): 2.
[25] Montgomery and Borghard, "Cyber Threats and Vulnerabilities."
[26] Erik Gartzke and Jon Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3, no. 1 (2017): 2–12.
[27] "Statement of General Paul M. Nakasone, Commander, United States Cyber Command, Before the Senate Committee on Armed Services," (February 14, 2019), 4.
[28] Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-based Logics," *Journal of Cybersecurity* 5, no. 1 (2019); Erica Borghard and Shawn Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* 13, no. 3 (2019): 122–145; Max Smeets, "A Matter of Time: On the Transitory Nature of Cyber Weapons," *Journal of Strategic Studies* 41, no. 1 (2017): 6–32; Henry Farrell and Charles Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine," *Journal of Cybersecurity* 3, no. 1 (2017): 7–17.
[29] Jason Healey and Robert Jervis make a similar point in their discussion of the implications of persistent engagement. See Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review* 3, no. 4 (Fall 2020): 31–53.
[30] Julie Hirschfeld Davis and David E. Sanger, "Obama and Xi Jinping of China Agree to Steps on Cybertheft," *The New York Times*, September 25, 2015.
[31] "U.S. Accuses China of Violating Bilateral Anti-Hacking Deal," *Reuters*, November 8, 2018.
[32] Maggie Miller, "Top FBI Official Says There is 'No Indication' Russia Has Taken Action Against Hackers," *The Hill*, September 14, 2021, https://thehill.com/policy/cybersecurity/572184-top-fbi-official-says-there-is-no-indication-russia-has-taken-action.
[33] Department of Defense, *Cyber Strategy,* (2018).
[34] Janne Hakala and Jazlyn Melnychuk, "Russia's Strategy in Cyberspace," *NATO Strategic Communications Centre of Excellence* (June 2021).
[35] Thomas Gibbons-Neff, "How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria," *The New York Times*, May 24, 2018, https://www.nytimes.com/2018/05/24/world/middleeast/american-commandos-russian-mercenaries-syria.html.
[36] Harknett and Fischerkeller, "Deterrence is Not a Credible Strategy," 386.
[37] Jacquelyn Schneider, "The Cyberspace Solarium Commission: From Competing to Complementary Strategies," *Lawfare Blog*, April 1, 2020, https://www.lawfareblog.com/cyberspace-solarium-commission-competing-complementary-strategies.
[38] Erica Borghard and Jacquelyn Schneider, "Russia's Hack Wasn't Cyberwar. That Complicates US Strategy," *WIRED*, December 17, 2020, https://www.wired.com/story/russia-solarwinds-hack-wasnt-cyberwar-us-strategy/.
[39] Ellen Nakashima, "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries," *The Washington Post*, September 20, 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html; "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," U.S. Department of Defense, March 2, 2020, https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.