To Defend Forward, US Cyber Strategy Demands a Cohesive Vision *for Information Operations*

The Honorable Patrick J. Murphy
Dr. Erica Borghard

INTRODUCTION

In 2018, the United States (US) Department of Defense (DoD) published the 2018 Cyber Strategy summary featuring a new strategic concept for the cyber domain: defend forward. It states DoD will, "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[1] This reflects an important shift in DoD's strategic posture, compared to the 2015 Cyber Strategy, in two key ways.[2] First, defend forward rests on the premise that to deter and defeat adversary threats to national security, the US could not solely rely on responding to malicious behavior after the fact. Rather, the DoD should be proactive in maneuvering outside of US cyberspace to observe and understand evolving adversary organizations and, when authorized, conduct operations to disrupt, deny, or degrade their capabilities and infrastructure before they reach the intended targets. Implied, but not explicitly stated, in the 2018 strategy summary is the role of information operations, and the relationship between cyberspace and the information environment. According to US doctrine, the former is a subset of the latter.[3] This article builds on our work as members of the US Cyberspace Solarium Commission to offer a conceptual framework and policy recommendations for integrating information operations in the context of defend forward. Many of the Commission's 82 recommendations are slated to pass in the Fiscal Year 2021 National Defense Authorization Act (NDAA).

Although the field of information warfare and information operations is not new, there has been a recent resurgence in academic and practitioner interest within the US on the relationship between the information environment and cyberspace operations.[4]

The Honorable Patrick J. Murphy is America's first Iraq War veteran elected to the U.S. Congress and later served as the 32nd Under Secretary of the Army until January 2017. Secretary Murphy is currently a Senior Managing Director at Ankura, the Distinguished Chair of Innovation at the United States Military Academy at West Point, and a Commissioner on the U.S. Cyberspace Solarium Commission. Patrick serves as a director on several public and private-held companies and is a graduate of King's College Army ROTC Program and the Widener University Commonwealth School of Law. He has two young children, Maggie and Jack, and they reside in Pennsylvania.

In particular, Russia's use of cyber-enabled information operations to interfere in the 2016 US Presidential election, foment social strife, and undermine public faith in democratic institutions was a key event that shaped the framing of these more recent discussions.[5] Much of the conversation has rightly centered on (a) how the US can better defend itself and thwart such behavior in the future;[6] (b) concerns about how other adversaries and competitors, such as China,[7] may be taking a page out of Russian President Vladimir Putin's playbook; and (c) critiques of the US tendency—potentially stemming from differences in American and Russian strategic culture—to neglect the information environment. Arguably, the DoD is ahead of other departments and agencies within the Federal government and is best positioned in terms of resources, planning, and conceptualizing the optimal role of information operations in military strategy in general, and in cyberspace in particular.[8] For example, Army Cyber Command (ARCYBER) is pursuing an initiative to integrate information, electronic, and cyber warfare capabilities and has even considered changing the command's name to Army Information Warfare Operations Command.[9] Moreover, at the 2018 Cyberspace Strategy Symposium, U.S. Cyber Command (USCYBERCOM) grappled with the implications of "[s]ynchronizing and coordinating information-related capabilities together in a coherent strategy,...[to integrate] IO [information operations] and cyberspace capabilities."[10]

From a grand strategy perspective, it is imperative that the US considers how best to employ and integrate the full range of diplomacy, information, military, and economic instruments of power in furtherance of national objectives.[11] As to strategic objectives in cyberspace more specifically, the Fiscal Year 2019 NDAA established the Cyberspace Solarium Commission to develop a comprehensive strategy to defend the US against cyberattacks of significant consequences, as well as to promulgate a set of policies and legislation that would be required to implement the strategy.

Dr. Erica Borghard is a Senior Fellow in the Scowcroft Center's New American Engagement Initiative at the Atlantic Council. She is also a Senior Director on the Cyberspace Solarium Commission. Prior to that, Dr. Borghard was an Assistant Professor in the Army Cyber Institute. Previously, she was a Council on Foreign Relations International Affairs Fellow, with placement at JPMorgan Chase and U.S. Cyber Command. Dr. Borghard 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 received her Ph.D. in Political Science from Columbia University. Dr. Borghard has published in numerous academic journals and policy outlets on topics ranging from cyber policy to grand strategy. Dr. Borghard is a term member at the Council on Foreign Relations and a Research Fellow at the Saltzman Institute of War and Peace Studies at Columbia University.

Comprised of fourteen commissioners, including members of Congress, senior leaders in the executive branch, and subject matter experts from academia and the private sector, the Commission organized itself into three task forces to investigate distinct strategic approach for cyberspace—deterrence through active disruption and cost imposition; denial and resilience; and entanglement and norms—as well as a fourth directorate to explore cross-cutting issues. Following a rigorous research process that included interviews with subject-matter experts (SMEs), domestic and international engagements, a series of red team analyses, a multi-stakeholder simulation, and quantitative analysis, the Commission produced a report in March 2020 unveiling a novel strategic approach and recommendations.

Specifically, the Commission advocates for a strategy of layered cyber deterrence.[12] Rather than rejecting cyber deterrence, the Commission updates the concept for the modern era. Specifically, the Commission Report urges the US to adopt a whole-of-nation approach to deter malign behavior and cohesively leverage the full range of instruments of national power. Layered cyber deterrence also posits that the range of deterrence tools, such as promoting international norms to shape behavior, improving domestic defense and resilience, and imposing costs on adversaries for engaging in malicious behavior in cyberspace, have varying utilities in different strategic contexts against different types of threat actors. In particular, the Commission Report distinguishes between the deterrence challenges associated with preventing cyber-attacks above the level of war, versus those aimed at reducing the magnitude and frequency of malicious cyber campaigns below that threshold. Furthermore, defend forward is a key aspect of the Commission's strategy of layered cyber deterrence. The decision to feature defend forward as a core component of the Report's strategic approach reflects the Commission's mindset that the US should be more

proactive and biased toward action to address adversary threats in cyberspace.

Consistent with its statutory mandate, the Commission Report extensively addressed strategic challenges in cyberspace. However, one area with important implications for the cyber domain and for the implementation of the Commission's strategy and recommendations is the nexus of cyberspace and the information environment. Therefore, in this article we build on the Commission's strategy and recommendations to more fulsomely address how the US can improve its strategic approach in two respects as to the information domain.[13] First, the Commission Report makes the point that information operations should be incorporated into defend forward. Put simply, the US needs to be more proactive in thinking about the strategic employment of information operations. In this article, we lay out the strategic thinking that went behind this recommendation and explore how the US should conceptualize coupling cyber and information operations to shape adversary perceptions and, by extension, behavior, particularly below the level of armed conflict. More specifically, we provide a framework to guide strategic thought and policymaking on employing information operations as part of the defend forward strategy in cyberspace. Importantly, while the notion of being proactive—owning the narrative and deliberately using information for clearly defined purposes—is not inherently controversial, who "owns" this mission is not without controversy because there are many stakeholders with an interest in this space.

Second, this article also goes beyond the boundaries of the Commission's recommendations to urge that, in addition to incorporating information operations into defend forward, the US should consider developing a coherent approach to revitalizing the role of information as part of a national cyber strategy more broadly. While outside of the statutory scope of the Cyberspace Solarium Commission's mandate, this is a natural extension of the Commission's work and strategic vision. Therefore, we also explore how to extend the spirit of the Commission's recommendations to address ways the US can more strategically leverage information beyond the military instrument of power.

It is also important to note that the Commission's March 2020 Report delves into several recommendations to shore up domestic defenses against influence operations. Strengthening the ability of American society to better defend itself against adversary information operations is a critical task to preserve American democracy. Specific Commission Report recommendations that address this concern include advocating for programs that promote digital literacy, civics education, and public awareness at the societal level to inoculate the American public against foreign malign influence campaigns.[14] The Report also recommends defense of the US election system against adversary information operations, including improving the structure of and increasing resourcing for the Election Assistance Commission and promoting voter-verifiable, auditable, paper ballots.[15]

INCORPORATING INFORMATION OPERATIONS INTO DEFEND FORWARD

Beyond domestic defense, information operations also played an essential role in how the Commission addressed implementing the defend forward concept in cyberspace to favorably influence adversary behavior. The concept of defend forward was introduced in the 2018 DoD Cyber Strategy, which posits that DoD will "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[16] It entails maneuvering where adversaries operate, sharing information with partners to enable their own defensive efforts, and, when authorized, delivering effects to disrupt, deny, and degrade adversary capabilities, infrastructure, and operations. Recognizing that defend forward is central to US cyber strategy, particularly in a context of strategic competition below the level of war, a key Cyberspace Solarium Commission recommendation is that the Executive Branch should issue an updated National Cyber Strategy to include defend forward as a key element.[17] Notably, the 2018 National Cyber Strategy lacks any reference to defend forward, even though this concept is the driving principle behind how DoD conceptualizes the nature of the strategic challenge in cyberspace, and how US military cyber forces should be organized and employed to counter adversary threats.[18]

Additionally, the Commission recommends that the defend forward concept should be expanded to encompass all of the instruments of national power—to include information as an instrument of power.[19] This concept is not explicitly discussed in the 2018 DoD Cyber Strategy summary or statements by leaders. Yet, the Commission recognized that the strategic employment of information is intertwined with conducting cyberspace operations to influence adversary decision-making and behavior.[20] Shaping behavior implicitly rests on affecting an adversary's perception of the strategic environment. Given this objective, integrating information operations into defend forward can assist in accomplishing the strategy's desired end state.

In Joint Publication 3-13, DoD defines information operations as "the integrated employment, during military operations, of IRCs [information-related capabilities] in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own."[21] The immediate locus of information operations is the mind of the adversary, although the ultimate objective is to manipulate adversary behavior in a desired direction. As Dr. Herbert Lin and Dr. Jaclyn Kerr describe, information warfare and influence operations entail "the deliberate use of information by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes."[22] Accordingly, "[t]he targets...are the adversary's perceptions, which reside in the cognitive dimension of the information environment," while the objective is to "[use] words and images to persuade, inform, mislead, and deceive so that the adversary does not use the (fully operational) military assets it does have, and the military outcome is the same as if those military assets had been destroyed."[23]

Importantly, we are not suggesting that the US government should replicate adversary campaigns that use cyberspace to conduct widespread disinformation against civilian populations.[24] To do so would be inconsistent with democratic values, especially when these types of campaigns take place outside of a context of active hostilities or conflict. Instead, we posit that *tailored* information operations conducted in conjunction with cyber operations against defined adversary military entities could enhance the effects of defend forward campaigns. Essentially, rather than conducting cyber-enabled information operations similar to those of US adversaries, in which disinformation is the objective and cyberspace is only one medium through which to achieve it, the US should consider how it could conduct "information-enabled cyber operations"—leveraging information to support the operational and strategic objectives of defend forward.

There are two notable examples of publicly disclosed efforts by the US to explore the nexus between cyber operations and the information space at the operational level. However, these have been almost wholly focused on employing cyber capabilities to disrupt adversary information activities—rather than integrating information into cyber capabilities for the purposes of shaping adversary behavior. The first, Operation GLOWING SYMPHONY in 2016, entailed countering the social media activities of the self-proclaimed Islamic State of Iraq and the Levant (ISIL).[25] In this example, cyber operations were reportedly used to undermine the adversary's ability to leverage social media to recruit, to spread propaganda, and for command and control purposes, specifically to "find and destroy the key nodes in ISIS online infrastructure and media operations."[26] Then-Deputy Secretary of Defense Robert Work described this effort as "dropping cyberbombs."[27] In the second example, in 2018 USCYBERCOM—replicating the task force model of the counter-ISIL campaign—worked with interagency partners to form the Russia Small Group. Among other measures, USCYBERCOM reportedly conducted cyber operations to disrupt adversary information operations targeting the 2018 midterm elections.[28] While these represent important efforts, the US should consider how it can move beyond cyber responses to adversary use of the information environment. Specifically, the US should improve its ability to incorporate information operations into cyber campaigns. This would require further maturation of thought about how to incorporate such operations into the defend forward strategic framework, and appropriate capabilities, authorities, and processes to enable its deliberate implementation at scale across multiple campaign plans.

STRATEGIC FRAMEWORK

Defend forward aims to address a central challenge for the US in cyberspace: how to change adversary behavior in cyberspace short of war to produce a more favorable status quo while mitigating potential escalation risks.[29] An improved status quo would be one in which the magnitude and effects of adversary campaigns targeting the US political system, critical infrastructure, and military capabilities are reduced. In the immediate term, defend forward

endeavors to do this by reducing the effectiveness and/or increasing the costs of adversary operations. Over time, the cumulative effect of defend forward operations and campaigns, in theory, is hypothesized to shift the adversary's perception of the environment; assessments of the relative costs, benefits, and risks of conducting malicious campaigns; and calculations about the likelihood of success, ultimately driving adversaries to divert resources to other efforts and reduce undesirable activities.

Conducting cyber operations to disrupt, deny, and degrade adversary operations and campaigns (which include, for example, their offensive cyber capabilities, infrastructure, and command and control) is a centerpiece of defend forward.[30] As a form of denial, these operations are directed at adversary offensive capabilities and strategies, and not at the broader civilian population.[31] However, given that the purpose of these operations is to affect an adversary's decision calculus, there is an opportunity for information operations—which, by definition, are directed at a target's perception—in tandem with cyber operations to enhance the latter's effects. Information operations that are aimed at shaping an adversary's decision calculus may be especially useful when conducted parallel to, or in support of, cyber operations. This is because academic research has demonstrated that cyber operations, in themselves, present challenges for discerning the intent behind them and, in some instances, may not always be immediately observed and understood by the intended target.[32]

US adversaries are conducting strategic cyber campaigns to subvert US interests, such as China's campaigns to steal intellectual property at scale from the defense industrial base and broader economy or Russia's campaigns to undermine US and other democratic elections.[33] These are not simple, one-off operations. Rather, they are long-term campaigns that rely on multiple organizations and entities within adversary military and intelligence services, as well as proxy groups.[34] Within the Russian government, for example, both its military and foreign intelligence (GRU and SVR) and internal state security (FSB) organizations are known to conduct cyber operations, in addition to external entities such as the Internet Research Agency that are affiliated with the government.[35] Successfully planning and conducting long-term cyber campaigns require some level of bureaucratic maturity and an organizational apparatus to support them.[36] Of particular concern, detailed in the recent DoD report, *Military and Security Development Involving the People's Republic of China*, is the threat posed by the Chinese Communist Party's (CCP) incorporation of cyberspace and information operations into its broader military strategy, specifically through its Military-Civilian Fusion (MCF) Development Strategy and its Strategic Support Forces (SSF).[37] China's investment in its warfighting capability and capacity is real and growing. Additionally, its continued cyber-enabled theft of American intellectual property at scale; the collection of personal data of hundreds of millions of Americans; and the development of information operations capabilities are essential to China's "whole of country" economic and military strategy. In this sense, it represents a greater threat to the US and its allies and partners than Russia.

In countering adversary cyber campaigns, cyber operations represent one element of this effort. However, beyond disrupting, denying, and degrading adversary cyber capabilities and operations via cyber means, information operations can have several complementary effects at various levels of analysis. At the strategic level, they can shape the adversary's perception of the environment. This would entail conducting information operations that target the broader military and intelligence agencies which provide the organizational capacity to carry out cyber campaigns, the locus of decision-making within the government, and the proxy groups that are known to operate on their behalf. These could be conducted for purposes such as peeling away critical stakeholders within the adversary's national security apparatus, generating competition or friction among different elements of the military or intelligence services, or otherwise undermining the bureaucratic politics that play out among governmental entities.[38]

At the operational level, information operations could be conducted to affect the command and control capabilities required to execute operations. This is particularly salient with respect to the proxy organizations that adversary governments rely on for cyber operations, because these often already depend on ambiguous command and control relationships and plausible deniability.[39] Finally, at the tactical level, information operations could influence the willingness of individual operatives to carry out their missions. For instance, these operations could be crafted to introduce uncertainty among operatives that they can continue to execute missions without admonishment or consequences, undermining their resolve. These operations could work even if they only produce shirking behavior, rather than defection (e.g., timeliness in following orders, willingness to carry out a specific objective, etc.). Because effects in cyberspace are difficult to observe and uncertain, the absence of a successful outcome could be blamed on the environment, rather than on an individual operator's propensity to shirk. In the aggregate, this could have strategic effects. Taken together across the strategic, operational, and tactical levels, coupling information operations with cyber operations can reduce adversary cyber capabilities writ large.

IMPLEMENTATION

The Cyberspace Solarium Commission Report recommends several specific authorities, capabilities, and processes that will improve USCYBERCOM's ability to integrate information operations in support of defend forward. Specifically, there are three recommendations essential for effective implementation. First, as part of DoD's next Cyber Posture Review, the Commission urges Congress to request analysis of the extent to which Title 10 cyber-related authorities should be further delegated down to USCYBERCOM.[40] In particular, the Report identifies authorities pertaining to "information operations (IO), which include authorities to create, procure, and deploy personas; military information support operations (MISO); military deception (MILDEC); and counterintelligence."[41] This would enable a rapid, cohesive, and seamless implementation of information operations against defined adversaries as part of approved cyber campaign plans. Section 1642 of the FY2019 NDAA stipulates that, if the

National Command Authority determines that Russia, China, Iran, and/or North Korea are engaged in "an active, systemic, and ongoing campaign of attacks...in cyberspace," then the Secretary of Defense, acting through the Commander of USCYBERCOM, may "take appropriate and proportionate action in foreign cyberspace to disrupt, defeat, and deter such attacks...to conduct cyber operations and information operations as traditional military activity."[42] DoD should assess the conditions under which these Secretary-level authorities should be delegated to USCYBERCOM to reduce the overall friction and aid in rapid execution of such cyber and information operations.

There are, of course, potential functional concerns with delegating certain types of information-related authorities to USCYBERCOM. For example, MISO (formerly Psychological Operations, or PSYOP) is currently defined as a core activity of U.S. Special Operations Command (USSOCOM).[43] This potentially means that content generated for proactive messaging would be implemented by USSOCOM personnel, even when cyberspace is the mechanism for delivering the message (versus, for instance, dropping leaflets from an aircraft). Additionally, there are important geographic concerns that should be considered. These operations seek to influence a target audience outside of cyberspace—actual human beings—into making a decision consistent with US objectives. This takes places in the physical world, in some geographic location. Therefore, regardless of which entity may produce the content (e.g., USSOCOM) or deliver it (e.g., USCYBERCOM), the message is ultimately targeting individuals in a geographic combatant command's area of responsibility. This adds an additional stakeholder involved in signing off on a single operation. Multiple combatant command approval of a given operation can create implementation challenges.

Therefore, this Commission recommendation seeks to streamline this process and reduce the friction—within defined circumstances and considering appropriate limits and restrictions—to enable USCYBERCOM to more proactively implement cyber campaigns as part of defend forward. Accepting this recommendation would empower DoD to weigh competing concerns of relevant stakeholders, including geographic and functional combatant commands. This recommendation seeks not to delegate information warfare authorities to USCYBERCOM writ large, but rather, to urge DoD to assess how it can improve and streamline decision-making processes to enable USCYBERCOM to better meet the strategic objectives of defend forward.

Beyond authorities, the Commission recommends DoD to consider the appropriate size, organization, resourcing, and manning of the Cyber Mission Forces (CMF) for the plethora of missions it supports. Specifically, the Commission recommends that Congress direct DoD to conduct a force structure assessment of the CMF, which is at the core of USCYBERCOM's operational capability.[44] As part of this assessment, the Commission urges evaluation of the requirements these missions create for relevant intelligence agencies in their combat support agency roles.[45] Additionally, for information operations to be incorporated into defend forward cyber campaigns, organizational and personnel requirements should be part of that force

structure assessment. For instance, information operations should be deliberately included in the campaign planning process, which would require increasing the planning staff within USCYBERCOM and relevant supporting commands. With regard to the Intelligence Community, there are additional requirements to provide strategic and tactical intelligence support to cyber campaigns—such as identifying centers of gravity, adversarial weak points, and other targetable entities to influence—that should also be assessed. Senior leaders have acknowledged there is room for improvement in this area. For instance, Admiral Michael Rogers, then-Commander of USCYBERCOM, testified in a 2017 House Armed Services Committee hearing that conducting information operations "is not right now in our defined set of responsibilities per se." He also noted the personnel shortage that has persisted since the end of the Cold War, stating that "[m]any of the individuals who had the skill sets are no longer with us.... I would be the first to admit it is not what our workforce is optimized for."[46]

Finally, the Commission urges Congress to create a Major Force Program (MFP) funding category for USCYBERCOM to enable it to acquire cyber-peculiar goods and services.[47] Congress granted limited acquisition authorities in the FY2016 NDAA to USCYBERCOM totaling $75 million, which sunset in December 2021.[48] However, a true MFP for USCYBERCOM would enable it to rapidly acquire the technical capabilities or requisite talent to conduct information operations (such as seasoned, credible personas) that are critically needed by operational enablers.

US policymakers should consider domestic and international issues in implementing these recommendations. First, from a domestic perspective, given that public trust in government institutions is at a historical low, it is important for policymakers to consider how to communicate with the American people about the military's role in these efforts. Recently, the government has taken positive steps to improve the transparency associated with cyber operations. While considering operational security, engaging the American people is essential to preserve public trust in the military. From an international perspective, perhaps the most significant comparative advantage the US enjoys relative to its adversaries is its deep and enduring constellation of allies and partners. The US should take care that, as it strives to improve its capabilities and processes to fully implement defend forward, it redoubles outreach efforts to allies and partners to (a) strengthen consensus on a shared vision for the defense of cyberspace, (b) clearly distinguish between acceptable and unacceptable behavior in cyberspace, and (c) collaborate whenever possible to achieve operational and strategic objectives.

LOOKING AHEAD

With the release of the Commission report and its consideration by Congress, the US is at a moment of strategic opportunity to capitalize on these efforts and significantly bolster its ability to counter adversary cyber campaigns. The Commission's findings also coincide with parallel DoD efforts to conceptualize and operationalize links between the cyber and information

environments. As the Commission's recommendations make their way into legislation, and as assessments and studies derived from the Commission Report surface, follow-up actions should be taken to ensure the successful, efficient implementation of defend forward, including integrating information operations into cyber campaigns.

Additionally, Congress should also consider how to extend the contributions of the Commission beyond the more tightly-scoped challenge of developing a strategy to defend the US in cyberspace. One core insight of the Commission's report, drawing inspiration from the Eisenhower Administration's original Project Solarium to develop a grand strategy to deter the Soviet Union, is that a single instrument of national power, in isolation, is insufficient to have decisive and sustainable strategic effects.[49] A consequence, likely unintended, of post-9/11 US strategy has been a preponderant focus on military solutions to address a diverse range of foreign policy challenges.[50] The Commission urged that policymakers should be wary of always turning to the military instrument of power. While crucially important, military capabilities hardly address the full scope of cybersecurity challenges.

There are further parallels between the Commission's efforts and the Eisenhower Administration's approach to Cold War grand strategy. In June 1953, six months before conducting Project Solarium, Eisenhower established the President's Committee on International Information Activities, also known as the Jackson Committee, to develop policies pertaining to the role of information and propaganda in US national security. Ultimately, the Committee's findings played a significant role in driving US grand strategy during the Cold War.[51] One important Committee outcome was establishment via Executive Order 10477 of the U.S. Information Agency (USIA) in 1953. USIA was the principal vehicle for US information and propaganda efforts during the Cold War, but was abolished in the Foreign Affairs Reform and Restructuring Act of 1998.[52]

Currently, there is no comparable, independent entity leading a US government information strategy. The State Department has a natural leadership role in this space. As the US seeks to be more proactive in defending forward against adversarial threats—to include information operations—diplomatic efforts must drive engagement. Of note, the Global Engagement Center (GEC) within the State Department, initially created in 2016 to coordinate US government communications to counter terrorist messaging and information campaigns, was given a broader mandate and increased funding in the FY2017 NDAA.[53] The 2017 NDAA defined its role as to "synchronize, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national security interests."[54] Within DoD, a Principal Information Operations Advisor exists to "coordinate and deconflict its operations with the GEC, who is the lead."[55] However, it is unclear whether the GEC is sufficiently staffed or resourced to accomplish this important mission.[56] Moreover, a 2018 staff report prepared for the Senate Committee on Foreign Relations on Russia's information operations noted that, within the

GEC, "operations have been stymied by the Department's hiring freeze and unnecessarily long delays by its senior leadership in transferring authorized funds to the office."[57]

Given our nation's vulnerabilities posed by the ongoing weaponization of information by US adversaries, it is imperative that Congress and the executive branch take a bold stance toward not only implementing the recommendations in the Cyberspace Solarium Commission but also think more broadly about a whole-of-nation effort to promote US interests and values in the information space. While resurrecting a Cold War agency such as the USIA, or further empowering the GEC are not perfect solutions, the essential question of the role of information as an instrument of power in US grand strategy and the appropriate locus of these efforts within the executive branch are issues that Congress should not shy away from addressing.

NOTES

1. "Summary: Department of Defense Cyber Strategy," *U.S. Department of Defense*, January 2018, 1.
2. "The Department of Defense Cyber Strategy," *U.S. Department of Defense*, April 2015.
3. "Joint Publication 3-12: Cyberspace Operations," June 8, 2018, viii-ix.
4. For examples of early work, see John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica, CA: RAND Corporation, 1997); Richard Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (1996): 93-107.
5. David V. Gioe, "Cyber Operations and Useful Fools: The Approach of Russian Hybrid Intelligence," *Intelligence and National Security* 33, no. 7: 954-973.
6. Shawn Henry and Aaron Brantly, "Countering the Cyber Threats," *Cyber Defense Review* 3, no. 1 (Spring 2018): 47-56, Herbert Lin, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations," *Lawfare*, September 6, 2018, https://www.lawfareblog.com/developing-responses-cyber-enabled-information-warfare-and-influence-operations.
7. Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* 3, no. 1 (2018): 105-122.
8. "Defense Primer: Information Operations," *Congressional Research Service*, December 18, 2018. However, there are also important limitations on DoD's ability to conduct information operations, specifically stemming from concerns about operations that may have an impact on the American people.
9. Kimberly Underwood, "Army Cyber to Become Information Warfare Command," March 14, 2019, https://www.afcea.org/content/army-cyber-become-information-warfare-command. Kimberly Underwood, "Army CEMA Teams Advance Information, Electronic and Cyber Warfare," August 6, 2018, https://www.afcea.org/content/army-cema-teams-advance-information-electronic-and-cyber-warfare.
10. "USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings," *U.S. Cyber Command*, February 15, 2019, 2, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427.
11. For a comprehensive discussion of grand strategy, see Hal Brands, *What Good Is Grand Strategy? Power and Purpose in American Statecraft from Harry S. Truman to George W. Bush* (Ithaca NY: Cornell University Press, 2014).
12. "Cyberspace Solarium Commission Report," *Cyberspace Solarium Commission*, 11 March 2020, https://www.solarium.gov/report. For a discussion of the strategic approach, 23-30.
13. John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Congress, 2018; "Cyberspace Solarium Commission Report," *Cyberspace Solarium Commission*, March 11, 2020, https://www.solarium.gov/report.
14. "Cyberspace Solarium Commission Report," 69-70.
15. Ibid., 66-67.
16. "Summary: Department of Defense Cyber Strategy," 2018, 1. There are references to the idea of defend forward in the 2018 Command Vision for U.S. Cyber Command, but the concept is not the central feature of that document.
17. "Cyberspace Solarium Commission Report," 2020, 32.
18. "National Cyber Strategy of the United States of America," *The White House*, September 2018, and "Summary: Department of Defense Cyber Strategy," 2018.
19. "Cyberspace Solarium Commission Report," 2020, 6; Erica D. Borghard and Mark Montgomery, "Defend Forward as a Whole-of-Nation Effort," *Lawfare*, March 11, 2020, https://www.lawfareblog.com/defend-forward-whole-nation-effort.
20. For example, when speaking on the topic of offensive cyber operations, former National Security Advisor John Bolton stated, "We're now opening the aperture, broadening the areas we're prepared to act in… Our response doesn't have to be only in cyberspace so we're really looking at the full range of things we can do." Kenneth Rapuano, Assistant Secretary of Defense for Homeland and Global Security, told the house Armed Force Committee that DoD's defend forward "strategy normalizes the department's efforts in the cyberspace domain, integrating cyberspace operations into military operations across all physical domains, and reinforces the need to prevent or degrade threats before they harm U.S. national interests." See Shannon Vavra, "U.S. Ramping up Offensive Cyber Measures to Stop Economic Attacks, Bolton Says," *CyberScoop*, June 11, 2019, https://www.cyberscoop.com/john-bolton-offensive-cybersecurity-not-limited-election-security/; Terri Moon Cronk, "DOD's Cyber Strategy of Past Year Outlined Before Congress," *U.S. Department of Defense News*, March 6, 2020, https://www.defense.gov/Explore/News/Article/Article/2103843/dods-cyber-strategy-of-past-year-outlined-before-congress/.

NOTES

21. Joint Publication 3-13 (November 27, 2012), ix.
22. Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations," f*orthcoming, Oxford Handbook of Cybersecurity* (2019), 4.
23. Ibid., 5.
24. Herbert Lin, "The Existential Threat from Cyber-Enabled Information Warfare," *Bulletin of Atomic Scientists* 75, no. 4 (2019): 187-196.
25. For a discussion of recently declassified documents on Operation GLOWING SYMPHONY and Joint Task Force-ARES, obtained through Freedom of Information Act requests, see Cyber Vault project at the National Security Archive, "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL," https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil.
26. "Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, Before the Senate Committee on Armed Services," February 27, 2018, 4. Also see, David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *The New York Times,* April 24, 2016, https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyber-weapons-at-isis-for-first-time.html.
27. Ryan Browne and Barbara Starr, "Top Pentagon Official: 'Right now it sucks' to be ISIS," *CNN,* 14 April 2016, https://www.cnn.com/2016/04/13/politics/robert-work-cyber-bombs-isis-sucks/index.html.
28. "Statement of General Paul M. Nakasone, Commander, United States Cyber Command, Before the Senate Committee on Armed Services," February 14, 2019, 4. Dina Temple-Raston, "Task Force Takes on Russian Election Interference," *NPR,* August 14, 2019, https://www.npr.org/2019/08/14/751048230/new-nsa-task-force-takes-on-russian-election-interference; and Julian E. Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *The New York Times,* February 26, 2019, https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html.
29. Brandon Valeriano, "Managing Escalation Under Layered Cyber Deterrence," *Lawfare,* April 1, 2020, https://www.lawfareblog.com/managing-escalation-under-layered-cyber-deterrence. For a general discussion of the risks of escalation in cyberspace, see Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* 13, no. 3 (2019): 122-145.
30. General Nakasone does note that information-sharing with partners and enabling others is also an important part of defend forward. *United States Special Operations Command and United States Cyber Command: Hearing Before the Senate Armed Services Committee,* 116th Congress, 2 (February 14, 2019) (statement of General Paul M. Nakasone, Commander United States Cyber Command); and William T. Eliason, "An Interview with Paul M. Nakasone," *Joint Force Quarterly* 92 (1st Quarter 2019), 6.
31. Daniel Byman and Matthew Waxman, *The Dynamics of coercion: An American Foreign Policy and the Limits of Military Might,* (Cambridge, UK: Cambridge University Press, 2002); and Glenn Snyder, *Deterrence and Defense,* (Princeton, NJ: Princeton University Press, 1961).
32. Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452-481; Borghard, "The 'Known Unknowns' of Russian Cyber Signaling," *Council on Foreign Relations-Net Politics Blog,* April 2, 2018, https://www.cfr.org/blog/known-unknowns-russian-cyber-signaling; Gartzke and Lindsay argue that cyber operations should be understood in the context of intelligence and covert operations capabilities and have utility in their role in aiding deception, precisely because of their ambiguity and problems associated with clear signaling. See Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316-348.
33. The Solarium Commission Report describes adversarial campaigns in depth. See "Cyberspace Solarium Commission Report," 2020, 8-14; and Erica D. Borghard and Shawn W. Lonergan, "Public-Private Partnerships in Cyberspace in an Era of Great Power Competition," forthcoming.
34. Tim Maurer, *Cyber Mercenaries,* (Cambridge, UK: Cambridge University Press, 2018); and Erica D. Borghard and Shawn Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?" *Orbis* 60, no 3 (2016): 395-416.
35. Michael Connell and Sarah Volger, "Russia's Approach to Cyber Warfare," Center for Naval Analyses, September 2016; "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System," The Department of Justice, February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere; Andrew Radin, Alyssa Demus, and Krystyna Marcinek, "Understanding Russian Subversion: Patterns, Threats, and Responses," RAND Corporation, February 2020.

NOTES

36. Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (2017): 72-109; and Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," Security Studies 22, no. 3 (2013): 365-404.
37. Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF. Also see Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hachette Books, 2020).
38. Barbara Geddes, Joseph Wright, and Erica Frantz, "Autocratic Breakdown and Regime Transitions: A New Data Set," *Perspectives on Politics* 12, no. 2 (2014): 313-331; Bruce Bueno De Mesquita, et al., "Testing Novel Implications from the Selectorate Theory of War," *World Politics* 56, no. 3 (2004): 363-388; and Jessica L. Weeks, "Autocratic Audience Costs: Regime Type and Signaling Resolve," *International Organization* 62, no. 1 (2008): 35-64.
39. Borghard and Lonergan, "Risks of Using Cyber Proxies."
40. For a discussion of the implications of the 2019 National Defense Authorization Act, which defined cyber operations as traditional military activity, see Robert Chesney, "The Law of Military Cyber Operations and the New NDAA," *Lawfare*, 26 July 2018, https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa.
41. "Cyberspace Solarium Commission Report," 2020, 115.
42. John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Congress, 2018, Section 1642.
43. "Core Activities," U.S. Special Operations Command, https://www.socom.mil/about/core-activities.
44. "Cyber Mission Force Achieves Full Operational Capability," *U.S. Department of Defense News*, May 17, 2018, https://www.defense.gov/Explore/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/.
45. "Cyberspace Solarium Commission Report," 2020, 113.
46. HASC Hearing, "Hearing to Receive Testimony on United States Cyber Command, 9 May 2017, 20-21.
47. "Cyberspace Solarium Commission Report," 2020, 114.
48. Erica D. Borghard, "Cyber Command Needs New Acquisition Authorities," *Lawfare*, May 12, 2020, https://www.lawfareblog.com/cyber-command-needs-new-acquisition-authorities.
49. William B. Pickett, ed, *George F. Kennan and the Origins of Eisenhower's New Look: An Oral History of Project Solarium* (Princeton: Princeton Institute for International and Regional Studies, 2004).
50. See, for example, Rosa Brooks, *How Everything Became War and the Military Became Everything: Tales From the Pentagon* (New York: Simon & Schuster, 2016).
51. For further discussion, see Shawn J. Parry-Giles, "The Eisenhower Administration's Conceptualization of the USIA: The Development of Overt and Covert Propaganda Strategies," *Presidential Studies Quarterly* 24, no. 2 (Spring 1994), 263-276.
52. 105th Congress of the United States of America. H.R. 1757: Foreign Affairs Reform and Restructuring Act of 1998, (January 27, 1998).
53. Executive Order 13721: Developing an Integrated Global Engagement Center to Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584, Section 1287, https://www.hsdl.org/?abstract&did=791347.
54. NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2017, Sec. 1287, https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf#page=548.
55. "Defense Primer: Information Operations," Congressional Research Service, January 14, 2020, 2.
56. Abigail Tracy, "A Different Kind of Propaganda: Has America Lost The Information War?" *Vanity Fair*, April 23, 2018.
57. "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," January 10, 2018, 3.