#ACcyber

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF
JUNE 2022

Victory reimagined: Toward a more cohesive US cyber strategy

EMMA SCHROEDER, STEWART SCOTT,
and TREY HERR

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The Cyber Statecraft Initiative works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

EXECUTIVE SUMMARY

A strategy to defeat US adversaries in cyberspace is not the same as, nor sufficient for, securing cyberspace. US policy is on two potentially divergent paths: one that prioritizes the protection of American infrastructure through the pursuit of US cyber superiority, and one that seeks an open, secure cyber ecosystem. Defend Forward was a compelling and necessary shift in thinking, but it is just one of many policy tools available to implement the US cyber strategy. In the *new* National Cyber Strategy, policymakers and practitioners should heed the costly lessons of a generation of counterinsurgency and ensure that efforts to defeat adversaries in cyberspace do not displace efforts to secure it. In an article published by *Foreign Affairs*, National Cyber Director Chris Inglis and Harry Krejsa, assistant national cyber director for strategy and research, emphasized, "security is a prerequisite for prosperity in the physical world, and cyberspace is no different."[1] A revised national cyber strategy should: (1) enhance security in the face of a wider range of threats than just the most strategic adversaries, (2) better coordinate efforts toward protection and security with allies and partners, and (3) focus on bolstering the resilience of the cyber ecosystem, rather than merely reducing harm.

INTRODUCTION

With a new US cyber strategy in the offing, policymakers will have the chance to readjust to meet the demands of the constantly changing cyber environment. The stakes are high. Even on the most tranquil days in cyberspace, millions of malicious emails flicker and fall against Department of Defense (DoD firewalls,[2] security firms track salvos of hundreds of thousands of attacks across the planet,[3] and attackers scan the entire internet for vulnerable targets within

[1] Chris Inglis and Harry Krejsa, "The Cyber Social Contract," *Foreign Affairs*, February 21, 2022, https://www.foreignaffairs.com/articles/united-states/2022-02-21/cyber-social-contract.

[2] Frank Konkel, "Pentagon Thwarts 36 Million Email Breach Attempts Daily," Nextgov.com, January 11, 2018, https://www.nextgov.com/cybersecurity/2018/01/pentagon-thwarts-36-million-email-breach-attempts-daily/145149/.

[3] "Cyber Threat Map," FireEye, accessed May 27, 2022, https://www.fireeye.com/cyber-map/threat-map.html.

hours of bugs becoming public.[4] Markets trade in tools and certificates for offensive use and churn billions of dollars' worth of products ranging from basic keyloggers to exploit suites built by the National Security Agency (NSA) built exploit suites.[5] Meanwhile, legislation aims to harvest zero-days at their source, diverting them from industry to government use.[6] All this activity persists—and by most accounts is increasing—despite vast investments of time, effort, and money from government and industry alike.

The 2018 National Cyber Strategy embedded a central dissonance between the defense of US assets and interests and the security of a safer cyber ecosystem. While efforts toward each of these policies are not mutually exclusive, protection is not sufficient for security, and if improperly balanced, their implementations risk working against each other. US cyber-protection operations are organized on the assumption that protecting US assets in cyberspace through establishing superiority is a necessary and constructive step toward a more secure digital ecosystem at large. Defend Forward is a manifestation of this pursuit, developed by the DoD to create friction as close as possible to the source of malicious activity to prevent, and eventually disincentivize, attacks against US cyber assets.

Defend Forward has garnered much attention in debates over strategy in cyberspace. Its advocates cheer the agility and proactive stance it affords the military, anticipating a greater ability to disrupt adversaries before they can cause harm and even behavioral changes brought about by better imposing costs on malicious actors.[7] Its critics have concerns, meanwhile. Some worry about the systemic risk to the cyber ecosystem that might accrue through more frequent exploitation.[8] Others warn that the relatively constrained level of conflict in cyberspace—having not yet escalated to the equivalent of armed attacks—is a product of the world's current geopolitical context more than anything inherent to the domain.[9]

The effort to Defend Forward has pulled policy attention and resources to counter high-end and strategic adversaries, while leaving pervasive insecurities in commonly used technology systems and a permissive operating environment for a host of other threats. There is a similar dissonance between protection and security in the conduct of counterinsurgencies, and the parallels are instructive. Unlike conventional war, the central goal of a counterinsurgency is not to render an adversary incapable of further resistance but to create a secure environment for a society.[10] Pursuing protection requires offensive action against enemy forces, but those operations alone are not sufficient to create the larger strategic aim of security. While an important concept in the current US strategy in cyberspace, Defend Forward must work within a broader effort to secure, rather than merely protect, the United States in cyberspace.

Taking these lessons to heart can build on the successes of Defend Forward, including pulling the US policy community past latent Cold War assumptions and rhetoric while ensuring US strategy is adequate to the goal of creating security and not merely removing significant harm. By producing a national cybersecurity strategy that redoubles a commitment to security and accounts for the important but auxiliary role of protecting itself and its allies, the United States will be better able to secure cyberspace and all the social and economic activities within it.

This paper uses the analogy of counterinsurgency operations to help frame a more cohesive implementation of Defend Forward. In some ways, the lessons learned from the counterinsurgent military operations that sought to disrupt and degrade an insurgency's ability to mount attacks apply to US Defend Forward efforts. Like destroying insurgent forces, offensive cyber operations and the maintenance of access to third-party systems necessary to sustain Defend Forward are a useful and distinctly martial step in an ongoing campaign, but on their own they are insufficient to achieve "victory." In real-world analogs, such as the United States' recent engagement in Afghanistan, that "victory" is something close to nation building, and in cyberspace, it is achieving markedly improved security writ large. To avoid burdening Defend Forward (and the DoD) with too much of the responsibility for improving the security of cyberspace, the next cybersecurity strategy, in close conversation with the national security strategy, should strive toward its integration with a suite of complementary policy tools.

[4] Sergiu Gatlan, "Attackers Scan for Vulnerable VMware Servers after PoC Exploit Release," BleepingComputer, February 25, 2021, https://www.bleepingcomputer.com/news/security/attackers-scan-for-vulnerable-vmware-servers-after-poc-exploit-release/.

[5] Winnona DeSombre, James Shires, JD Work, Robert Morgus, Patrick Howell O'Neill, Luca Allodi, and Trey Herret al., "Countering Cyber Proliferation: Zeroing in on Access-as-a-Service," Atlantic Council, March 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/.

[6] Robert Lemos, "China's Claim on Vulnerability Details Could Chill Researchers," Dark Reading, July 20, 2021, https://www.darkreading.com/vulnerabilities-threats/china-s-claim-on-vulnerability-details-could-chill-researchers.

[7] Erica Lonergan and Mark Montgomery, "Defend Forward as a Whole-of-Nation Effort," Lawfare, March 11, 2020, https://www.lawfareblog.com/defend-forward-whole-nation-effort.

[8] Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," Journal of Cybersecurity 5, no. 1 (August 26, 2019), https://doi.org/10.1093/cybsec/tyz008; Max Smeets and Herbert Lin, "An Outcome-Based Analysis of US Cyber Strategy of Persistence & Defend Forward," Lawfare, November 28, 2018, https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward; Max Smeets, "Cyber Command's Strategy Risks Friction With Allies," Lawfare, May 28, 2019, https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.

[9] Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," Texas National Security Review 3, 4 (2020), 30–53, http://dx.doi.org/10.26153/tsw/10962.

[10] Carl von Clausewitz, On War, Michael Howard and Peter Paret, eds. (Princeton, NJ: Princeton University Press, 1976), 75, https://www.usmcu.edu/Portals/218/EWS%20On%20War%20Reading%20Book%201%20Ch%201%20Ch%202.pdf; "US Government Counterinsurgency Guide," Department of State, Bureau of Political-Military Affairs, January 2009, 3, https://2009-2017.state.gov/documents/organization/119629.pdf; Heather S. Gregg, "Beyond Population Engagement: Understanding Counterinsurgency," US Army, December 29, 2009, https://www.army.mil/article/32363/beyond_population_engagement_understanding_counterinsurgency.

CURRENT US CYBER STRATEGY: GOALS AND MEANS

Strategy is the effort to achieve policy goals through the application of appropriate means on the adversary and on the operating environment. As these factors change and policymakers better understand those changes, strategy must evolve to ensure that the foundation of action remains that intended outcome (i.e. ends)—not the means themselves. This tension between means, especially those of the offensive military variety, and political goals has long stood as one of the central domestic debates during times of war and conflict. Assigning priority to a goal that should be the subsidiary, such as claiming territory or killing enemy forces, risks constant, strategically stagnant conflict.

This tension is not unique to cyberspace. A telling manifestation is the cooperative and contentious relationship between Prussian Chancellor Otto von Bismarck and Helmuth von Moltke, chief of the Prussian General Staff during the mid-nineteenth century. Moltke believed the military commander must have total freedom of decision within the operation of war itself, as "no plan of operations extends with certainty beyond the first encounter with the enemy's main strength."[11] As a statesman, Bismarck was more concerned with the utility of war to realize state goals. He considered the objectives and capabilities of the armed forces to be of extreme importance, but only inasmuch as they could contribute to achieving the overall political objective of a war.[12] Killing the enemy, in Bismarck's eyes, was a means rather than a goal in and of itself. Moltke and Bismarck were often at odds with one another's views, yet in practice, the Prussian government benefited from this push and pull between political intent and means on strategy. Though these three—strategy, means, and politics—are all inseparably linked, politics must act as the driving force, determining the desired outcomes of action, while means must act as the constraining force, determining which actions are possible and effective.

There is a similar tension in the conception and execution of US cyber strategy. The 2018 National Cyber Strategy lays out four pillars to strive towards:

1. ***Defend the homeland*** *by protecting networks, systems, functions, and data;*
2. *Promote American prosperity by nurturing a* ***secure, thriving digital economy and fostering strong domestic innovation****;*
3. *Preserve peace and security by strengthening the ability of the United States—in concert with allies and partners—to* ***deter and, if necessary, punish*** *those who use cyber tools for malicious purposes; and*
4. *Expand American influence abroad to extend the key tenets of an* ***open, interoperable, reliable, and secure Internet****.*[13]

While the first and third pillars focus on the relationship between the cyber domain and the United States or entities within it, the more expansive, final pillar illustrates how the United States conceives of desired goals for the entire domain and how it imagines getting there.

US policy is on two potentially divergent paths: *one that prioritizes the protection of American infrastructure through the pursuit of US cyber superiority,* and *one that seeks an open, secure cyber ecosystem*.

Many policies can contribute constructively to both US cyber superiority and an open, secure ecosystem. However, stability and offensive prowess do not always perfectly align, particularly in cyberspace, where patching vulnerabilities or exploiting them are often in direct tension. The method to pursue the first and third pillars—towards defending forward—is to some degree incompatible with and possibly counter to the goal of the fourth without complement. That tension expresses itself in the incomplete Defend Forward doctrine, the competing equities of US offensive and defensive cyber elements, and the vagueness of achieving "cyber superiority." Clarifying US strategic cyber objectives and grounding them in the domain's dynamics and actor interactions is key to incorporating Defend Forward within a cohesive, national cyber strategy based on achievable, constructive, and proactive national security goals. The protection of US infrastructure is crucial, but the central goal of US operations in the cyber domain must be a secure ecosystem.

DEFEND FORWARD AS CYBER PROTECTION

Defend Forward undergirds the first and third pillars of the 2018 National Cyber Strategy: protecting US entities by disrupting and imposing costs on malicious actors. General Paul Nakasone, commander of US Cyber Command, wrote in 2019 that "we must take this fight to the enemy … to compete with and contest adversaries globally, continuously, and at scale, engaging more effectively in the strategic competition that is already under way."[14] Defend Forward includes actions in cyberspace during day-to-day competition but focuses on strategic threats, specifically calling out China and Russia.[15] The repeated back-and-forth between actors in cyberspace, termed competitive interaction, helps players locate the line between the

[11] Helmuth von Moltke, "On Strategy," in Moltke on the Art of War: Selected Writings, Daniel J. Hughes, ed. (Novato, CA: Presidio Press, 1995), 46.

[12] Otto von Bismarck, Bismarck: the Man and the Statesman: Being the Reflections and Reminiscences of Otto Prince Von Bismarck, vol. 2, 105 (London: Smith, Elder & Co., 1898).

[13] "National Cyber Strategy of the United States of America," Office of the President of the United States, September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[14] Paul Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly*, no. 92 (January 22, 2019): 10–14.

[15] "Summary: Department of Defense Cyber Strategy," US Department of Defense, September 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

acceptable and the escalatory.[16] If the United States wants to play a role in shaping the development of this threshold, explain Michael Fischerkeller and Richard Harknett, "it can do so only through active cyber operations."[17]

Importantly, while some debate how Defend Forward focuses on its potential to deter by imposing costs on adversary operations, those effects are second-order and highly speculative. For example, Erica Lonergan writes, "Defend Forward hypothesizes the US can change adversary behavior through making attacks less effective and, cumulatively, by altering the adversary's decision calculus regarding the perceived benefits, costs and risks of conducting malicious campaigns against the United States."[18] That may be the case, but knowing an enemy's risk calculus and how it changes over time is extremely fuzzy, especially in the cyber domain where many operations confound observation. This cumulative change in behavior may also run in unanticipated and harmful directions.[19] Defend Forward finds tangible value in breaking up enemy attacks ahead of time—incentivizing behavioral change is possible but also extremely difficult to measure and further outside the remit of DoD operations. Evaluating Defend Forward by its impact on adversary choice sets a high bar for the concept and makes success far less measurable while downplaying the significance of its main goals—protecting US cyber interests by interrupting attacks before they can cause harm.

There are circumstances that lend themselves to successful Defend Forward operations. Knowing who the adversary is, which networks the adversary operates on and against, and the adversary's general objectives and timelines all help calibrate operations. In the physical analogy, the most disruptive, successful offensive sweeps will anticipate when and where an enemy is gathering its forces and disrupt them at the source ahead of any campaigns they may undertake. Narrowly tailored, these proactive efforts to disrupt and defend outside the 'wire' can be an effective way to avoid costly pitched battles close to home.

For example, offensive cyber operations were reportedly used to counter Russian cyber campaigns targeting the United States' 2018 midterm and 2020 presidential elections.[20] In his testimony before the Senate Armed Services Committee, Nakasone told the panel that US Cyber Command had conducted more than two dozen operations across nine different countries "to get ahead of foreign threats before they interfered with or influenced our elections in 2020."[21] The operations to counter malign foreign influence on US elections, appeared successful, establishing the Russian Small Group, disrupting botnets,[22] and stemming Russian information operations at their source in concert with Department of Justice efforts across both election cycles.[23] Similarly, while the public record of the US role in the cyber component of the war in Ukraine is extremely limited, simply being able to identify the most likely targets—Ukrainian infrastructure—and match them to the general timeline of on-the-ground offensives is likely to have contributed to successful Defend Forward operations.

SECURING CYBERSPACE

Viewing Defend Forward as protective offense casts it more accurately as one of several contributors to overall security. In real-world counterinsurgencies, the ability of the United States to directly degrade an enemy's capacity through preemptive strikes is critical. However, this requires careful coordination with the overall counterinsurgency effort and clear scoping—for instance, the ability of Defend Forward to disrupt endemic crime (cyber or physical) where rule of law is unenforced or to build resilient infrastructure for civilian use is limited, but both are key to successful counterinsurgency. The central task of counterinsurgency efforts cannot be limited to destroying the enemy but must aim primarily to create a secure environment.[24]

Various military historians and practitioners have through the years written on the US preference, through several counterinsurgencies, for attrition to the detriment of strategy. According to British Brigadier Nigel Aylwin-Foster, for example, US forces in Iraq were "inclined 'to consider offensive operations as the key' without understanding the penalties of that approach."[25] Similarly, Defend Forward

[16] Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (June 21, 2017): 381–93, https://doi.org/10.1016/j.orbis.2017.05.003.

[17] Ibid.

[18] Erica Lonergan, "Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior," Lawfare, March 12, 2020, https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior.

[19] Jenny Jun, "Preparing for the Next Phase of US Cyber Strategy," Atlantic Council, March 30, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/preparing-the-next-phase-of-us-cyber-strategy/

[20] Eric O'Neill, "Defend Forward Amid a New Era of Cyber Espionage," Newsweek, April 23, 2021, https://www.newsweek.com/defend-forward-amid-new-era-cyber-espionage-opinion-1585854.

[21] *United States Special Operations Command and United States Cyber Command*, *Before the Senate Armed Services Committee*, 117th Congress (2021) (Gen. Paul Nakasone, Commander, US Cyber Command) https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-25-21.pdf.

[22] Erica Lonergan, "Cyber Command's Role in Election Defense: Important, But Not a Panacea," Lawfare, October 30, 2020, https://www.lawfareblog.com/cyber-commands-role-election-defense-important-not-panacea.

[23] Mark Pomerleau, "The US Military Is Targeting Foreign Actors to Defend the Presidential Election," C4ISRNet, October 30, 2020, https://www.c4isrnet.com/cyber/2020/10/30/the-us-military-is-targeting-foreign-actors-to-defend-the-presidential-election/.

[24] David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford: Oxford University Press, 2011), 266.

[25] John Mackinlay and Alison Al-Baddawy, "Rethinking Counterinsurgency: RAND Counterinsurgency Study—Volume 5," RAND, April 15, 2008, https://www.rand.org/pubs/monographs/MG595z5.html; Nigel Aylwin-Foster, "Changing the Army for Counterinsurgency Operations," Military Review LXXXV, 6 (2005), https://www.hsdl.org/?view&did=484927; John A. Nagl, Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam (Chicago: University of Chicago Press, 2005), 116; Colin S. Gray, "Irregular Enemies and the Essence of Strategy: Can the American Way of War Adapt," Strategic Studies Institute, US Army War College, March 1, 2006, https://www.jstor.org/stable/resrep11464.

literature claims contributions to the broader security of the cyber ecosystem. Yet, these generated effects may not be as beneficial to the security of the domain as they are to the day-to-day defense of US infrastructure. As Max Smeets and Herb Lin argue, even though the US government may believe that US superiority in cyberspace is a precondition for security throughout the cyber domain, this is far from the only possible truth.[26]

Defend Forward does not lend itself to securing cyberspace from all malicious activity and seems better suited to addressing the most dangerous campaigns emanating from strategic adversaries or those targeting selected high consequence targets within the United States. In fact, the actions required for successful forward defense may necessitate a degree of insecurity throughout the domain. This entails persistent preparation of, and operation through, cyberspace to identify and maintain access for future operations, as well as disrupting, degrading, and eavesdropping through those gaps indefinitely. This is not to say that Defend Forward is a bad strategy so much as it is not a strategy on its own and not a means of fully realizing the goals of the current US cybersecurity strategy. Indeed, its place as the paramount concept of US cyber strategy is in tension with broader US objectives of a secure and stable cyberspace.

A new US National Cyber Strategy should explicitly set the improved security of the cyber domain as its central strategic goal, supported by other tactical priorities—not least of which is the direct and proactive protection of US assets and interests. This paper argues that such a strategy should focus on three areas: enhancing security across the spectrum of threats, better coordinating with allies and partners at a strategic level, and improving the resilience of the cyber ecosystem.

1. SECURITY ACROSS THE SPECTRUM OF THREATS

There is a wide spectrum of threats that exceeds the capacity of the DoD to address alone. Military operations intended to claim territory or damage adversary capacity cannot create a secure environment without cooperation along all the levers of power. As General James Mattis famously offered in a 2013 Senate Armed Services Committee hearing, "If you don't fund the State Department fully, then I need to buy more ammunition."[27] Defend Forward seeks out adversary activity that may become a threat to the security and interests of the United States as close to the source of that activity as possible. Operationally, that means making decisions about the type of adversaries and potential targets to prioritize. The Command Vision for US Cyber Command explicitly focuses on the actions of Russia and China, and relegates its considerations of a broader set of adversary operations impacting overall economic prosperity to a footnote.[28]

Even against nation-state actors, against whom Defend Forward takes primary aim, the United States cannot repel or even detect every operation. For example, though Defend Forward operations helped stymie Russia's interference with the 2018 and 2020 US elections, around the same time Russia conducted a massive espionage operation in US cyberspace. Russian operators successfully inserted a backdoor into a SolarWinds Orion software update and methodically gained access to hundreds of targets across the US private sector and within the US government itself, only discovered through the disclosure of a private cybersecurity company.[29] This does not mean that ongoing Defend Forward efforts failed—just that the success was in countering a known threat. But seeking out adversaries where and when they are suspected to strike is insufficient on its own, especially in a domain where perfect adversary awareness is impossible and operations ubiquitous and constant. Defend Forward is an effective strategy for higher levels of threat—especially when their timing and targeting can be "guessed"—but the United States needs a strategy that underpins defense against malicious cyber activity across the entire spectrum.

However, state actors are not the only threats to US interests or the security of cyberspace. Ransomware—a relatively simple but effective tactic that persistently features in cybercriminal activity and against which sub-Fortune 100 businesses are deeply vulnerable—remains a persistent scourge against organizations large and small. While individual ransomware perpetrators may pose little threat to the entire digital ecosystem, on aggregate their impact is staggering, with most estimates putting the net global cost of cybercrime over the past few years at trillions of dollars.[30] States like Russia and North Korea sponsor or provide safe haven for ransomware attackers and may even partake at the state level themselves. There is a thriving marketplace for black-market exploits, certificates, and data links malicious actors at all levels of sophistication.[31] Precisely because of their decentralized nature, private-

[26] Max Smeets and Herbert Lin, "Chapter 4: A Strategic Assessment of the U.S. Cyber Command Vision," in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, Amy Zergart and Herbert Lin, eds., (Washington, DC: Brookings Institution Press, 2019), 81–104, https://www.brookings.edu/book/bytes-bombs-and-spies/.

[27] *Mattis on Ammunition* (Washington, DC, 2013), https://www.c-span.org/video/?c4658822/user-clip-mattis-ammunition.

[28] "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," US Cyber Command, April 2020, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

[29] Trey Herr et al., *Broken Trust: Lessons from Sunburst* (Atlantic Council, 2021), https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/.

[30] Kelly Bissell, Ryan LaSalle, and Paolo Dal Cin, "The Cost of Cyber Crime: Ninth Annual Cost of Cybercrime Study - Unlocking the Value of Improved Cybersecurity Protraction," (AccentureSecurity, Ponemon Institute, March 6, 2019), https://www.accenture.com/us-en/insights/security/cost-cybercrime-study; James Andrew Lewis, Zhanna Malekos Smith, and Eugenia Lostri, "The Hidden Costs of Cybercrime," (San Jose, CA: CSIS, McAfee, December 9, 2020), https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

[31] Winnona DeSombre, et al., Countering Cyber Proliferation: Zeroing in on Access-as-a-Service, Atlantic Council, March 1, 2021, https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/the-proliferation-of-offensive-cyber-capabilities/.

sector targets, and widely varied tactics, ransomware and similar incidents of cybercrime are a systemic source of insecurity that the current Defend Forward strategy is not well equipped to counter.

Assuring security requires action to counter a range of threats, not merely those most strategic or capable. There are similar limits on the applicability of Defend Forward-like tactics in counterinsurgency operations. According to the 2009 US Counterinsurgency Guide, counterinsurgency centers on "securing and controlling a given population" rather than "defeating a particular enemy group."[32] In environments of insecurity, tools aimed at creating and encouraging a broad environment of security may better serve the strategic purpose than those aimed only at countering the most sophisticated actors. In counterinsurgencies, these measures, often diplomatic and economic in nature, prioritize the construction of resource pathways intended to incentivize cooperative behavior and sustain healthy local security, governance, and political processes. In cyberspace, achieving security against the entire spectrum of threats requires finding balance across a wide range of policy tools. As it updates its cyber strategy, the United States must set the security of the domain as its central strategic goal, with defense within and across that domain as subordinate but still critical priorities.

Recommendations

Impose cost, but also deny benefit:[33]

The vast majority of malicious cyber activities at the lower end of the cyber conflict spectrum are financially motivated. With relatively inexpensive purchases of capability, malicious actors can reap impressive profits—a Deloitte study found that penetration tools costing an average of just $3,800 a month could net cybercriminals $1 million over the same time.[34] And while much criminal activity, such as phishing, is relatively unsophisticated, individual incidents can still threaten security on a national scale. For example, the ransomware attacks that impacted fuel pipeline services and meat production in recent years.[35] Raising the baseline of defensibility should make cybercrime less profitable at a greater scale than Defend Forward can.

The next US Cyber Strategy should take account of ongoing policy changes and redouble efforts to support public-private partnerships investing against capabilities and in infrastructure rather than just response. To aid smaller, less well-resourced companies, the US government should fund security tooling access and professional education for small-to-medium enterprises (SMEs) while working to improve the size and capacity of the cybersecurity workforce at a national scale. There have been several legislative efforts to effect such a change: HR 4515, the Small Business Development Center Cyber Training Act[36] and the cybersecurity provisions within HR 5376, the Build Back Better Act.[37] In addition, further legislation is required to make permanent the cybersecurity grant program under the recently passed infrastructure bill (Public Law 117-58) with the added guidance from the Cybersecurity and Infrastructure Security Agency (CISA).[38]

CISA, in cooperation with its Joint Cyber Defense Collaborative (JCDC), the Department of Justice, and the Treasury Department, should compile clear, updated guidance for victims of ransomware, including how victims unable or unwilling to make ransomware payments can request aid from the Cyber Response and Recovery Fund.[39] Further legislation should focus on federal subsidies for access to basic, managed cybersecurity services like email filtering, secure file transfers, and identity and access management services.[40]

2. WORK ACROSS ALLIES AND PARTNERS

Defend Forward operations themselves must move through allied and partner networks—known as the "grey space"—to target adversaries.[41] The Defend Forward imperative to operate "as close as possible to adversaries and their operations" means carrying out US operations and likely causing friction within this grey space. Even allied states may not accept US operations affecting and degrading infrastructure in their territory, especially without their prior knowledge. Prior knowledge of specific operations through open, honest bilateral dialogue is unlikely in a domain where vulnerabilities are fleeting and secrecy central. The

[32] David Kilcullen, Matt Porter, and Carlos Burgos, "U.S. Government Counterinsurgency Guide," US Department of State, January 1, 2009, 12, https://apps.dtic.mil/sti/citations/ADA494660.

[33] For context on several of these recommendations and more, see the *Buying Down Risk* series from the Cyber Statecraft Initiative - https://www.atlanticcouncil.org/content-series/buying-down-risk/home/

[34] Andrew Morrison, Emily Mossburg, and Ed Powers, "Black-Market Ecosystem: Estimating the Cost of 'Pwnership'" (New York, NY: Deloitte, December 14, 2018), https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-announces-new-cyber-threat-study-on-criminal-operational-cost.html.

[35] Jacob Bunge, "JBS Paid $11 Million to Resolve Ransomware Attack," Wall Street Journal, June 9, 2021, https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781; William Turton and Kartikay Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password," Bloomberg, June 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

[36] US Congress, Senate Small Business and Entrepreneurship Committee and House Small Business Committee, *Small Business Development Center Cyber Training Act*, 117 Cong., 2021, https://www.congress.gov/bill/117th-congress/house-bill/4515.

[37] US Congress, House Budget Committee, *Build Back Better Act*, 117 Cong., 2021, https://www.congress.gov/bill/117th-congress/house-bill/5376?q=%7B%22search%22%3A%22hr+5376%22%7D&s=2&r=3.

[38] US Congress, House Transportation and Infrastructure Committee, *Infrastructure Investment and Jobs Act*, 117 Cong., 2022, https://www.congress.gov/bill/117th-congress/house-bill/3684/text.

[39] "Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force," Institute for Security and Technology, April 2021, https://securityandtechnology.org/ransomwaretaskforce/report/.

[40] Stewart Scott et al., "Buying down risk: Cyber poverty line," Atlantic Council, May 3, 2022, https://www.atlanticcouncil.org/content-series/buying-down-risk/cyber-poverty-line/.

[41] Max Smeets, "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection," *Intelligence and National Security* 35, 3 (2020), 444–453, https://doi.org/10.1080/02684527.2020.1729316.

states and private sector entities that comprise the grey zone would likely have concerns ranging from sovereignty, privacy, and threats to their own ongoing cyber operations and services. For instance, a 2019 French Ministry of Armed Forces communique asserted that "any cyberattack against French digital systems, or any effects produced on French territory by digital means by a State organ … constitutes a breach of sovereignty."[42] US interference could very likely impede the ability of others to pursue their own strategies, persistent or not, in cyberspace. Commenters have noted that such operations risk "undermining allies' trust and confidence in ways that are subtle and not easily observable."[43] Adversaries, knowing this point of friction, would then benefit from moving through this grey space, pairing their operational goals with the strategic impact of forcing the United States to move against the interest of US allies.

The parallels to counterinsurgency are apparent here as well. When a foreign power assists or intervenes in a domestic counterinsurgency effort, its ability to move through the space is hindered by the acceptance of the local population and governance structures as much as geography and resource limitations. Even with explicit requests from the local government, the presence of a foreign power exerting influence and control may be viewed locally as occupation and a challenge to independence. The presence of US forces abroad, in places like Iraq and Afghanistan, can ignite the very tensions their presence intended to douse.[44]

As in cyberspace, this tension is an attractive point of vulnerability for exploitation by adversaries, with little incentive to prioritize security. Inviting retribution against the population, or incentivizing actions that create insecurity and friction, may incur tactical or operational losses but can translate into strategic gains. Certain American offensive operations in Iraq and Afghanistan—such as US drone strikes accused of killing or injuring civilians—undoubtedly contributed to the lack of popular support for these wars. [45] Cyber conflict, despite its technical and largely intangible nature, shares a population-centric element with insurgencies—the population is attacker, target, bystander, and an intrinsic part of the medium through which these conflicts are waged. Friction and discord with local populations, or at the points where cyber meets the physical world, are only a benefit to the adversary.

Coordination with allies and partners is not only crucial in denying adversaries potential opportunities for exploitation, but in creating a more free and secure domain through positive and constructive interaction. Cyberspace, an interconnected and relatively borderless domain, requires coordinated effort from states and the private sector alike to affect change. In areas of persistent conflict where state control is not absolute, like cyberspace and conflict zones, improving security is an exercise in cooperation. US efforts toward stabilization through cooperation in Afghanistan were exceptionally complex. However, there are lessons learned, both positive and negative, that apply to the problem of cooperation within the cyber domain. Namely, that stabilization was most successful where there was continuous dialogue among US and allied forces and local governance structures, where long-term programs were not usurped by those looking for quick gains, and where local governments saw clear evidence of the benefits of their participation.[46]

This means a shared, or at least commonly understood, vision for the state of the domain, as well as agreement and understanding as to the acceptable methods of operation outside a state's "territory" and through privately owned infrastructure. And, of course, the entities through which such agreements can be discussed and amended. The vast majority of activity in the cyber domain is conducted through and with infrastructure and tools operated by the private sector. Private sector companies, in a way, are both the native human terrain as well as the deepest network of information on the activity within that terrain. This means that true coordination cannot be an imposition of the state or states but must more closely resemble a partnership between countries, companies, and civil society organizations.

Recommendations

US strategic cohesion: The United States government must ensure that its operations in cyberspace are consistent with an overall strategy to enhance security. The recently established Department of State Bureau of Cyberspace and Digital Policy's (CDP) intent is to "encourage responsible state behavior in cyberspace and advance policies that protect the integrity and security of the infrastructure of the

[42] Harriet Moynihan, "The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace," Journal of Cyber Policy 6, 3 (2021), 394–410, https://doi.org/10.1080/23738871.2020.1832550.

[43] Max Smeets, "Cyber Command's Strategy Risks Friction With Allies," Lawfare, May 28, 2019, https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.

[44] Angela O'Mahony, et al., "U.S. Presence and the Incidence of Conflict," RAND, 2018, https://www.rand.org/pubs/research_reports/RR1906.html; Eric Neumayer and Thomas Plümper, "Foreign Terror on Americans," Journal of Peace Research 48, 1 (2010), 3–17, https://doi.org/10.1177/0022343310390147; Alex Braithwaite, "Transnational Terrorism as an Unintended Consequence of a Military Footprint," Security Studies 24, 2 (2015), 349–375, https://doi.org/10.1080/09636412.2015.1038192; Alexander Cooley, "Base Politics," Foreign Affairs 84, 6 (2005), 79–92; Thomas Gries, Daniel Meierrieks, and Margarete Redlin, "Oppressive Governments, Dependence on the USA, and Anti-American Terrorism," Oxford Economic Papers 67, 1 (2015), 83–103, https://doi.org/10.1093/oep/gpu038.

[45] Amrit Singh, "Death by Drone: Civilian Harm Caused by U.S. Targeted Killings in Yemen," Open Society Justice Initiative, Mwatana Organization for Human Rights, 2015, https://www.justiceinitiative.org/publications/death-drone; Sarah Kreps, Paul Lushenko, and Shyam Raman, "Biden Can Reduce Civilian Casualties during US Drone Strikes. Here's How," Brookings, January 19, 2022, https://www.brookings.edu/articles/biden-can-reduce-civilian-casualties-during-us-drone-strikes-heres-how; Chantal Grut and Naureen Shah, "Counting Drone Strike Deaths," Columbia Law School Human Rights Clinic, October 2012, https://web.law.columbia.edu/sites/default/files/microsites/human-rights-institute/files/COLUMBIACountingDronesFinal.pdf; "Drone Warfare," Bureau of Investigative Journalism, last visited May 27, 2022, https://www.thebureauinvestigates.com/projects/drone-war.

[46] John Sopko, "Stabilization: Lessons from the U.S. Experience in Afghanistan," Special Inspector General for Afghanistan Reconstruction, May 2018, https://www.sigar.mil/interactive-reports/stabilization/index.html.

Internet, serve U.S. interests, promote competitiveness, and uphold democratic values."[47] The CDP should have the explicit priority of promoting US and allied policies that improve the security of the cyber domain at large while expanding internet freedom. This work must align with the security of cyberspace as much as the promotion of free, open, and secure technologies such as the internet and liberal information environments that have more traditionally been the State Department's focus. As the CDP engages with allies and partners, the bureau should act as a credible, capable partner within the US government to support the "cooperative security" strategic perspective. Rebalancing equities in the US National Cyber Strategy demands a more even handling of roles for the Defense and State Departments as much as it does continued improvements in State's capacity to operate effectively as an interagency partner on these security issues.

Coordination in strategy: Cyberspace is an inherently cooperative domain. The US government must work in tandem with allies and partners in the private sector to improve domain security. The US National Cyber Strategy must build this coordination into its foundation. In the previous National Cyber Strategy, allies and partners primarily focused on establishing and encouraging norms of responsible behavior, securing critical infrastructure, combating cybercrime, and promoting US economic prosperity. The new strategy needs a more robust framework for how US government agencies and entities will engage with and consider consequences for allies and partners while pursuing their respective missions. United States Cyber Command (CYBERCOM) should coordinate explicitly with the defense entities of US allies to set expectations and parameters for Defend Forward operations. These should include agreed-on standards for disclosure of operations and upper limits on operational freedom to an appropriate degree, recognizing that such decisions are rarely black and white. Similarly, DoD should work with CISA's JCDC to coordinate its offensive action with the largest private-sector entities through whose networks and technologies retaliatory blows, and subsequent operations, are likely to pass. This coordination should strive to establish a precedent for communication and cooperation as possible, recognizing the significant effect that offensive activities can have on defenders.

3. ENSURING A MORE RESILIENT CYBER ECOSYSTEM

In emphasizing offensive operations outside of home networks, US forces must continually prepare the potential battlespace—cyber operations cannot launch on a whim. The 2018 US Cyber Command Vision defines cyberspace superiority as "the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations." [48] Essentially, it defines superiority as freedom of movement. To give policymakers and military leaders options, operators must locate and retain vulnerabilities, developing exploits beforehand and carefully retaining and cultivating them. These capabilities require monitoring, maintenance, and management, as the shifting cyber domain makes tools and capabilities temporary.[49] However, an exploit maintained is an exploit unremedied. Vulnerabilities and exploit tools—despite best intentions—can also serve adversaries.

This freedom of movement, often considered an enabling factor of victory in counterinsurgencies, is "always a reversible condition."[50] There is no end in sight and no set of metrics on which to measure progress or success. While US cyber strategy might not explicitly seek to protract cyber conflict, it nonetheless implies perpetual action taken toward an insufficiently outlined goal. The sophisticated, intense cyber operations conceived of by the current US strategy rely on considerable effort: the "defender" must identify a target, find useful vulnerabilities, create tools to exploit them, maintain control over the tools' launch and continued effects, and orchestrate many complex, interdependent operations. Therefore, Defend Forward requires preserving some measure of technical insecurity.

The threat posed by continued conflict to ecosystem security is familiar in insurgency literature. In his 2007 study of modern insurgency, Stephen Metz, a professor of national security and strategy at the US Army War College, wrote, "Protracted conflict, not insurgent victory, is the threat ... the deleterious effects of sustained conflict, and if it is part of systemic failure and pathology in which key elites and organizations develop a vested interest in sustaining the conflict."[51] The same risk exists for cyberspace. Unsurprisingly, vague cyber policy aims mirror the lack of endgame often critiqued in US counterinsurgency operations, and for good reason—adversary goals of eroding an asymmetry, compromising an organization, or undermining a government are tangible and finite. Preserving advantage is weakly defined, difficult to measure, and potentially without end.

[47] Jennifer Bachus, "Bureau of Cyberspace and Digital Policy," *United States Department of State* (blog), accessed May 27, 2022, https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/.

[48] "Achieve and Maintain Cyberspace Superiority," 6.

[49] Lonergan, "Operationalizing Defend Forward."

[50] Ben Connable, et al., "Assessing Freedom of Movement for Counterinsurgency Campaigns," RAND, 2012, 23, https://www.rand.org/pubs/technical_reports/TR1014.html.

[51] Steven Metz, "Rethinking Insurgency" (Strategic Studies Institute, US Army War College, June 1, 2007), Summary vi, https://www.jstor.org/stable/resrep11642.

The EternalBlue debacle, while predating Defend Forward, exemplifies this tension between shoring up the cyber ecosystem and preserving offensive capabilities inherent to the current strategy. The NSA developed an exploit, EternalBlue, that allowed it to carry out reportedly effective and widespread intelligence collection.[52] The agency debated whether to disclose information about the pervasive, deep-reaching vulnerability in Microsoft's software to the Redmond giant or to use it offensively, opting for the latter.[53] However, in April 2017, some entity identifying as an independent organization called the Shadow Brokers released information about EternalBlue and other NSA tools online.[54] Though the NSA privately disclosed the existence of EternalBlue to Microsoft after discovery of the theft and shortly before it became public, adoption of the company's security update lagged, as is common.[55] Microsoft's decision to initially restrict the distribution of the patch to customers with paid support contracts exacerbated the lag.[56] Within two months, North Korean government hackers converted the exploit into a worm and then used the borrowed capability to launch the massive ransomware operation, WannaCry.[57]

Despite continued efforts by Microsoft to patch its systems, EternalBlue is now a ubiquitous malware feature used by state-affiliated groups like Russia's Fancy Bear and Iran's Chafer, as well as a myriad of non-state and unsophisticated criminal actors.[58] Much of the response to the incident, however, focused on the failure to secure the capability, rather than its development—cries of "how could you lose control?" reigned.[59] However, the fallout from the incident also inspired questions about the apparent paradox of securing cyberspace by preparing weapons to compromise it.[60]

US cyber strategy must combine judicious offensive activity with deep investment in both the architecture of and distribution of risk across the cyber ecosystem. Attacker speed, incident impact, and the opportunity for exploitation increasingly outpace the efforts of cyber defenders throughout the software and basic technologies forming the fabric of cyberspace. These security challenges are widespread and must be confronted through resilient architectures, standards, and practices to address the risk at the root of widely used technology systems. The centrality of the private sector in this effort requires government to create policy that enables and incentivizes industry to manage risk across the ecosystem.

The NSA has since updated its policies on releasing discovered vulnerabilities. In cooperation with several other entities across the United States government, the agency engages in the Vulnerabilities Equities Process (VEP) to determine "which software vulnerabilities it discloses, and which ones it withholds for its own use in espionage, law enforcement, and cyber warfare."[61] However this balance is fragile. One that operates under an impermanent executive policy and still lacks legislative investiture.[62] The improved transparency is a welcome step. However, the government needs to do more to instill confidence in the public that US efforts balance the need to create and preserve offensive capabilities alongside the potentially competing desire to create a more secure ecosystem by reducing overall vulnerability.

Recommendations

Balance security and maintained vulnerability: Retaining and managing vulnerabilities that enable Defend Forward operations necessitates a purposeful balance, neither radical transparency nor opacity. The practice of Defend Forward is complex and might include instances where adversarial access is degraded preemptively rather than disrupted. Therefore, the government should encourage

[52] Ellen Nakashima and Craig Timberg, "NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did.," *Washington Post*, May 16, 2017, https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

[53] Ibid.

[54] Andy Greenberg, "Major Leak Suggests NSA Was Deep in Middle East Banking System," *Wired*, April 14, 2017, https://www.wired.com/2017/04/major-leak-suggests-nsa-deep-middle-east-banking-system/.

[55] Dan Goodin, "Fearing Shadow Brokers Leak, NSA Reported Critical Flaw to Microsoft," Ars Technica, May 17, 2017, https://arstechnica.com/information-technology/2017/05/fearing-shadow-brokers-leak-nsa-reported-critical-flaw-to-microsoft/.

[56] Richard Waters and Hannah Kuchler, "Microsoft held back free patch that could have slowed WannaCry," Financial Times, May 17, 2017, https://www.ft.com/content/e2786cbe-3a97-11e7-821a-6027b8a20f23.

[57] Ali Islam, Nicole Oppenheim, and Winny Thomas, "SMB Exploited: WannaCry Use of 'EternalBlue,'" Mandiant, May 26, 2017, https://www.mandiant.com/resources/smb-exploited-wannacry-use-of-eternalblue; Nakashima and Timberg, "NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did."; Lily Hay Newman, "How Leaked NSA Spy Tool 'EternalBlue' Became a Hacker Favorite," *Wired*, March 7, 2018, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

[58] Nakashima and Timberg, "NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did."; "Chafer: Latest Attacks Reveal Heightened Ambitions," Symantec, February 28, 2018, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions.; Andy Greenberg, "A Russian Hacker Group Used a Leaked NSA Tool to Spy on Hotel Guests," Wired, August 11, 2017, https://www.wired.com/story/fancy-bear-hotel-hack/; "Fancy Bear Hackers (APT28): Targets & Methods," CrowdStrike, February 12, 2019, https://www.crowdstrike.com/blog/who-is-fancy-bear/.

[59] Nakashima and Timberg, "NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did."; Thomas Brewster, "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak," Forbes, May 12, 2017, https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/?sh=40a8274ae599.

[60] Brad Smith, "The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack," Microsoft, May 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.0001g1c7g94cgcqzpqt24knkjj2ra; Amy Zegart, "The NSA Confronts a Problem of Its Own Making," Atlantic, June 29, 2017, https://www.theatlantic.com/international/archive/2017/06/nsa-wannacry-eternal-blue/532146/.

[61] Lily Hay Newman, "Feds Explain Their Software Bug Stash-But Don't Erase Concerns," Wired, November 15, 2017, https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/.

[62] William Loomis and Stewart Scott, "A Role for the Vulnerabilities Equities Process in Securing Software Supply Chains, Lawfare, January 11, 2021, https://www.lawfareblog.com/role-vulnerabilities-equities-process-securing-software-supply-chains.

time-delayed declassification of VEP disclosure decisions where possible to increase transparency with allies and partners. Moreover, the government should require an automatic review of decisions to withhold vulnerabilities from disclosure no later than one year after a decision. This automatic process would encourage consistent enforcement and should include input from defensive collaboration vehicles like CISA's JCDC to better contextualize the security benefits of disclosure.

Improve measurement: While there is no shortage of headline-grabbing figures about insecurity in the cyber ecosystem, many of those metrics also lack standardization and transparency, leading to great variety among measures and reducing insight into their fluctuations over time. Many figures rely on private datasets and voluntary reporting. Understanding the state of security across the domain will require more rigorous measurement. The National Science Foundation (NSF) should fund select universities and research institutions to develop more rigorous statistics and measurement methods for cybersecurity (and insecurity). Multiple parallel studies undertaken across academia will prevent overreliance on single methodology sources while driving greater statistical rigor. This grant program should closely coordinate with improved information sharing among the private sector through CISA's JCDC to give academic studies some access to proprietary datasets. It should coordinate similarly with Department of Justice mandatory reporting standards.

Invest proactively in resilience: Excessive strategic focus on offensive and forward defense activity preferences preemptive disruption over defensibility. While there is language about the importance of improved ecosystem resilience throughout US cyber strategy documents, this topic deserves far richer treatment than a framing device. Just as a successful counterinsurgency campaign needs to create secure governance as much as it requires degrading insurgent capabilities, policy must reduce the adversary's ability to do harm—both in disrupting criminal activities and in bolstering the social, economic, and political resilience. In the cyber ecosystem, this should start with prioritizing secure designs in information-technology (IT) systems. Starting at the root of common technologies gives policymakers the widest possible impact and helps nudge complex, dynamic systems towards security at scale.[63] A strong example of this would be public-private investment in memory-safe code that can reduce the prevalence of entire classes of vulnerability while providing the opportunity to prioritize mission-critical code in government and industry.[64] Refocusing on resilience and strengthening the security of core technology architectures should improve the lot of cyber defenders and users, producing systems that are innately easier to defend, more costly to compromise, and better able to improve over time—driving security without compromising efforts at protection.

CONCLUSION

Many policies can contribute constructively to both US cyber superiority and an open, secure ecosystem. However, stability and offensive prowess do not always perfectly align. Put more directly—US victory over major adversaries is not sufficient to ensure a secure and stable cyberspace. Neither withdrawing from nor completely pacifying the digital domain is possible—all that remains is to secure it incrementally and continually. The work to develop a new US cybersecurity strategy can help reshape the balance of policy toward greater security and help ensure an important, but complementary role, for the offensive and Defend Forward activities at the center of the current strategic concept.

Defend Forward operations have a key role to play in disrupting adversaries before they can do harm, especially when targets and timelines are known; that entails, to some extent, preserving and exploiting insecurity. Yet, the observable shortcomings of these efforts resemble common critiques of US counterinsurgency efforts—mission creep, unquantifiable objectives, and indefinite timelines—precisely because of the assumption that effectively protecting US assets from adversaries in cyberspace is the same as creating a secure digital ecosystem at large. Instead, it is one step among many toward that end and may indeed be counterproductive to the larger goal if applied poorly or to excess. In the same way that killing insurgents is necessary to, but insufficient for, winning a counterinsurgency, offensive and forward defensive activities can realize much more strategic value alongside efforts that better address the full spectrum of cyber threats, improve coordination with allies, and encouraging a more resilient cyber ecosystem. All these will contribute to a key pivot in framing: from Defend Forward as a whole-of-nation endeavor to one piece in a whole-of-nation strategy.[65]

As the United States redevelops its national cyber strategy, the question of overall political intent must stand at the forefront. This strategy needs to clearly address the dissonance between the stated policy goals of protection and domain security—a tall order, but a feasible one. Proactive offensive cyber operations that protect US infrastructure and interests are, and will continue to be, necessary. But just as in counterinsurgencies of the past, the United States must ensure that it does not fall into a "strategy of tactics,"[66] losing the war by winning the battles.

[63] Loomis and Scott, "A Role for the Vulnerabilities Equities Process."

[64] Stewart Scott et al., "Buying down risk: Memory safety," Atlantic Council, May 3, 2022, https://www.atlanticcouncil.org/content-series/buying-down-risk/memory-safety/.

[65] Lonergan and Montgomery, "Defend Forward as a Whole-of-Nation Effort."

[66] Gray, "Irregular Enemies and the Essence of Strategy," 20.

ABOUT THE AUTHORS

Emma Schroeder is an assistant director with the Atlantic Council's Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security. Her focus in this role is on developing statecraft and strategy for cyberspace that is useful for both policymakers and practitioners.

Stewart Scott is an assistant director with the Atlantic Council's Cyber Statecraft Initiative, within the Scowcroft Center for Strategy and Security. He works on the Initiative's systems security portfolio, which focuses on software supply chain risk management and open source software security policy.

Trey Herr is the director of the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His team works on the role of the technology industry in geopolitics, cyber conflict, the security of the internet, cyber safety, and growing a more capable cybersecurity policy workforce.

Atlantic Council

Board of Directors