#ACcyber

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

MARCH 2022

Preparing the next phase of US cyber strategy

JENNY JUN
Nonresident Fellow, Cyber Statecraft Initiative, Atlantic Council
PhD Candidate, Department of Political Science, Columbia University

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

This paper considers tensions in the current US cyber strategy for the Defense Department and the broader cyber policy community in the Biden-Harris administration as they form the next phase of the strategy. Specifically, it argues that the current strategy may not incentivize other cyber powers to conduct campaigns in ways that minimize accidents and reckless behavior. In addition, the paper highlights a lingering, and deleterious, ambiguity in how Defend Forward relates to the concept of deterrence in cyberspace. These tensions reveal that simply hoping that states will arrive at common "rules of the road" through tacit interactions is not sufficient. A renewed US strategy also needs active diplomacy and explicit bargaining among states, with the United States proactively shaping the contours of that debate. The revised strategy should also streamline how, when, and under what conditions Defend Forward can best serve as a means to the goal of achieving superiority in cyberspace.

INTRODUCTION

Four years after the 2018 Cyber Posture Review, the Department of Defense (DoD) will likely soon complete a review of how cyber capabilities and operations relate to the broader US military strategy. A key strategic concept in the current US cyber strategy is Defend Forward, which aims to "disrupt or halt malicious cyber activity at its source" in order to "stop threats before they reach our targets."[1] Several documents articulate this concept including the 2018 Command Vision for US Cyber Command, the 2018 DoD Cyber Strategy, and the 2020 Cyberspace Solarium Commission Final Report.[2]

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

2 "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command" (US Cyber Command, March 23, 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010; "2018 Department of Defense Cyber Strategy"; "Cyberspace Solarium Commission Final Report" (Cyberspace Solarium Commission, March 11, 2020), https://www.solarium.gov/report.

Though scholars have debated on the merits of this concept in the past four years, at least for this cycle of review, Defend Forward as a strategic concept is likely here to stay. That is not to say that the concept is not without unresolved tensions. First, while proponents of Defend Forward argue that there is a downstream positive effect by forcing the adversary to spend its resources on defense, this may only be true in some conditions. The review should recognize that Defend Forward can also directly lead to downstream negative effects in other cases, such as increased reckless behavior due to a shortening tempo of operations. Second, key US documents on Defend Forward are not in alignment as to whether the United States seeks to achieve deterrence in cyberspace or not, and if so, against whom and for what level of activities. Furthermore, some actions taken in cyberspace for purely defensive purposes can potentially undermine the deterrence that the United States purports to seek. The next iteration of US cyber strategy must work to resolve these tensions and find ways to explicitly link with other instruments of policy to complement the strategic concept.

DEFEND FORWARD AND ITS RISKS

Does the current strategy incentivize others to minimize accidents and reckless behavior?

One of the stated objectives of Defend Forward is to shape adversary behavior by making it more costly to launch a cyber operation. However, the strength with which different publications on US cyber strategy have made this argument varies.[3] Taken together, Defend Forward hopes to have a cumulative positive effect via repeated cyber operations against an adversary, forcing the adversary to spend more time and resources on defense, and eventually persuade the adversary to change their strategic calculus and give up future campaigns.[4]

Nonetheless, in its original formulation, proponents may have overemphasized the accumulating positive effects of Defend Forward and overlooked the potential downstream negative effects. For instance, some adversaries may prioritize mission success over risk management. Adversaries may also deliberately adopt more reckless tactics as well as unintentionally make mistakes, such as launching tools before sufficiently testing them.[5] In this light, Defend Forward may incentivize more dangerous behavior, especially from adversaries that do not think it is worth it to respond by spending resources on defense.

Threat groups often choose to exercise restraint not because they feel altruistic, but because they are making an explicit intelligence tradeoff between the benefit from exploiting a target versus the chance for premature detection of their operation. Russian hackers most likely chose not to exploit the vast majority of systems they could have targeted by compromising SolarWinds. Indiscriminate exploitation would have increased the likelihood of a Russian group being detected and prematurely prevented access to their priority targets. Similarly, some malware like Stuxnet, contained deliberate controls to try to limit how the code propagated, so as to limit collateral damage but also to minimize chances of detection. Often, operational restraint in cyberspace is a strategic choice, as well as a luxury, which takes considerable time and energy to prepare and not a constraint imposed by technical or economic shortcomings.[6] So what could drive adversaries to think that designing a cyber campaign with restraint in mind is a luxury they can no longer enjoy?

Early detection of their activities may trigger a "use it or lose it" mentality for threat groups, when they expect to have a relatively short window of opportunity to exploit a vulnerability. These groups would then no longer see a need to exercise restraint as their activity will be detected regardless of such careful and costly efforts. In addition, this closing window of opportunity could encourage groups to hasten the tempo of their operations. This race against time could increase the likelihood of coding errors or the omission of critical controls such as "kill switches," leading to more collateral damage or open doors to further third-party exploitation.

Earlier in 2021, in anticipation of a soon-to-be-released patch, a group of Chinese operators decided to indiscriminately install web shells on hundreds of thousands of Microsoft Exchange servers, making those systems vulnerable not just to further Chinese network exploitation but also to other opportunistic state and criminal groups.[7] Threat groups may also deliberately use access to one type of vulnerability to open doors to many others, expecting a short window of opportunity on the initial vulnerability. Increased exploitation of software supply chain vulnerabilities may be a symptom of such tradeoffs. Furthermore, expecting that

3 For instance, US Cyber Command's 2018 Command Vision states, "continuous engagement imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks." The 2020 Cyberspace Solarium Commission implies a deterrence by denial effect with, "layered cyber deterrence combines different ways to shape adversaries' decision making. The central idea is simple: increase the costs and decrease the benefits that adversaries anticipate when planning cyber attacks against American interests." This claim is more muted in Nakasone and Sulmeyer's 2020 *Foreign Affairs* article, "US forces must compete with adversaries on a recurring basis, making it far more difficult for them to advance their goals over time." "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command"; "Cyberspace Solarium Commission Final Report"; Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," Foreign Affairs, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

4 "Cyberspace Solarium Commission Final Report," 24.

5 Perri Adams et al., "Responsible Cyber Offense," Lawfare, August 2, 2021, https://www.lawfareblog.com/responsible-cyber-offense.

6 Antoine Lemay and Sylvain Leblanc, "Operational Tempo in Cyber Operations," 2019, https://www.proquest.com/docview/2261019998/abstract/BB533DD948A1449APQ/1?accountid=10226#; Ben Buchanan, "The Legend of Sophistication in Cyber Operations" (Cyber Security Project, Belfer Center, January 2017), https://www.belfercenter.org/publication/legend-sophistication-cyber-operations.

7 Nicholas Weaver, "The Microsoft Exchange Hack and the Great Email Robbery," Lawfare, March 9, 2021, https://www.lawfareblog.com/microsoft-exchange-hack-and-great-email-robbery.

intelligence gathered from one operation may jeopardize another ongoing operation, threat groups may not fear using destructive tactics to slow down an investigation, for example, the North Korean decision to use a wiper attack against Banco de Chile to obfuscate its theft of $10 million from the bank.[8] Highly skilled threat groups may still successfully exploit targets making few such tradeoffs. However, less skilled threat groups may increasingly resort to "smash and grab" operations without regard for limiting collateral damage. The Microsoft Exchange incident is a reminder that adversaries can always decide to engage in more reckless behavior if they so choose.

In addition, the likelihood of mistakes and accidents may increase as adversaries' cyber operation lifecycles shorten, with the need to develop new tools faster and deploy them quickly before detection of their operations.[9] The best case for advocates of Defend Forward would be that this pressure limits adversary ability to compromise targets, puts these groups on the defensive, and eventually convinces them that continuing to compete with the United States carries more costs than benefits. This is certainly possible, as gleaned from publicly available narratives of Operation Glowing Symphony, a US Cyber Command campaign to disrupt the Islamic State of Iraq and Syria (ISIS) propaganda operations.[10] Policymakers, however, need to evaluate the full range of scenarios beyond the best case to prepare for crises and assess the effectiveness of the strategy from a broad perspective. The alternative scenario is that threat groups will be quick to deploy tools before sufficiently testing them, resulting in unintended consequences with second- and third-order effects. Furthermore, because malware can also have vulnerabilities, just like software, the deployment of malware prematurely can result in a more unstable condition where other adversaries can piggyback on an existing malware to obfuscate attribution or add their own added features.[11]

In the future, adversary groups, expecting that US Defend Forward efforts will disrupt their operations more often, such as takedowns of their command and control (C&C) servers, may increasingly rely on automating the different phases of a cyber operation such that the malware continues to spread from network to network without direct control from the operators. Threat groups may resort to more self-propagating worms that exploit a widespread vulnerability, such as in the case of NotPetya, or malware that is pre-programmed to execute at a certain time or when certain conditions trigger execution. Although more difficult, threat groups may also decide to invest in research on artificial intelligence enabled attacks that help to further automate other phases of a cyber operation, such as automated vulnerability discovery.[12] This profusion of dead man switches and human out-of-the-loop control mechanisms would reduce the US and allied ability to influence operations by impacting adversary organizations directly. Such measures would not only result in more collateral damage of unrelated targets, but would also decrease the operator's control on the cyber operation, increasing chances for unintended consequences. The point is, it is not a *priori* clear that Defend Forward's only cumulative effect will be to compel adversaries to shift resources toward defense rather than to double down on making offense work.

While Defend Forward as a strategic concept is likely here to stay, the next Cyber Posture Review should recognize that Defend Forward can also lead to significant downstream negative effects, and thus seek ways to actively manage such adversary behavior. Doing so requires tools outside the mechanisms of "tacit bargaining," as suggested by the proponents of Defend Forward.[13] Recognizing that operational restraint is often a strategic choice and a luxury opens the door to a variety of questions qualifying how, not whether, to use Defend Forward. For instance, would actions that disrupt an adversary's operation at the testing phase cause the adversary to abandon their campaign or deploy the tool before sufficient testing? Facing an ongoing counter-cyber operation that foils their attempts to compromise a target, are Russia and North Korea equally likely to divert resources to cyber defense? The next phase of US cyber strategy must consider such nuances to minimize the chances and the impact of downstream negative effects of Defend Forward.

Does the current strategy sufficiently clarify the United States' cyber deterrence posture?

The next Cyber Posture Review also needs to resolve a key tension in the current US cyber strategy as to whether it seeks to achieve deterrence in cyberspace or not, and if so, against *whom* and for *what* level of activities. Policymakers also must examine whether the apparent mutual restraint among major powers regarding strategic cyber attacks on each other's critical infrastructure is a direct result of Defend Forward or the product of some other mechanism. Then, it needs to assess whether any aspects of current US cyber operations would stand in tension with these mechanisms.

8 Tara Seals, "Banco de Chile Wiper Attack Just a Cover for $10M SWIFT Heist," Threatpost, June 13, 2018, https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/.

9 Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review 3*, no. 4 (2020), http://dx.doi.org/10.26153/tsw/10962.

10 "How The U.S. Hacked ISIS," NPR, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

11 Adams et al., "Responsible Cyber Offense."

12

13 Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *The Cyber Defense Review*, December 9, 2019, 267–85.

Defend Forward emerged as a strategic concept largely in reaction to the argument that neither deterrence by punishment nor denial is a credible strategy in cyberspace.[14] Fischerkeller and Harknett instead see cyberspace characterized by a condition of "constant contact." They argue that the United States should continuously engage cyber threats outside of its networks through "persistent engagement" rather than trying to dissuade the adversary from conducting cyber operations in the first place.[15]

Yet, deterrence continues to feature in key publications on US cyber strategy. The 2018 Cyber Command Vision seeks to "deter aggression" through "persistent action and competing more effectively below the level of armed conflict."[16] In DoD's 2018 Cyber Strategy, the word "deter" appears eleven times, including "preempt, defeat, or deter malicious cyber activity targeting US critical infrastructure that could cause a significant cyber incident," and "deterring malicious cyber activities that constitute a use of force."[17] In the Cyberspace Solarium Commission's 2020 Final Report, there is an entire section dedicated to the concept of "layered deterrence" and how Defend Forward can directly achieve this through cumulative effects.[18] The only documents where deterrence is notably absent are in General Paul Nakasone's 2019 Joint Forces Quarterly article and his 2020 Foreign Affairs article with Michael Sulmeyer on his vision for how the United States will compete in and through cyberspace.[19]

There is clearly tension within the current US cyber strategy as to whether Defend Forward is a *substitute* to deterrence or its *complement*. It is also not clear whether they coexist on different levels of analysis in no relation to each other, one targeting day-to-day competition and another targeting strategic attacks. There is yet more tension in that DoD's 2018 Cyber Strategy seems to want to achieve deterrence by punishment vis-à-vis critical infrastructure and attacks that constitute a use of force, while the 2020 Cyberspace Solarium Commission explicitly calls for deterrence by denial by making cyber operations more costly than beneficial for adversaries. The current language leaves much room for misjudgment and misinterpretation, especially for analysts in foreign governments trying to gauge how the United States will respond in cyberspace.

One way to untangle this Gordian knot is to start with a small but specific set of behavior for which mutual cyber deterrence does seem to exist, then seek ways to strengthen that mutual understanding. Over the past several years, there have been hints that major powers may have chosen not to launch destructive cyber attacks out of fear that its targets would retaliate in kind. Bruce Schneier, citing several sources, wrote that in 2016 the US government contemplated cyber attacks against Russia in response to its election interference, but chose not to do so out of concern that Russia could in turn target US critical infrastructure.[20] Jackie Schneider noted in her February 2022 testimony to Congress that while China's People's Liberation Army (PLA) doctrine a decade ago suggested that they might target US critical infrastructure in a crisis, more recent Chinese discourse suggests that China may have concerns about its own critical infrastructure vulnerabilities.[21] What seems to be emerging is an implicit sense that targeting an adversary's electrical grid, for example, may not be worth it if it means they can do the same.

This implicit understanding, however, hangs in a precarious balance. There is a big difference, for example, between gaining access to and keeping a foothold, or persistence, in an adversary's electrical grid versus choosing to create destructive effects exploiting that access. To what extent must states maintain a presence in each other's electrical grids to credibly convey that an attack on one grid will likely lead to retaliation? How quickly can each side expect to patch one's own systems, rendering that retaliatory threat less credible? Can the United States and an adversary agree on exactly what systems constitute "critical infrastructure" and agree on how costly their outages might be?

Policymakers must not take the fine print for granted, and this may require explicit communication between two states, rather than just trusting the forces of tacit bargaining. If there are no ready answers to any of the above questions, should the United States prepare for a scenario in which this implicit understanding could break down at any moment, especially during a crisis? Perhaps the reality of sharing mutual vulnerabilities in cyberspace is much more complicated than the simple assumption that a cyber attack that has devastating effects "overshoots the strategic utility of cyber operations."[22]

Furthermore, policymakers need to recognize the possibility that Defend Forward operations with purely defensive intent can still undermine the delicate balance of this mutual understanding. Suppose that in a future crisis with China, the United States starts a campaign to actively kick out

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

15 Fischerkeller and Harknett "Deterrence Is Not a Credible Strategy"; Fischerkeller and Harknett, "Persistent Engagement, Agreed Competition."

16 "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command."

17 "2018 Department of Defense Cyber Strategy."

18 "Cyberspace Solarium Commission Final Report."

19 Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Forces Quarterly* 92 (2019): 10–14; Nakasone and Sulmeyer, "How to Compete in Cyberspace."

20 Bruce Schneier, "An Example of Deterrence in Cyberspace," *Schneier on Security* (blog), June 7, 2018, https://www.schneier.com/blog/archives/2018/06/an_example_of_d.html.

21 Jacquelyn Schneider, "Testimony before the U.S.-China Economic and Security Review Commission: Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States," February 17, 2022,https://www.uscc.gov/sites/default/files/2022-02/Jacquelyn_Schneider_Testimony.pdf.

22 Fischerkeller and Harknett, "Persistent Engagement, Agreed Competition," 275.

all identified Chinese access to the US electrical grid, shut down Chinese C&C servers, and/or disrupt Internet access of a Chinese offensive cyber operations unit, all without explicitly communicating US intentions. While the United States carries out these actions to mitigate threats to the US grid and believes these actions to be purely defensive, China may interpret them as potentially destabilizing. This is because the tacit bargain rests on sharing mutual vulnerability. Unilaterally mitigating a shared vulnerability means that the United States can no longer credibly assure that it will refrain from attacking the Chinese grid. (The same logic exists in various rounds of debate over strategic missile defense – even deploying a defensive system can impact the strategic balance by removing a vulnerability). China could erroneously interpret these actions as a prelude to destructive cyber operations on its own critical infrastructure and/or a signal that the United States is planning to escalate the crisis. This hypothetical example illustrates that there may be inconsistencies where Defend Forward and deterrence undermine each other. There needs to be appropriate scope conditions as to when and how to use Defend Forward, and how diplomacy should complement those actions.

At lower levels of cyber activity that the US government categorizes as "day-to-day competition," policymakers again need greater clarity as to whether the hope is to simply mitigate the frequency and impact of adversary cyber operations or to eventually deter the adversaries from engaging in cyber operations at this lower level as well. Being too eager to sign up for the latter goal may set the US government up for failure, and unnecessarily hurt US credibility in the process. More importantly, these discussions may bring policymakers to a clearer consensus on how Defend Forward as a means should serve ends in cyberspace. One can still achieve superiority in cyberspace without necessarily dissuading the adversary from engaging in this space altogether, by simply denying their ability to achieve effects while securing one's own ability to do the same. This superiority can also be temporary and local depending on the goals of the campaign, rather than permanent or global. While it would be great if an adversary decided to give up its cyber operations altogether as a result of these operations, selecting this as a strategic goal may lead US interests astray from the reason that Defend Forward was conceived of in the first place.

POLICY IMPLICATIONS AND CONCLUSION

Explicit bargaining matters

The above tensions in current US cyber strategy show that the United States cannot rely on tacit bargaining alone to arrive at mutually accepted rules with other states.[23] First, Defend Forward may create a *divergence*, rather than a convergence of behavior depending on how different adversaries react to the shortening tempo of cyber operations. Some may divert resources to the defensive and refrain from launching offensive operations. Yet, others may decide to launch offensive operations anyway without sufficiently testing them or may design operations to prioritize mission success at the expense of limiting collateral damage or maintaining human-in-the-loop processes. Second, analysts may "mirror-image"—or assume that another thinks the same way they do—when they presume that adversaries will also interpret Defend Forward activities as having purely defensive intent. There is no reason why the United States should limit itself to relying on tacit communication with other states in cyberspace.

As Emily Goldman suggests, the US government, especially the State Department, should resume a more active and explicit role in shaping the contours of acceptable and unacceptable behavior in cyberspace.[24] Diplomatic efforts must complement Defend Forward to limit the likelihood and impact of accidents and reckless behavior in cyberspace. Adams et al. already offer an excellent primer as to which behaviors might be especially dangerous.[25] While the world may not be able to collectively agree on broad norms against behaviors such as engaging in cyber espionage, a significant portion of those states may be able to agree on specific promises not to create and launch worms that exploit a widespread vulnerability such as NotPetya or WannaCry. At a minimum, states might be able to agree that a kill switch should be built into any such worm and appoint a body of subject matter experts to monitor and verify the code. The United States should lead efforts in identifying technical aspects of a cyber operation, such that an international body can monitor its restrained use and publicly verify any deviations from it. Over time, these efforts may even develop into formal treaties similar to the Chemical Weapons Convention (CWC) or the Convention on Cluster Munitions (CCM). The accumulation of these explicit efforts can also shape state behavior, especially as new states consider investing in cyber capabilities.

The United States should also not shy away from engaging in bilateral conversations, whether they are in the form of private talks, Track II dialogues, etc. These conversations would clarify the fine print concerning the implicit mutual understanding on establishing and maintaining deterrence vis-à-vis each other's most important critical infrastructure

23 Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," Lawfare, November 9, 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace; Fischerkeller and Harknett, "Persistent Engagement, Agreed Competition."

24 Emily O. Goldman, "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy," 3, no. 4 (2020), https://tnsr.org/wp-content/uploads/2020/09/TNSR-Vol3-Iss4-Goldman.pdf.

25 Adams et al., "Responsible Cyber Offense."

systems. Even the simple process of knowing who the counterpart is at each level and being able to clarify a point of potential misunderstanding through explicit communication may help deescalate a potential crisis. Because access and persistence can be fleeting in cyberspace, mutual restraint based on shared mutual vulnerability would be strengthened through explicit communication.

How, when, and what, to Defend Forward

The next Cyber Posture Review should also streamline its thinking on how Defend Forward can best serve as a means to achieve superiority in cyberspace. Over the four years since its introduction, our collective body of knowledge has grown to include academic articles that explain the theoretical underpinnings of Defense Forward, several official US government publications, policy articles by leaders such as General Nakasone, as well as an array of commentary by scholars and analysts interpreting the concept. Yet, as discussed in this paper, not all are in agreement as to why Defend Forward is needed and how it is to be used or not used. In particular, the documents disagree as to what the relationship is between Defend Forward and cyber deterrence.

Policymakers should delink Defend Forward from a rhetoric of deterrence, leaving the debate on whether cyber deterrence can or cannot be achieved to a relatively small set of important critical infrastructure targets. The main goal of Defend Forward should be to achieve superiority in cyberspace at a time and place of one's choosing, rather than to dissuade states or non-state groups from engaging in what even the US government characterizes as "day-to-day competition." Just as naval blockades help to ensure freedom of activity of one's forces in the open sea by denying the adversary's ability to contest it, Defend Forward may achieve just the same—simple denial, rather than deterrence by denial.

Providing clarity to the political purpose of Defend Forward may also help clarify a long set of questions on the fine print for which situations and in what manner to plan a Defend Forward operation. As Healey et al. note, there is significant variation in the effect and duration of a counter-cyber operation, ranging from more passive actions, such as sinkholing (or redirecting) malicious traffic, to invasive acts that include seizing or destroying the adversary's infrastructure.[26] The United States would like to engage in tacit bargaining through these actions, but which behavior should it encourage and which behavior should it discourage? Perhaps at times, the United States would be better off by allowing the adversary to conduct sufficient testing and take the time to review its code thoroughly. In other situations, it would be better off by constantly disrupting the adversary's development cycle. Sometimes the United States might benefit from being able to reverse the disruption rather than achieve permanent effects. Operators could better answer many of these questions with a clear definition of the strategic concept.

These lingering tensions and questions about the nature of Defend Forward actually indicate progress, for there is a common meeting point in this debate rather than many scattered meetings across a vast landscape. The challenge now is to bring ourselves forward, if not in chorus, then at least in some vague melody such that we might better protect all that animates us in the first place.

CYBER STRATEGY SERIES

The Atlantic Council's Cyber Statecraft Initiative, within the Scowcroft Center for Strategy and Security, presents the Cyber Strategy Series to curate and present new and expanded perspectives on the most pressing topics in cybersecurity strategy. This series is intended to challenge existing assumptions and spark discussion, to help build a better understanding of how the United States can and should operate in the cyber domain.

26 Jason Healey, Neil Jenkins, and JD Work, "Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations" (2020 12th International Conference on Cyber Conflict, 2020), https://ccdcoe.org/uploads/2020/05/CyCon_2020_14_Healey_Jenkins_Work.pdf.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*C. Boyden Gray
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
John Bonsell
*Rafic A. Bizri
Linden P. Blue
Adam Boehler
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Alan H. Fleischmann
*Michael Fisch
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Frank Haun
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Brian Kelly
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Christian Marrone
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
W. DeVier Pierson
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Ali Jehangir Siddiqui
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
Gil Tenzer
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of February 15, 2022