Defending Forward? Implications for Safety, Security, and Sovereignty in Cyberspace

Katrin Marquez, YLS ‘20

In September 2018, the Department of Defense released a summary report of its U.S. Cyber Command strategy. The first DoD cyber strategy report during the Trump Administration, it drew significant attention as it represented “a fundamental reorientation in strategic thinking” for the U.S. government. Unlike the 2015 strategy, which focused on risk-mitigation and preventing escalation, the current strategy takes a more proactive approach. The 2018 strategy promises that Cyber Command “will defend forward to disrupt or halt cyber activity at its source, including activity that falls below the level of armed conflict.”

The 2018 strategy is different from the 2015 strategy in a number of ways, but perhaps the most significant is its embrace of the concept of “defending forward.” Since the release of the summary report in 2018, cyber experts have debated the implications of defending forward. This paper provides a summary of the current debates and concerns surrounding defending forward.

Defining “Defending Forward”

The 2018 strategy repeatedly references the concept of defending forward. The strategy focuses on the goal of “seek[ing] to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD’s warfighting readiness or capability.” The strategy says that the U.S. will “defend forward by levering [its] focus outward to stop threats before they reach their targets.” Yet the strategy never formally defines precisely what “defending forward” means.

The lack of a formal definition of “defending forward” has led cyber experts and scholars to try to define the term. Robert Chesney of the University of Texas School of Law defined defending forward as “operations that are intended to have disruptive or even destructive effect on an external network: either an adversary’s own system or, more likely, a midpoint system in a third country that the adversary has employed or is planning to employ for hostile action.” A simpler definition of the term is “getting as close to adversaries as possible to see what they’re planning as a means of informing others to prepare or take actions themselves.” For the most part, however, attempts at defining defending forward have focused on contrasting the concept with the 2015 strategy. Most definitions have looked to what makes defending forward different than what came before. Attempting to define defending forward by reference to the 2015 strategy, however, poses significant conceptual and practical issues. Jonathan Reiber, drafter of the 2015 strategy, has argued that the 2015 strategy “meant almost the same things as ‘defending forward’ does today.” Though practitioners have suggested that the shift in the 2018 strategy has allowed more flexibility, it remains unclear exactly what constitutes “defending forward” and what consequences the shift may have for sovereignty and security in cyberspace.

Context

To fully understand the implications of defending forward, it is helpful to understand the context in which the 2018 strategy was published. The cyber landscape changed significantly from 2015 to 2018. In the intervening years between the two strategy reports, cyber technology was
used to interfere with the 2016 election and ransomware attacks on critical infrastructure and the exploitation of U.S. intellectual property rights flourished. The Obama Era emphasis on risk-mitigation of the 2015 strategy had been criticized as “excessively passive” in the context of these evolving threats. Though the extent to which defending forward actually differs from the prior strategy is disputed, the emphasis on preemptive instead of reactive response has been lauded by some experts.

The evolving nature of cyber threats in the interim between the 2015 and 2018 led to several realizations for the U.S. government that justified a move to a more proactive approach, argues Erica Borghard of the Cyberspace Solarium Commission. She identifies three such realizations:

Adversary operations span global cyberspace because the environment is not defined by geographic boundaries or even shared understandings about how sovereignty applies in this domain. If the Defense Department’s ability to operate outside of its own networks was more limited and circumscribed, as envisioned in the 2015 Department of Defense Cyber Strategy, the department would be giving free reign to adversary actors that traverse global networks constrained only by capabilities. Second, intelligence collection in cyberspace against an adversary cannot be conducted solely through static, passive collection. . . . Third, to rapidly generate effects in cyberspace at the desired time, forces and capabilities have to routinely operate where the adversary is.

Potential Concerns

Though some welcomed the shift to a strategy of defending forward, others have criticized the approach. Many of these critiques express concerns for the implications that defending forward may have. Two of the most prevalent concerns relate to the role that defending forward may have on increasing the possibility of escalation and on norm development. Here, I present the basic substance of and responses to these two critiques.

Concern 1: Possibility of Escalation

A primary concern for those critical of defending forward is the role it may serve in escalating conflict between nations below the level of armed conflict. Of particular concern for some is the language in the 2018 summary report that by defending forward the DoD “will . . . disrupt or halt malicious cyber activity . . . that falls below the level of armed conflict.” The concern stems from the broader idea of the cyber security dilemma—the notion that when one nation acts to defend itself in cyberspace, another nation may perceive that action as offensive or threatening. Defending forward may create more opportunities for the cyber security dilemma to manifest.

The cyber security dilemma may exist in any circumstances in which one nation is taking cyber action which may seem to impose on another nation’s networks. What makes defending forward a particular concern is that “as hard as it is to differentiate between intelligence collect and attack in cyber operation, it [may be] even harder still to distinguish between defending forward and attacking forward.” To the extent that the defending forward strategy makes it more likely that U.S. Cyber Command carries out operations on foreign governments’ networks – as the
National Defense Authorization Act of 2018 allowed for certain nations, there will be a greater number of opportunities for other nations to perceive U.S. actions as offensive. Since there is no clear consensus as to what cyber actions, if any, are sufficient to constitute a use of force under Article 2(4) of the United Nations Charter or an “armed attack” under Article 51, there is a danger that defending forward—if perceived to be offensive rather than defensive—may aggravate or create hostilities not well-regulated by international law. Defending forward may also create issues in cases where allies perceive the United States as acting inappropriately when using allies’ networks as means to access targets’ networks.

A response to the concerns over the role of defending forward in escalation is to consider the fact that the cyber security dilemma exists even without defending forward. Escalation resulting from the misinterpretation of a defensive cyber acts could have occurred under the 2015 strategy as well. An important consideration, then, is to consider what forces may escalation more or less likely. Ben Buchanan of the Georgetown University School of Foreign Service identifies three explanations for why we have not seem more escalation: (1) most cyber activity takes place outside the public view; (2) nations work to prevent engaging in cyber activities that may lead to kinetic conflict; and (3) as related to the U.S. specifically, the Obama Administration was especially cautious regarding offensive cyber operations. While defending forward—depending on how it is defined and applied—seems to undo the third reason, the first and second reasons may still serve an important role in preventing excessive escalation.

Concern 2: Role in Norm Development

Intertwined with the concern that the use of defending forward may lead to escalation is a concern over the role that defending forward will have in cyber norm development. The lack of clarity as to the application of Articles 2(4) and 51 to cyber operations means that nation-states are attempting to cooperate to develop norms regarding cyber operations. The process of cyber norms development is already quite complicated as there are competing approaches—one side for the protection of fundamental freedoms in the use of information and telecommunications technologies (ICTs) and the other side focusing on nations’ power to retaining control of domestic ICT infrastructures. For the U.S., which has faced the consequences of cyber interference on something as foundational to our system of governance as elections, there may be a need to reconsider what norms it wishes to promote. In the case of preventing election interference, protecting fundamental freedoms necessarily means being able to use strategies like defending forward to retain control of domestic networks.

Defending forward has important implications for cyber norm development because it serves as a model for how a powerful nation behaves in cyberspace. To the extent that defending forward may be understood as a more proactive and assertive defense strategy, it can impact norm development by suggesting more muscular defensive approaches are appropriate under international law. For those concerned with the possibility of escalation, having defending forward as a model for norms may lead to the worry that nations will be willing to significantly escalate cyber conflicts so long as their actions are arguably “defensive” and do not reach the armed conflict threshold. In the context of the cyber security dilemma, such a norm of more aggressive cyber defense may contribute to inter-state hostility.
One response to the concern that defending forward may harm norms is to consider the possibility that being able to defend forward actually depends on having a strong norms foundation. Members of the Cyberspace Solarium Commission have argued that “the application of cyber norms of responsible state behavior is an essential foundation for effective defend forward operations.” They argue that a norms-based approach must be combined with defending forward because norms allow U.S. cyber diplomacy to explain and differentiate U.S. actions to defend forward from adversaries’ wrongful cyber behavior.

Illustration: U.S.-China Relations

The concerns articulated above can already be seen in debates over U.S.-China relations in the wake of the new policy. Soon after the publication of the 2018 summary report Lyu Jinghua, a visiting scholar at the Carnegie Endowment for International Peace and retired colonel from the Chinese People’s Liberation Army, published an essay criticizing the U.S.’s embrace of a defending forward strategy from a Chinese perspective. She argued that defending forward risked escalation, particularly as the change in strategy seemed aimed at China specifically.

The essay quickly drew responses challenging Jinghua’s representation of the issues. Ben Buchanan and Robert D. Williams’s response specifically addressed the Jinghua’s escalation argument in light of norms development. It highlighted why the United States perceived a need to take on a more assertive defensive strategy rather than wait for norms to develop. Buchanan and Williams’s argument argues that attempts at establishing baseline standards for cyber operations between the U.S. and China had failed and that necessitated defending forward. They agreed with Jinghua that, conceptually, international norms to avoid escalation are appropriate. However, they pointed to the China’s unwillingness to cooperate with the norm-setting process of the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), as well as a broken agreement with the Obama administration.

The academic debate between Jinghua and Buchanan and Williams highlights the practical importance of the role of defending forward in escalation and norms development. Jinghua’s essay clearly shows how defending forward may be perceived as an offensive stance from the perspective of a sometime-adversary nation. Buchanan and Williams’s response shows why the interaction between norms development of a defending forward is so complicated—even when there is agreement that non-escalation is an appropriate norm, there may be practical barriers to effectuating that norm.

Remaining Questions

There remain a number of questions regarding the implications of a defending forward strategy for addressing cyber issues. Some of the questions relate to issues as seemingly straightforward as trying to understand just how different from the prior strategy defending forward actually is. Other questions relate to which actors may be necessary to include in the discussion. For example, an understanding of defending forward that conceptualizes of non-government networks being part of critical infrastructure implicate the role of private industry in defending forward. While most of the discussion so far surrounding defending forward has focused on
escalation and norms development, other issues are likely to become salient as the U.S. moves further with this approach. For example, former DoD Analyst Phillip Lohaus has written on the relevance of defending forward to the Internet of Things, which he argues expands the cyber attack surface and puts early adapter nations like China at increased risk.

Suggested Background Reading

- Summary Department of Defense Cyber Strategy 2018
- Max Smeets, US Cyber Strategy of Persistent Engagement & Defend Forward: Implication for the Alliance and Intelligence Collection, 35 INTELLIGENCE & NAT’L SECURITY 444 (2020)
- Laura Bate, Phoebe Benich, Val Cofield, Karrie Jefferson, Ainsley Katz, Sang Lee, Defending Forward by Defending Norms, LAWFARE (March 11, 2020)
- Mark Pomerleous, Here’s How Cyber Command is Using ‘Defend Forward’, FIFTH DOMAIN (November 12, 2019)