The Collateral Frictions of “Defending Forward”

Simon Chin, YLS ’22

The Department of Defense’s new cyber strategy calls for the Pentagon to adopt a proactive, rather than merely reactive, posture toward cyber threats. This new proactive strategy is built upon a vision of “persistent engagement.” Under this approach, the United States seeks to achieve and maintain superiority in cyberspace by “continuously engaging and contesting adversaries.” This continuous engagement will require the United States to “defend forward to disrupt or halt malicious cyber activity at its source.”

“Defending forward,” therefore, will require the Pentagon to undertake active, offensive cyber operations as the norm. The objective of these operations is to alter the strategic calculations of adversaries. The Defense Department believes that persistent engagement will impose “tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks.”

The crux of this strategy, thus, lies in the ability of the Pentagon to convince hostile actors that offensive cyber operations against the United States are not worth undertaking. By influencing and shaping adversary behavior, this approach will, in the Defense Department’s thinking, “improve the security and stability of cyberspace.”

Under the Department Defense’s strategy, the “tactical friction” generated by “defending forward” will be directed toward adversaries in the cyber domain and lead to strategic stability. At the same time, the DoD strategy contains crucial internal tensions, as well as the potential to impose different kinds of friction on other government agencies, U.S. partners and allies, the private sector, and the concept of sovereignty under international law. This background paper explores the unintended or collateral frictions of the “defend forward” strategy and suggests that only by understanding its internal tensions and broader ramifications can all relevant stakeholders effectively evaluate the strategy.

Internal Tensions in the Theory

The Defense Department’s strategy envisions cyberspace as a domain defined by constant competition and active contact between offensive and defensive forces. This conception of the cyber domain has its origins in academic ideas about the nature of cyber conflict. Jason Healey, of Columbia University, has traced the intellectual lineage of the current DoD strategy to the work of Richard Harknett, Emily Goldman, and Michael Fischerkeller. The central idea arising out of this academic work is that in cyberspace, contact is constant and inescapable, even when adversaries are not engaged in formal hostilities. In cyber competition, adversary forces are always contending with each other in active operations below the level of armed attack.

A key insight from this work, which was adopted in the DoD cyber strategy, is that classical deterrence will not be effective in this kind of strategic environment. As Fischerkeller and Harknett have argued, “deterrence is not a credible strategy for cyberspace” because deterrence aims to avoid operational contact. However, in cyberspace, "operations always involve contact, whether it is recognized or not." While deterrence options might be effective against high-end cyber attacks, they will not be useful against the persistent, level-lower offensive operations that occur all the time. If the United States wants to shape the behavior of adversaries in the uniquely interconnected domain of cyberspace, "it can do so only through active cyber operations."

The new strategy, according to Healey, "is a compelling assessment of cyber conflict as a state of constant contact and presents a strong case that … tactical friction to regain the initiative will nudge conflict back towards lower levels of aggression." That is to say, active cyber operations will inflict "tactical friction"—the disruption of cyber operations, the infiltration of networks, and the degradation of cyber infrastructure and other offensive resources. These tactical successes, according to the strategy, will impose cumulative costs and force adversaries to shift resources away from offensive operations and toward defensive capabilities. Over time, adversaries will engage in tacit bargaining with the United States and moderate their behavior, leading to overall strategic stability.

The strategy, thus, crucially relies upon the assumption that increased tactical friction will lead to strategic stability rather than escalation—a casual mechanism that is underexplained and under-theorized in the strategy. The strategy will only work if proactive cyber operations lead adversaries to shift resources away from offensive capabilities. However, as Healey explains, if offensive cyber capabilities are relatively inexpensive and easy to repurpose—as many believe they are—then an adversary could adapt to U.S. offensive operations, with tactical friction leading to an escalatory spiral rather than stability.

The other internal tension in the theory is located in the idea that "defending forward" is a cost-imposing strategy that works to the long-term advantage of the United States. Cost imposition, at least as an American competitive strategy, has its intellectual origins in the work of Andy Marshall and the Office of Net Assessment during the Cold War. The key for Marshall's concept of cost imposition is that it must be asymmetric in order to undermine an adversary's competitive position. A classic example of an effective cost-imposing strategy is the American investment in bomber aircraft and stealth technology, which exploited the Soviet preoccupation with territorial defense and vast Soviet borders to impose disproportionate costs on Soviet air defenses. If "defending forward" in the cyber domain leads to escalation rather than strategic stability, then the United States could find itself on the wrong side of a cost-imposing strategy. It is worth noting that the United States has more attack space in the cyber domain than its adversaries and is thus particularly vulnerable to offensive threats. In the face of more aggressive cyber activity, the United States could have to devote even more resources not only to offensive operations but also to defending its vulnerable networks and systems—a task DoD appears appallingly bad at.

Theory and Practice

There will be inevitable tension when theory is translated into practice. Healey has documented how policymakers, like former National Security Advisor John Bolton and Vice

President Mike Pence, have described the new cyber strategy far less subtly than the military and have even confused forward defense and deterrence. What will happen when policymakers are called to implement and act upon the cyber strategy in practice? Just as importantly, there is the possibility that this carefully drafted military strategy is, at least part, simply cover for the military's desire for enhanced offensive capabilities and operational concepts.

Stewart Baker, a former General Counsel of the National Security Agency, has rather cynically opined on the possible origins of the "defend forward" strategy in the end of the Obama administration. Baker hypothesizes that the strategy's complex discussion of persistent engagement was really about developing a way to unshackle U.S. offensive cyber capabilities—capabilities that had been constrained by the Obama administration's National Security Council. There is a possibility, therefore, of a kind of strategic mismatch or miscalibration. A strategy that was intended to serve one kind of internal bureaucratic purpose in a particular administration now encounters a new political environment, with potentially less restrained political decisionmakers.

The Challenges of Alliance Management

One of the paradoxes of the "defend forward" strategy is that it holds the potential to generate significant external tension with U.S. allies and the private sector—the very partners the Pentagon has stated are critical to the success of the strategy. U.S. Cyber Command envisions "maneuvering seamlessly … across the interconnected battlespace"—meaning across national borders and private sector network perimeters. Yet this strategy carries the risk of damaging the trust and confidence of the partners that the United States will need to operate seamlessly in cyberspace.

A critical component of DoD's cyber strategy is operationalizing international partnerships. DoD recognizes that U.S. allies and partners have advanced and complementary cyber capabilities, and the Pentagon hopes to leverage those capabilities and engage in information-sharing relationships. The objective, DoD states, will be to "increase the effectiveness of combined cyberspace operations and enhance our collective cybersecurity posture."

The danger of this approach, as Max Smeets has argued, is that it could cause more friction with U.S. allies than it inflicts on its adversaries. Smeets writes, "[I]n seeking to successfully create friction in cyberspace for adversaries, Cyber Command may also seek to act within allied networks, even if the ally does not approve … [T]his strategy runs a real risk of undermining allies' trust and confidence in ways that are subtle and not easily observable." Indeed, adversaries could strategically direct activity through intermediate nodes located in the networks of U.S. allies, driving a wedge between the United States and its international partners.

DoD's cyber strategy also envisions building "trusted private sector partnerships." Again, DoD recognizes the value of its partners, in this case, the fact that the private sector owns and operates most of U.S. infrastructure. Indeed, as Healey observes, "unlike other warfighting domains, cyberspace is dominated by the private sector, civil society, and individuals." The new strategy carries with it the profoundly damaging possibility that persistent military operations in private networks will, over the long-run, compromise Internet infrastructure to such an extent that it erodes trust in the technologies underlying so much of daily life. The potential conflict here is not between public and private interests. Rather, it is between competing visions and values of public life. There is also a conflict here between different visions of the global order, as the new strategy will make it more difficult for the United States to collaborate on global rules because it intends to break them.

The Question of Sovereignty

The friction between the "defend forward" strategy and the concept of sovereignty under international law may not be unintended so much as inevitable. Fischerkeller and Harknett have made clear that a strategy of persistent engagement is based upon the understanding that the absence of sovereignty is a structural and operational characteristic of the cyber domain. The question, then, becomes whether sovereignty exists as a rule of international law that can be violated by the kinds of proactive cyber operations, which fall below the level of armed conflict, envisioned by U.S. strategy.

Under the Fischerkeller and Harknett view, cyberspace is a uniquely interconnected and malleable domain, with a low barrier to entry for all kinds of actors. In the absence of an internationally agreed upon concept of sovereignty in cyberspace, states and other significant actors are continually seeking to exert influence through cyber operations that involve constant contact. Traditional notions of deterrence are a strategic mismatch with the cyber domain because they rely upon threats of force if territorial boundaries are crossed. Fischerkeller, Harknett, and Goldman have called for a strategy that recognizes and leverages the interconnectedness and malleability of cyberspace, with friction-producing operations employed "seamlessly" across national borders and network perimeters.

The clear implication of this strategy, as Healey observes, is the potential need to redefine the concept of sovereignty. A debate over this redefinition is ongoing in international law, which Bobby Chesney, from the University of Texas School of Law, has helpfully summarized. The central question is "whether 'sovereignty' is a stand-alone rule of international law that might be violated by military operations in cyberspace even in circumstances that do not constitute the use of force or coercive intervention." In 2018, the U.K. government rejected this view, stating its position that "there is no such rule as a matter of current international law." This position means, as Michael Schmitt has explained, that "a hostile cyber operation would have to either violate the prohibition on intervention, which requires intrusion into the *domaine réservé*, or cross the high threshold for a use of force before being unlawful."

Meanwhile, France and the Netherlands have expressed the opposing view that respect for sovereignty is an independently binding rule of international law. For these countries, as Schmitt writes, "the issue is not the existence of a rule of sovereignty, but the challenge of identifying its parameters in light of the unique characteristics of cyber operations."

In March 2020, Defense Department General Counsel Paul C. Ney, Jr., staked out a position on the question of sovereignty similar to the U.K. Government's, but with some crucial nuances. Ney stated that "it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law."

At the same time, as Schmitt observes, Ney included a critical nuance by drawing an analogy to traditional espionage operations. Ney observed that "international law, in our view, does not prohibit espionage *per se* even when it involves some degree of physical or virtual intrusion into foreign territory… In examining a proposed military cyber operation, we may therefore consider the extent to which the operation resembles or amounts to the type of intelligence or counterintelligence activity for which there is no *per se* international legal prohibition." A critical inquiry for government lawyers, therefore, becomes whether a proposed cyber operation resembles traditional espionage. That inquiry, Schmitt suggests, could form the basis for the United States to operate under a workable legal rule to decide whether or not an operation violates sovereignty.

A Whole-of-Nation Approach

Ney's speech, as Chesney has observed, was not the product of an interagency, whole-of-government process but rather only reflected the Pentagon's views. The DoD position appears to pay short shrift to the broader diplomatic, economic, and societal implications of the new cyber strategy the Pentagon's legal position is intended to support. "Defending forward" is intended to impose a certain kind of friction on cyber adversaries, yet it holds the potential to inflict different kinds of damaging friction on U.S. partners and allies, the private sector, and the rules-based global order. What may be needed is not so much a whole-of-government but a "whole-of-nation" assessment—bringing together all relevant stakeholders to think through, together, how a cyber strategy can achieve our national objectives.

Suggested Background Readings

Department of Defense, *Summary: Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, September 2018).

Jason Healey and Stuart Caudill, "Success of Persistent Engagement in Cyberspace," Strategic Studies Quarterly 14, no. 1 (Spring 2020): 9-15.

Michael Schmitt, "The Defense Department's Measured Take on International Law in Cyberspace," *Just Security*, March 11, 2020, https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/.

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