The Structural and Strategic Imperative: The Need for Persistent Engagement

Michael P. Fischerkeller

The Challenge: The emergent strategic framework for cyberspace, comprising strategies of defense, deterrence, and persistent engagement, is well-suited for the cyber strategic environment but requires vigilance by policymakers not to succumb to strategic conflation and confusion.

It is critically important to avoid adopting strategic concepts developed for one environment and indiscriminately overlaying them in an attempt to secure another.

Background

In May 2017, Richard Harknett and I argued that a strategy of deterrence should not be the central strategy for securing and advancing U.S. national interests in, through, and from cyberspace due to the unique structural and operational characteristics of cyberspace (Fischerkeller and Harknett 2017, 381–93).[1] In the 18 months since, dramatic changes in U.S strategic guidance—the National Security Strategy and National Defense Strategy and, most recently, the Department of Defense Cyber Strategy—now reflect this perspective, arguing that a central challenge to the U.S. lies in strategic competition short of armed conflict in cyberspace (as well as other domains) and that a strategy of deterrence is not an effective anchoring approach for ensuring security in this strategic competitive space (Department of Defense 2018a, 2; Department of Defense 2018b, 2; White House 2017, 3, 31). We argued in 2017 that recognizing the emergence of this new strategic competitive space, one in which adversaries are realizing strategic gains through cumulative effects from cyber campaigns, was a necessary first hurdle to overcome in developing an effective strategic approach to the same.

In February 2018, U.S. Cyber Command published its *Command Vision*, a document describing the cyberspace strategic environment as a new strategic competitive space below armed conflict and prescribing a strategic approach for securing U.S. national interests in cyberspace consistent with what we argued in 2017: a strategy of persistent engagement (United States Cyber Command 2018). This was captured in guidance in the recently released Department of Defense Cyber Strategy, which argues the Department must preserve

[1] Dr. Harknett and I have written several other IDA monographs on cyber strategy since this publication (and have a few more in the pipeline). I'm grateful for his review of and thoughtful recommendations for this article.

U.S. military advantages and defend U.S. interests in, through, and from cyberspace by taking action to contest persistently adversaries' malicious cyber activity during day-to-day competition (Department of Defense 2018b, 4). The strategy rests on recognizing the distinctive structural features of cyberspace and how adversaries have been exploiting them; it is, thus, not a choice if the United States is seeking security in this space, but a structurally and strategically driven imperative to reorient our approach to security. We argued in 2017 that cyberspace's structural feature of interconnectedness and its core condition of constant contact create a strategic necessity to operate persistently in cyberspace. The states that master persistent engagement will not only be more secure in cyberspace, they will also position themselves to enhance their national power relative to others.

From our perspective, then, the United States has made significant progress in the past year toward arriving at a strategic approach that is aligned more effectively with the unique structural and operational characteristics of cyberspace. We are cautiously optimistic that strategic development will continue along a path more consistent with what we've argued is necessary to ensure U.S. security. We use the modifier "cautiously" because a strategy of deterrence and the strategic concepts associated therewith continue to hold a strong place in the minds of U.S. policymakers and other senior leaders. This is to be expected given that a strategy of deterrence has been the dominant U.S. security strategy for the last 70 years. And so the defense community must now be vigilant in ensuring that a strategy of deterrence and a strategy of persistent engagement are viewed as two distinct, yet complementary, strategic approaches grounded in and developed for uniquely different strategic environments. It is critically important to avoid adopting strategic concepts developed for one environment and indiscriminately overlaying them in an attempt to secure another. By understanding the differences between the two strategies, we, in the end, can develop an overarching framework that leverages both (properly applied) to advance U.S. interests in cyberspace. In support of that objective, this article highlights two often seen or heard examples of how the discourse of deterrence too easily, and potentially dangerously, continues to bleed into discussions of a strategy of persistent engagement: the strategic concept of deterrence by denial and equating the generation of a deterrence effect with security.

Deterrence by Denial

When discussed in U.S. strategic guidance, *deterrence is often split into two forms: deterrence by punishment and deterrence by denial.*[2] Given the infrequency of cyber operations targeting the United States having caused effects equivalent with

[2] This is often referred to as *deterrence by cost imposition*, a choice not made here because it will be argued that deterrence both by punishment and by denial impose costs.

armed attack, one could argue that a strategy of deterrence by punishment has been effective in the strategic space of armed conflict (i.e., the strategic space above the threshold of armed attack). It is likely states and other actors understand that such operations would justify under U.N. Article 51 a conventional force (or even nuclear) response in self-defense. The potential (or promise) to inflict punishment on adversaries considering cyber operations equivalent with armed attack, however, has done nothing to reduce the scale or scope of strategic cyber campaigns and operations generating effects short of that threshold.

In fact, relative U.S. restraint in cyberspace appears to have incentivized adversaries' pursuit of strategic objectives in the cyber strategic competitive space short of armed conflict precisely to avoid a conventional confrontation with the United States (Fischerkeller and Harknett 2018). Interestingly, war (or pushing the threshold of war), we've argued, would, in almost all cases, actually represent a failure of an adversary's cyber strategy. Ten years of cyber campaigns and operations by the same have demonstrated it is possible to generate strategic effects through cyber campaigns/operations short of armed attack.

In efforts to mitigate the consequences of adversary cyber operations short of armed attack equivalence, U.S. policymakers have doubled down on the strategic concept of deterrence by denial, routinely identifying hardening and resiliency as operational capabilities/activities necessary to support the same (Department of Defense 2017, 3, 7; United States Congress 2017, 696; United States Congress 2018, 491).[3] Given the unique characteristics of cyberspace that Harknett and I have discussed, we argue that the primary function of these capabilities/activities actually supports a strategy of defense in the cyberspace strategic environment, not a strategy of deterrence by denial.

Glenn Snyder was the first scholar to make a sharp distinction between the objectives of the strategic concepts of deterrence by punishment and denial and a strategy of defense and did so within the context of the nuclear strategic environment (Snyder 1958; Snyder 1961).[4] Snyder argued that an overall strategy of deterrence—"by denial" coupled with "by punishment"—targets an adversary's *intentions* to attack, whereas a strategy of defense reduces an adversary's *capability* to damage or deprive the defender if attacked. Thus, the "deterrent value" of military capabilities is their effect in reducing the likelihood of adversary military operations, and the "defense value" of military capabilities is their effect in mitigating the adverse consequences

[3] The Defense Science Board stated that "steps to promote deterrence by denial include improving cyber defenses and increasing resilience of key systems to attack" and "hardening and increasing the resilience of the most vital critical infrastructure systems – including electricity, water, and waste water – is urgently needed to bolster deterrence by denial."

[4] In 1959, Glenn Snyder published a foundational manuscript describing the difference between deterrence by punishment and deterrence by denial. Snyder incorporated much from that manuscript into a follow-on publication discussing a strategy of defense.

of adversary operations, including losses of territory or war damage.

John Mearsheimer, often cited as one of the principal architects of conventional deterrence theory, argues that conventional deterrence is primarily based on deterrence by denial, described as the ability to prevent an adversary from achieving its objectives through conflict (Mearsheimer 1983, 24, 30, 64, 206–08; see also Lebow 1981, 248; Rhodes 2000, 243–47; Van Evera 1999, 30–4). If states typically seek short and low-cost conflicts, he argued, then conventional deterrence largely depends on convincing an adversary that it cannot achieve its objectives rapidly or efficiently. In this context, the deterrent effect is achieved in large part by the possibility of getting bogged down in a long and costly war of attrition.

According to Mearsheimer, "… deterrence is best served when the attacker believes that his only alternative is a protracted war: The threat of a war of attrition is the bedrock of conventional deterrence" (Mearsheimer 1983, 206–7). That is, deterrence by denial seeks to make aggression unprofitable by rendering the target harder to take, harder to keep, or both (Mitchell 2015). A credible deterrence-by-denial posture, then, requires that a would-be attacker believe a defender's forces are inherently designed to fight and win a conflict in the event of a deterrence failure (Gerson 2009). The defender's capabilities have to be perceived as lethal and able to inflict substantial pain (Mitchell 2015). Like deterrence by punishment, deterrence by denial also threatens to impose costs but differs from punishment in that it threatens to impose costs during the act of aggression and in the place that it occurs, as opposed to at a time and place of the deterrer's choosing (Mitchell 2015).

To come full circle, policymakers continue to cite hardening and resilience as operational capabilities/activities that support a strategy of deterrence by denial in cyberspace. When considering foundational conventional deterrence scholarship, however, those operational capabilities/activities clearly do not match the requirements for an effective deterrence by denial strategy (i.e., hardening and resilience do not represent a lethal posture populated by capabilities that would support an attrition-based response to a cyberattack).

Moreover, the viability of any strategy relying on the concept of attrition warfare in cyberspace finds little support in the scholarly literature (see Brantly 2015).[5] Again, this is structurally determined – the features of cyberspace do not succumb to attrition. This is not to argue that investments in hardening and resilience are not worthwhile. They certainly are, because they support the critical objective of a strategy of defense as described by Snyder, which, to reiterate, is to reduce an adversary's capability to damage or deprive the defender.

[5] Brantly argues that the virtual nature of the cyberspace domain makes attrition warfare an inefficient allocation of resources and unlikely to achieve sustained effects on agile targets.

Why This Matters

If policymakers believe that investments in hardening and resilience are supporting a U.S. strategy of deterrence by denial in cyberspace, they will expect to see results toward that end. Continuing and intensifying adversary activity against U.S. interests accessible in, through, and from cyberspace strongly suggest that hardening and resilience are not affecting our adversaries' *intentions* to attack. There is little doubt that hardening and resilience capabilities/activities are reducing adversaries' *capability* to damage or deprive the United States (i.e., supporting a strategy of defense), but policymakers should not hold false expectations that continuing to invest in these capabilities/activities will lead to changes in our adversaries' intentions to continue to attack in, through, and from cyberspace.

Deterrence Does Not Necessarily Equal Security

In the nuclear and conventional strategic environments, the central strategy for the United States for the last 70 years has been a strategy of deterrence. In both environments, the generation of a deterrence effect has been equated with security. As was argued above, when applied to the cyberspace strategic environment over the past several years, the threat of punishment appears to have deterred adversary cyberattacks equivalent with armed attack, but the overall strategic end for the United States has, nonetheless, been a gradual erosion of its power relative to adversaries over the same period.

This erosion is in many ways directly attributable to strategic gains accumulated by adversary cyber campaigns/operations short of armed attack, gains resulting from cyber campaigns or operations targeting intellectual property, military overmatch, and social cohesion. It would be dubious, then, to associate the generation of a deterrence effect in cyberspace with the realization of security in the same. And yet, early commentary on the 2018 DoD Cyber Strategy's discussion of persistent contestation argues that a measure of effectiveness of a strategy of persistent engagement (or, at least, the "defend forward" aspect of it) should be its "deterrence value" (Pomerlou 2018).

This is another example of the indiscriminate overlaying of a strategic concept associated with a strategy of deterrence (i.e., a deterrence effect) onto the cyber strategic environment. The cyber strategic competitive space below the threshold of armed conflict is characterized by constant contact manifesting in continuous engagement, enduring campaigns, and competitive interactions between friends and foes alike. As Harknett and I have argued, operational persistence is a strategic imperative for states seeking security in this space (Fischerkeller and Harknett 2017; 2018). Any strategy for cyberspace that intends to coerce comprehensive operational restraint on the part of an adversary (i.e., generate a deterrence effect) will fail because such an outcome is not aligned with the strategic imperative presented by cyberspace.

Persistent engagement accepts this imperative and, consequently, does not claim deterrence as a strategic objective. Rather we have argued that persistent engagement has an operational objective of inhibiting, not eliminating, adversary cyber campaigns or operations that threaten U.S. national interests. Additionally, it has the strategic objectives of preventing extended or enduring imbalances (negative or positive) from emerging in the cyber strategic competition below the threshold of armed conflict and supporting the development of mutual understandings with adversaries of acceptable/unacceptable behavior in the same (Fischerkeller and Harknett 2018). It is through the combination of these effects that security can be realized in this strategic competitive space.

Conclusion

A significant reorientation has occurred in U.S. strategic guidance published over the past 12 months. Strategic competition below the threshold of armed conflict is now considered a central challenge to U.S. national security, and the cyberspace strategic environment has been accepted as a primary space in which this competition occurs. This reorientation was appropriately accompanied by an adjustment to the U.S. strategic framework, one that now emphasizes the equal importance of a strategy of deterrence and a strategy of persistent engagement in ensuring national security short of armed conflict.

This article encourages strategic discipline and vigilance on the part of the defense community to hold fast and true to understandings of the structural foundations and strategic features of each so that the strategic concepts and intended effects associated therewith are not conflated, confused, or otherwise used indiscriminately. Such muddling could result in a range of inefficient or even potentially dangerous behaviors, ranging from a misallocation of scarce resources to a misconception of intended strategic effects, none of which would well serve the pursuit of U.S. national security.

References

Brantly, Aaron F. 2015. "Strategic Cyber Maneuver," *Small Wars Journal*. http://smallwarsjournal.com/jrnl/art/strategic-cyber-maneuver.

Department of Defense. 2017. *Department of Defense – Defense Science Board Task Force on Cyber Deterrence*. Washington, DC: Department of Defense.

Department of Defense. 2018a. *Summary of the 2018 National Defense Strategy of the United States of America*. Washington, DC: Department of Defense.

Department of Defense. 2018b. *Summary: Department of Defense Cyber Strategy*. Washington, DC: Department of Defense.

Fischerkeller, Michael and Richard J. Harknett. 2017. "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 61(Summer): 3.

Fischerkeller, Michael and Richard J. Harknett. 2018. *Persistent Engagement, Agreed Competition, Cyber Interactions Dynamics, and Escalation*. Alexandria, VA: Institute for Defense Analyses.

Gerson, Michael S. 2009. "Conventional Deterrence in the Second Nuclear Age," *Parameters: United States Army War College Quarterly*.

Lebow, Richard Ned. 1981. *Between Peace and War: The Nature of International Crisis*. Baltimore, MD: Johns Hopkins University.

Mearsheimer, John J. 1983. *Conventional Deterrence*. Ithaca, NY: Cornell University Press.

Mitchell, A. Weiss. 2015, August 12. "The Case for Deterrence by Denial." *The American Interest*. https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/.

Pomerlou, Mark. 2018, September 28. "It's a New Era for Cyber Operations, but Questions Remain." *Fifth Domain*. https://www.fifthdomain.com/dod/2018/09/28/its-a-new-era-for-cyber-operations-but-questions-remain/.

Rhodes, Edward. 2000. "Conventional Deterrence," *Comparative Strategy* 19: 243–47.

Snyder, Glenn H. 1958. *Deterrence by Denial and Punishment: Research Monograph No. 1*, Princeton University.

Snyder, Glenn H. 1961. *Deterrence and Defense: Toward a Theory of National Security*, Princeton University Press: Princeton, NJ.

United States Congress. 2017. *National Defense Authorization Act 2018*. S. 1519, Report No. 115-125, Section 1621, (c) Denial Options.

United States Congress. 2018. *John S. McCain National Defense Authorization Act 2019*, H.R. 5515, Section 1636, (c) Denial Options.

United States Cyber Command. 2018. *Command Vision for U.S. Cyber Command: Achieve and Maintain Cyberspace Superiority*. Washington, DC: Department of Defense.

Van Evera, Stephen. 1999. *Causes of War: Power and the Roots of Conflict*. Ithaca, NY: Cornell University Press.

White House. 2017, December. *National Security Strategy of the United States of America*. Washington, DC: White House.

Dr. Fischerkeller is a Research Staff Member in IDA's Information Technology and Systems Division. He holds a Doctor of Philosophy in international security from the Ohio State University.