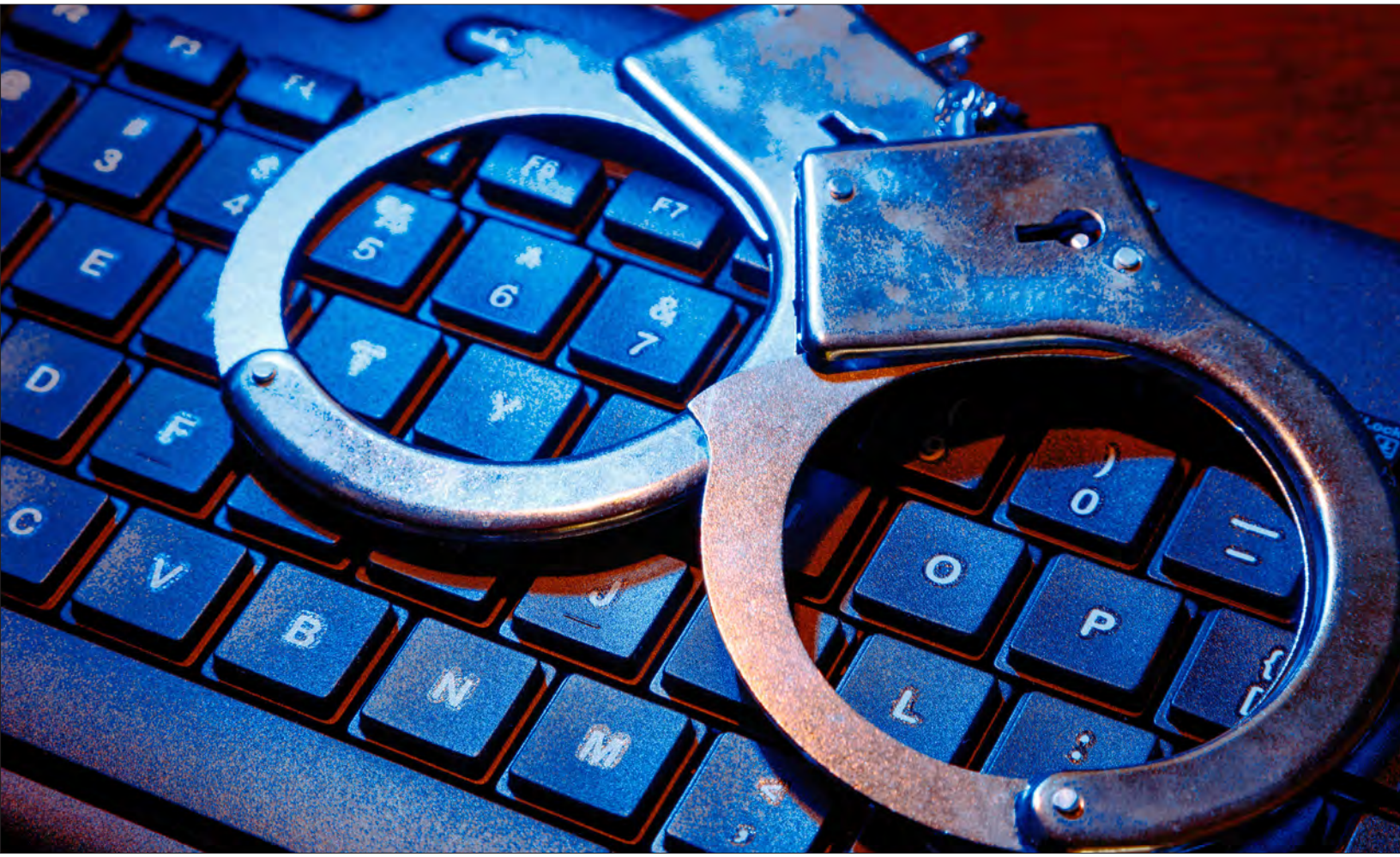
Deterrence Is Not a Credible Strategy for Cyberspace (and What Is)

Michael P. Fischerkeller and Richard J. Harknett

Much of U.S. defense policy over the past 20 years has been grounded in a deterrence framework. When the cyberspace operational domain emerged, it was promptly and similarly considered a domain of restraint and reaction, with insufficient attention paid to its unique characteristics and the strategic context. This article makes two central arguments. First, within cyberspace, the protection or advancement of national interests cannot rest on deterrence as the central strategy but can be realized through a strategic approach that captures and takes advantage of unique characteristics of the domain and the current strategic context—persistent engagement. Second, if the United States is to shape the development of international cyberspace norms that will bring stability and security, it can do so primarily through strategic cyber campaigns that begin to shape directly and indirectly the parameters of responsible behavior.



[1] The winning publication originally appeared in *Orbis* 61, no. 3 (Summer 2017): 381–393, https://doi.org/10.1016/j.orbis.2017.05.003.

Challenge of a New Domain

In a 2010 essay, William J. Lynn III, then U.S. Deputy Defense Secretary, outlined a new strategy for a new operating domain—cyberspace (Lynn 2010). In describing the strategy, consideration reasonably turned to a strategic framework to suggest norms of behavior for operating within cyberspace. Consistent with much of U.S. defense policy over the past 20 years, those norms were grounded in a deterrence framework. The operational norms associated with the air, land, and maritime domains are fundamentally derived from the centuries-old concept of Westphalian sovereignty, a structural feature rooted in segmentation (bounded territories) and derived from respect for the principle of non-intervention and territorial integrity that marked the end of the Thirty Years' War in 1648. Although specifics regarding these norms have evolved, the basic principle is still widely accepted by state actors in the international system and is codified in the United Nations Charter article 2(4), which states, "All members shall refrain in their international relations from the use of force against the territorial integrity or political independence of any state." Consistent with this language, the United States and its allies adopted and advocated for the principle of relative operational restraint associated with deterrence strategies (i.e., a "doctrine of restraint" came to anchor U.S. cyberspace strategy and inform perspectives on the substance of norms). Unfortunately, this perspective was adopted without comprehensive consideration of whether a strategy of deterrence was appropriate given cyberspace's unique characteristics and the current strategic context. It was not—as many actors realized their national interests could be advanced through strategic cyber campaigns comprised of continuous operations with strategic effects short of use of force or armed attack equivalence. While many of these actors might be considered "unlike-minded,"[2] the number and effectiveness of their aggressive cyber campaigns suggest that a sizeable number of effective actors are leveraging the U.S. default to restraint.

Uniqueness of Cyberspace

The cyberspace operational domain is defined as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Joint Chiefs of Staff 2018, GL-4). Thus, it is argued that cyberspace is uniquely a human-constructed domain, and thus malleable. Moreover, the scale and scope of this constantly shifting space is distinctive—state and non-state actors' abilities to modify other operational domains cannot occur at the pace and on the scale being witnessed in cyberspace. Strategy must recognize that there is a qualitative difference between the capacity to modify terrain and to create it whole cloth.

[2] See White House (2018, 21) for the strategy's specification of working with "like-minded" states to develop norms.

The uniqueness of cyberspace is also reflected in the low cost of entry, which allows a number of actors who can affect relative national power to operate in cyberspace that is orders of magnitude higher than the small number of states that operate with consequence in the land, air, maritime, and space operational domains. Moreover, no internationally agreed upon concept of cyberspace sovereignty prevails. This suggests a corollary—international relations (and nature) abhor vacuums; consequently, cyber security strategy should assume that states and other significant actors are continually seeking to exert their influence in cyberspace through strategic cyber campaigns or operations.

Agreement to compete robustly short of armed conflict may be the grand strategic consequence of cyberspace.

Whereas segmentation is the core structural feature of the air, land, and maritime domains, interconnectedness is the oft-cited, but rarely embraced, core structural feature of cyberspace. If one accepts interconnectedness as such, then fundamental international relations concepts for understanding or explaining actor behaviors and making strategic choices, such as sovereignty and territoriality, come into question because the core condition that follows from interconnectedness is constant contact, a term used by the United States Cyber Command (USCYBERCOM) to describe the cyberspace operating environment (USCYBERCOM 2018, 4).[3] This condition, when coupled with the nature and substance of cyberspace—a vulnerable yet resilient technological system that is a global warehouse of and gateway to troves of sensitive strategic information—encourages persistent opportunism to access and leverage those sensitive data while simultaneously requiring states to continuously seek to secure those data and data flows from others.[4] The combination of interconnectedness and constant contact with cyberspace's ever-changing character, both in "terrain" and in the capacity to maneuver across that terrain, further encourages operational persistence in order to secure and leverage critical data and data flows. When these factors are considered together, in operational reality, operational persistence/engagement (not operational restraint) becomes the appropriate strategic choice (if not imperative) for states seeking to secure and advance their interests in, through, and from cyberspace.[5] The past decade of voluminous and exploitative adversarial behavior in cyberspace suggests adversaries recognized and adapted to this imperative early in cyberspace's maturation. The consequence for the United States has been the gradual degradation of U.S. sources of national power by adversarial strategic cyber

[3] See also Fischerkeller and Harknett (2017).

[4] For a discussion of the nature, character, and substance of cyberspace and its implications for cyberspace strategy, see Fischerkeller (2018).

[5] This was the critical and concluding argument of the 2018 Welch Award–winning publication (Fischerkeller and Harknett 2017). The remainder of this article highlights extensions and applications of that argument as represented in the authors' publication (Fischerkeller and Harknett 2018).

campaigns targeting those same sources of power. This situation has not gone unnoticed by U.S. policy makers.

A strategic approach to securing national interests and pursuing norms codification in cyberspace that is based primarily on operational restraint, then, fails to take into account that the unique characteristics of cyberspace argue for a strategic approach of operational persistence. Analyses of behaviors in, through, and from cyberspace over the past decade reveal that state and non-state actors have increasingly understood and aggressively leveraged the value of cyberspace and strategic cyber campaigns short of armed conflict to support their interests. It is likely that these actors have also come to recognize that because norms emerge first through behaviors, then mature and are codified through international discourse, when the time comes for international discourse regarding codification, those who operationally dominate the domain will be in the strongest position to argue for norms supporting their positions.

Current Strategic Context

National Security Strategy of the United States of America, issued in December 2017, and its complement, *National Defense Strategy of the United States of America*, stand in marked contrast to their predecessors in their declarations that adversaries are executing strategic campaigns short of armed attack to secure and advance national interests. Indeed, both documents assert that the central challenge to U.S. security and prosperity is the re-emergence of a long-term, *strategic competition* with revisionist and rogue regimes and actors that have become skilled at operating *below the threshold of armed conflict* (White House 2017, 3, 31; Department of Defense 2018, 2). Cyberspace and its derivative cyber operations, in particular, have been identified as offering state and non-state adversaries the ability to wage strategic campaigns against American political, economic, and security interests without physically crossing U.S. borders (White House 2017, 12). This view is presented most comprehensively in *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*. Adversaries are described as continuously operating against the United States below the threshold of armed conflict—demonstrating the resolve, technical capability, and persistence to undertake strategic cyberspace campaigns to weaken U.S. democratic institutions and gain economic, diplomatic, and military advantages (USCYBERCOM 2018, 3).[6]

Strategic Approach of Persistent Engagement

Taking into consideration the unique characteristics of cyberspace and the current strategic context, USCYBERCOM recently described a strategic approach that is better aligned than deterrence with these realities. The approach

[6] Concern has been expressed regarding "the *persistence* [emphasis added] exhibited by adversary attempts to penetrate critical infrastructure and the systems that control these services" Rogers (2017, 2).

prescribes that the United States increase resiliency; defend forward as close as possible to the origin of adversary activity; and contest cyberspace actors to generate continuous tactical, operational, and strategic advantage.[7] USCYBERCOM argues that this strategic approach of *persistent engagement*—described operationally as the combination of seamless resiliency, forward defending, contesting, and countering—will compel many U.S adversaries to shift resources to defense and reduce attacks. Moreover, *persistent engagement* is expected to allow greater freedom of maneuver to impose tactical friction and strategic costs on U.S. adversaries pursuing activities that are more dangerous before they impair U.S. national power. This effort seeks to render the majority of adversary cyber and cyber-enabled activity inconsequential.

We have recently argued that through the adoption of this strategic approach, the United States would become an active participant in an ongoing *agreed competition* below the threshold of armed attack among major actors in cyberspace, all of whom are seeking to protect and/or gain strategic advantage short of armed attack through the same (Fischerkeller and Harknett 2018). The term *agreed competition* is a derivative of *agreed battle*, a term strategist Herman Kahn described as a concept rooted in factors relating to particular levels of escalation.[8] The concept emphasizes that in an escalation situation in which both sides are accepting limitations, there is in effect an agreement, whether or not it is explicit or even well understood. "Thus the term does not have any connotation of a completely shared understanding, an intention of containing indefinitely with the limitation, or even a conscious quid pro quo arrangement" (Kahn 2017, 3). From a norms-development perspective, what is important to note in Kahn's rendering is that agreement rests on *interactions* between adversaries, which, despite being complex and nuanced, can come to be understood and shared between actors. He notes that states can come to recognize "what the 'agreed battle' is and is not, what the legitimate and illegitimate moves are, and what are 'within the rules' and what are escalatory moves" (Kahn 2017, xiii).[9]

And so, to come full circle, in contrast to a strategy of deterrence, which emphasizes cyberspace operational restraint and norms establishment with like-minded significant actors, a strategic approach of *persistent engagement* emphasizes competitive interaction within an *agreed competition* and norms

---

[7] USCYBERCOM argues that superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver. It describes how USCYBERCOM would operate (maneuvering seamlessly between defense and offense across the interconnected battlespace_; where they would operate (globally, as close as possible to adversaries and their operations_; when they would operate (continuously, shaping the battlespace); and why they operate (to create operational advantage for the United States while denying the same to U.S. adversaries) (USCYBERCOM 2017, 5).

[8] Kahn attributes the term *agreed battle* to Max Singer.

[9] For a comprehensive discussion of interaction and escalation dynamics that would emerge from a strategic approach of persistent engagement, see Fischerkeller and Harknett (2018).

construction (through interaction) with all actors. Security and stability will emerge through interaction because more clarity will emerge on the demarcations between illegitimate and legitimate cyber operations and between operations outside and within the "rules" of *agreed competition*.

Conclusion

Several years ago, U.S. adversaries waded cautiously but strategically into the strategic competitive space between war and peace, perhaps most fulsomely in cyberspace. In response, the United States adopted a strategy of deterrence, one that was misaligned with both cyberspace's unique structural and operational characteristics and the strategic context. Consequently, adversaries are now pursuing aggressive strategic campaigns short of armed conflict in, through, and from cyberspace to gain strategic advantage in military, economic, and diplomatic arenas. As evidenced in recent U.S. strategic guidance, however, the United States has now recognized that it must operate persistently in this competitive space if it hopes to re-gain the upper hand on adversaries who have been reaping the benefits of their early strategic adaptation to cyberspace at the expense of U.S. national interests. A strategic approach of persistent engagement in cyberspace supports this newly adopted orientation while simultaneously, through continuous competitive interaction, supporting the development of norms of responsible behavior. Agreement to compete robustly short of armed conflict may be the grand strategic consequence of cyberspace.

References

Department of Defense. 2018. *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Fischerkeller, M. P. 2018. *Offense-Defense Theory, Cyberspace, and the Irrelevance of Advantage*. Alexandria, VA: Institute for Defense Analyses. IDA Document NS D-8939.

Fischerkeller, M. P., and R. J. Harknett. 2017. "Deterrence Is Not a Credible Strategy for Cyberspace." *Orbis* 61, no. 3: 381–393. https://doi.org/10.1016/j.orbis.2017.05.003.

———. 2018. *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation*. Alexandria, VA: Institute for Defense Analyses. IDA Document NS D-9076. https://www.idalink.org/D-9076.

Joint Chiefs of Staff. 2018. *Cyberspace Operations*. Joint Publication 3-12. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

Kahn, H. (with a new introduction by Thomas C. Schelling). 2017. *On Escalation: Metaphors and Scenarios*. London: Routledge.

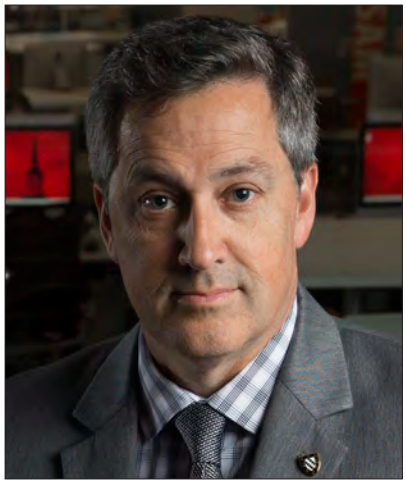
Lynn III, W. J. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

Rogers, M. S. 2017. *Statement of Admiral Michael S. Rogers, Commander United States Cyber Command, Before the Senate Committee on Armed Services, 9 May 2017*. https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf.

United States Cyber Command (USCYBERCOM). 2018. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf.

White House. 2017. *National Security Strategy of the United States of America*. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

——— 2018. *National Cyber Strategy of the United States of America*. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.



Michael Fischerkeller (with IDA President David S. C. Chu) is a Research Staff Member in the Information Technology and Systems Division of IDA's Systems and Analyses Center. He holds a doctorate in political science from the Ohio State University.

Richard Harknett (right), professor and department head of political science at the University of Cincinnati, holds a doctorate in political science from the Johns Hopkins University.