

Success of Persistent Engagement in Cyberspace

The US Department of Defense's 2018 cyber strategy is the most important development in this arena in the past 20 years.¹ It recognizes that states are continuously engaged in cyber operations and prescribes an imperative to “persistently contest” adversaries “in day-to-day competition” by, among other things, “defending forward to intercept and halt cyber threats.”² Persistent engagement is straightforward yet subtle. Countering malicious cyber activity below the level of armed conflict requires daily interaction and competition to “expose adversaries’ weaknesses, learn their intentions and capabilities, and counter attacks close to their origins.”³ US Cyber Command (USCYBERCOM) must consistently conduct operations to impose just enough friction on adversaries to moderate their behavior but not such disruption as to induce further attacks.

Academics and policy makers have debated the merits of persistent engagement, and perhaps it is indeed the correct strategy to deal with cyber conflict. However, as with the introduction of any new strategy, developing it is trivial compared to implementing it effectively against a competent adversary. At a minimum, persistent engagement requires (1) strong and sustained military and civilian leadership that embraces the strategy; (2) an organized, trained, and equipped force; (3) clear signaling to adversaries; (4) the trust of international and domestic partners; and (5) a robust interagency process. While the DOD might have the leadership and forces required to succeed, it is far from clear that the interagency process, the trust of partners, and signaling are or will be in place soon given the current political climate. Thus, the gains from persistent engagement will likely not be as significant as expected and will have a greater risk of encouraging, not discouraging, adversary attacks.

Strong and Sustained Leadership

Military strategies are useless without strong military and civilian leadership to implement and direct them—not just today but over the years (or even decades) needed for success. There is widespread agreement that USCYBERCOM commander Gen Paul Nakasone is an exceptionally well-qualified military leader.⁴ His staff and subordinates are equally well regarded.

Nonetheless, there are reasons for concern. First, it is not clear that leadership above the operational command understands the strategy and subtlety persistent engagement requires. In his confirmation testimony for appointment as chairman of the Joint Chiefs, Gen Mark Milley asserts that in cyberspace “a good offense is critical, and that is the best defense”—which may be true but is not the same as persistent engagement.⁵ This framing is similar to that of the White House and some members of Congress.

Second, the next cyber commanders may not embrace persistent engagement as fully as has General Nakasone. Continuity is more likely if the next generation gives rise to Nakasone protégés, but the next commander may be a more traditional war-fighting general eager to take the fight aggressively to the enemy. The instinct of many warriors is to triple down on aggression, losing not just the subtlety at the heart of the strategy but the strategy itself.

Effectively Organized, Trained, and Equipped Force

The United States is well along in having a properly organized, trained, and equipped cyber force. USCYBERCOM’s Cyber Mission Force (CMF) is at full operational capability with 133 teams comprising over 6,000 personnel.⁶ These teams have been operationally engaged against the Islamic State and Russian interference during the 2018 midterm elections.⁷ While they demonstrate significant capability, the CMF is not without its issues. Just five months after reaching full operational capability, many teams no longer met training standards.⁸ Given the high tempo of operations suggested by the new strategy, USCYBERCOM will be hard-pressed to keep enough trained personnel, infrastructure, and capabilities over the years or decades.

Clear Signaling to Adversaries

Perhaps the most important prediction of persistent engagement is that adversaries will learn which of their operations are far enough outside the norm as to invite significant US response. Michael Fischerkeller, a researcher at the Institute of Defense Analyses, and Richard Harknett, Political Science Department head at the University of Cincinnati, write about tacit bargaining such that over time each side will come to understand the “boundaries or limits on behaviors.”⁹ Operations that support persistent engagement are essentially a never-ending series of signals to shepherd adversaries toward preferred US norms.

Communicating intent in cyberspace is inherently difficult because operations are usually hidden and denied while offensive attacks, pre-attack reconnaissance, and espionage are hard to distinguish.¹⁰ Former National Security Agency (NSA) deputy director Chris Inglis notes that misreading “a limited action [such as routine espionage] as an existential threat” could lead to “escalating a situation in a manner unintended by the attacker.”¹¹ Despite this risk, there is a near total lack of communication between adversaries outside the arena of competition itself, inviting mistake and miscalculation. There is no direct contact between the DOD and the Chinese military as China’s leadership is still incensed over a signaling attempt: the US indictment of five Chinese cyber officers. There is also no direct contact between US and Russian militaries, though at least there are hotlines to connect the White House with the Kremlin and between each side’s computer emergency response teams.¹²

Hawkish rhetoric creates further uncertainty about US intentions. While US Cyber Command discusses persistent engagement primarily as a defensive strategy, the White House thinks of it as an offensive one. This gap will magnify the opportunities for mistake and miscalculation.

Even if adversaries detect and understand US signals, they may not be sure that the punishment will stop if they comply with US preferences.¹³ Could Russia’s or China’s leadership be confident that if it moderated its cyber operations against the United States, its respective countries might not still suffer covert action, espionage, indictments, sanctions, or “hostile” cross-border information that threaten regime stability?

Trust of International and Domestic Partners

The new strategy recognizes the importance of partnerships, emphasizing that the DOD “will collaborate with our interagency, industry, and international partners to advance our mutual interests.”¹⁴ However, there are conflicting interests as well as mutual interests in stopping adversary cyber operations. Persistent engagement and forward defense blur the lines between adversary (red space), US (blue space), and other networks (gray space). With these euphemisms, it can be easy to forget that gray space is typically shorthand for someone else’s property physically located in a country with which the United States is at peace.

Previously, cyber operations that would deliver an effect in red or gray space required extensive interagency coordination, often the approval of the president.¹⁵ Under this new strategy, and related authorizations by Congress and the White House, US cyber forces will have more freedom

of action to pivot with adversaries and disrupt threats in or through the networks of friendly nations.¹⁶

As Max Smeets of the Center for Security Studies at ETH Zurich remarks, “by operating in allied networks, Cyber Command is running the risk of causing the wrong type of friction,” eroding allied trust in the United States.¹⁷ Those nations will surely often be no happier with this policy than many in the United States government would be if French cyber warriors took down Russian targets in Wisconsin. Just because the US military sees itself as liberating other nations’ computers from adversary occupation does not mean cyber GIs will be greeted with open arms.

Perhaps, in more normal times, partners might trust US intentions. But even the closest and most trusted US allies are feeling antagonized by recent decisions and actions of the United States. Extraterritorial US cyber operations may be perceived as just more bullying, to be resisted even if the outcome is beneficial. Smeets’s suggestion for “memoranda of understanding on offensive cyber effects operations in systems or networks based in allied territory” is a step in the right direction.¹⁸

US technology companies will be key partners to securing cyberspace but have not forgotten the revelations of Edward Snowden. “As story after story emerged alleging that the NSA undermined encryption, hacked into cables carrying the data of U.S. companies, placed implants and beacons in servers and routers, and generally weakened Internet security,” observes cybersecurity expert Adam Segal, “policymakers failed to comprehend the depth of Silicon Valley’s anger.”¹⁹ If another Snowden-type revelation explodes, or more US military cyber weapons get stolen or leaked, the public-private partnerships called for in the strategy may disintegrate.²⁰

Robust Interagency Process

The latest National Cyber Strategy states that the US will use “diplomatic, information, military, . . . financial, intelligence, public attribution, and law enforcement capabilities” to counter malicious cyber activity—coordination that is especially needed to send clear signals and reassure partners.²¹

Shaping adversary behavior and improving stability require synchronized policy and operations across at least the National Security Council; Office of the Director of National Intelligence; Federal Bureau of Investigation; and Departments of State, Justice, Treasury, and Homeland Security. Coordinating these agencies has never been an easy task, yet the White House eliminated the cyber security coordinator position

in May 2018, and the Trump administration is already on its fourth national security advisor.²²

Conclusion

Offensive cyber operations can lead to “significant strategic advantages” for states, both the United States and its adversaries.²³ Persistent engagement may be the best chance to reduce conflict and return to a more secure cyberspace. But too many of the required elements are lacking to feel particularly confident.


Though the United States has strong military leadership and is building an effective cyber force, there are shortcomings in signaling to adversaries, building trust with partners, and establishing interagency coordination. Unfortunately, we cannot simply wish this were different or ignore the domestic and international political context.

Optimists and hawks may argue that having perhaps two of the five required elements is “good enough.” Some of the five elements could be merely preferable rather than strictly necessary, and these days even a weakly implemented strategy may be better than the alternatives. Incomplete advancement might still lead to significant national security gains or strategically delay adversaries long enough for the United States to develop the missing elements.

Pessimists will fear that persistent engagement might instead be like jumping a motorcycle across the Grand Canyon. Clearing two-fifths of the gap is a heroic feat but failure nonetheless—and may not be worth attempting without a greater chance of success. Defending forward could prompt adversaries to attack more, not less; international allies might see the United States as an adversary and not a partner; and US citizens and technology companies may believe that the US government cares more about taking the fight to the enemy than securing cyberspace, digital rights, or online privacy.

Persistent engagement may only be successful when used sparingly at the margins during a time of relative peace, when the effects on adversary operations, allies, and partners are easily overlooked. However, it may engender a harsher reaction when executed at scale—the main effort of a public and seemingly offensive strategy—or during a significant geopolitical crisis.

These issues might have been addressed when the strategy was still just an excellent idea rather than after its launch as the heart of a major military strategy. Now, government and military officials must shift attention to the lagging elements and, with researchers, track the effects of

the strategy to see if it is indeed stabilizing or inducing adversaries to step up their attacks.²⁴ 

Jason Healey

Senior Research Scholar
School of International and Public Affairs
Columbia University

Stuart Caudill

Master's Candidate
Columbia University

Notes

1. Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019): 5, <https://doi.org/10.1093/cybsec/tyz008>.

2. Department of Defense, *Summary: Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, September 2018), 4, <https://media.defense.gov/>.

3. US Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Fort Meade, MD: US Cyber Command, April 2018), 6, <https://www.cybercom.mil/>.

4. Ellen Nakashima, "Incoming NSA Chief Has a Reputation for Winning 'All the Important Fights.' Russia Will Be His Biggest Test Yet," *The Washington Post*, 1 April 2018, <https://www.washingtonpost.com/>.

5. United States Senate, Committee on Armed Services, "Hearing to Consider the Nomination of: General Mark A. Milley, USA, for Reappointment to the Grade of General and to Be Chairman of the Joint Chiefs of Staff," 11 July 2019, transcript, 116th Cong., 1st sess., 64, <https://www.armed-services.senate.gov/>.

6. US Cyber Command Public Affairs, "Cyber Mission Force Achieves Full Operational Capability," 17 May 2018, <https://www.cybercom.mil/>.

7. Dina Temple-Raston, "How the U.S. Hacked ISIS," NPR, 26 September 2019, <https://www.npr.org/>; and Julian E. Barnes, "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *The New York Times*, 26 February 2019, <https://www.nytimes.com/>.

8. Government Accountability Office, *DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*, GAO-19-362 (Washington, DC: Government Accountability Office, March 2019), 17, <https://www.gao.gov/>.

9. Michael Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare* (blog), 9 November 2018, <https://www.lawfareblog.com/>.

10. For example, see Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (May 2017): 452–81; and Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48.

11. Chris Inglis, "Illuminating a New Domain: The Role and Nature of Military Intelligence, Surveillance, and Reconnaissance in Cyberspace," in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, eds. Herbert Lin and Amy B. Zegart (Washington, DC: The Brookings Institution, 2018), 32.

12. Sean Gallagher, "US, Russia to Install 'Cyber-Hotline' to Prevent Accidental Cyberwar," *Ars Technica*, 18 June 2013, <https://arstechnica.com/>
13. Borghard and Lonergan, "The Logic of Coercion in Cyberspace," 471.
14. Department of Defense, *Summary: Department of Defense Cyber Strategy*, 1.
15. Eric Geller, "Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand," *POLITICO*, 16 August 2018, <https://politi.co/2MSWCnS>.
16. Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," 5.
17. Max Smeets, "Cyber Command's Strategy Risks Friction with Allies," *Lawfare* (blog), 28 May 2019, <https://www.lawfareblog.com/>.
18. Max Smeets, "NATO Allies Need to Come to Terms with Offensive Cyber Operations," *Lawfare* (blog), 14 October 2019, <https://www.lawfareblog.com/>.
19. Adam Segal, "The Internet Is Undermining America's Power," *Time*, 22 February 2016, <https://time.com/>.
20. Dan Goodin, "Stolen NSA Hacking Tools Were Used in the Wild 14 Months before Shadow Brokers Leak," *Ars Technica*, 7 May 2019, <https://arstechnica.com/>.
21. The White House, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 21, <https://www.whitehouse.gov/>.
22. Nicole Perloth and David E. Sanger, "White House Eliminates Cybersecurity Coordinator Role," *The New York Times*, 15 May 2018, <https://www.nytimes.com/>.
23. Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (Fall 2018): 105, <https://www.airuniversity.af.edu/>.
24. Jason Healey and Neil Jenkins, "Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence Is Working or Failing," in *11th International Conference on Cyber Conflict: Silent Battle*, eds. T. Minarik et al. (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence Publications, 2019), 1–20, <https://ccdcoe.org/>.

Disclaimer and Copyright

The views and opinions in *SSQ* are those of the authors and are not officially sanctioned by any agency or department of the US government. This document and trademarks(s) contained herein are protected by law and provided for noncommercial use only. Any reproduction is subject to the Copyright Act of 1976 and applicable treaties of the United States. The authors retain all rights granted under 17 U.S.C. §106. Any reproduction requires author permission and a standard source credit line. Contact the *SSQ* editor for assistance: strategicstudiesquarterly@us.af.mil.