Paradigm Change Requires Persistence – A Difficult Lesson to Learn

Dr. Emily O. Goldman

Persistent engagement and defend forward are new cyberspace concepts and approaches that are gaining traction across the cyber enterprise. They challenge the assumptions and prescriptions of deterrence theory and thus require perseverance in ensuring the right lessons are learned. Claims by some that SolarWinds represents a failure of these approaches misses the mark in many respects, most of all by applying deterrence metrics inappropriately. Rather, recent experience has demonstrated that competition in cyberspace is going to be continuous. Competing requires persistence rather than episodic responses, and anticipation rather than reaction.

2018 Shift

When future historians look back at 2018, they will see it as a pivotal year in the evolution of the United States' (US) cyberspace strategy. The unlearned cyber lessons from previous years took form in strategy and policy in 2018. US political leaders, operational commanders, military strategists, and scholars worked out a theory about the nature of cyberspace conflict and competition, how to confront national-security threats emanating from cyberspace, and ways to employ cyberspace capabilities as a tool of national power. Persistent engagement and defend forward are new cyberspace concepts and approaches that challenge the previously dominant assumptions and prescriptions of deterrence theory and thus require perseverance in ensuring the right lessons are learned and applied. Experience has demonstrated that competition in cyberspace will be continuous. The lesson is that it requires persistence rather than episodic responses, and anticipation rather than reaction.

Dr. Emily Goldman serves as a strategist at U.S. Cyber Command and a thought leader on cyber policy. She was cyber advisor to the Director of Policy Planning at the Department of State, 2018–19. From 2014 to 2018 she directed the U.S. Cyber Command / National Security Agency Combined Action Group, reporting to a four-star commander and leading a team that wrote the 2018 U.S. Cyber Command vision, *Achieve and Maintain Cyberspace Superiority.* She has also worked as a strategic communications advisor for U.S. Central Command and for the Coordinator for Counterterrorism at the State Department. She holds a doctorate in Political Science from Stanford University and was a professor of Political Science at the University of California, Davis, for two decades. Dr. Goldman has published and lectured widely on strategy, cybersecurity, arms control, military history and innovation, and organizational change.

In March 2018, U.S. Cyber Command (USCYBERCOM) released its *Command Vision* introducing the concepts of defend forward and persistent engagement. In September 2018, the U.S. Department of Defense (DoD) declared in its new cyber strategy, "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict," and "[p]ersistently contest malicious cyber activity in day-to-day competition." Defend forward and persistent engagement pivoted US cyber teams from a "response force" to a "persistence force" and represented the shift from a coercive strategy aimed at preventing cyberspace attacks by threatening to impose costs on bad actors to an initiative-persistent strategy aimed at thwarting and frustrating adversaries before they lock in gains.

This new conception of operations in cyberspace supplemented the longstanding coercion paradigm that still holds sway in policy deliberations among strategic theorists and practitioners alike. The legacy coercion framework views strategy in terms of deterrence and compellence, even though deterrence was advanced during the Cold War to address a novel and acute problem: how to secure with nuclear weapons when you cannot defend against them. Deterrence thus rests on credible threats to impose costs to influence the adversary's cost-benefit calculus to deter or compel their behavior. In cyberspace, however, the opponent's calculus is a given: they are expected to persist because entry costs are low, attribution is not timely, redlines are ambiguous, and pervasive system vulnerabilities invite exploitation for strategic gain.

Insights Gained and Accumulated into Broader Lessons

We are beginning to grasp early lessons from this shift in strategic thinking for cyberspace. The operational approach of persistent engagement emerged from Operation Glowing Symphony (OGS), USCYBERCOM's first global-scale operation to persistently disrupt and

degrade ISIS media infrastructure. General Paul Nakasone (then Commander of Joint Task Force-Ares) observed that one of the first things learned during OGS was that threats are not going to stop after one engagement. Rather, they will be continuous and require persistence. The operation lasted seven months and dramatically reduced the scale and speed of the virtual caliphate's media voice. Operational learning has thus informed learning at the policy and strategy levels. Consider this a primer on insights gained over the past five years. What have we learned?

1. Cyberspace is strategically consequential and US adversaries seeking strategic effects from cyberspace operations do so to defend themselves against perceived "Western" ideological (i.e., liberal democratic) subversion of their regimes, to resist sanctions, and to advance their interests at US expense. Operations and activities in and through cyberspace enable dictators and other bad actors to affect sources of national power (thus having strategic impact). They seek to protect their regimes through continuous campaigns of cyber operations, including the theft of intellectual property at-scale to reduce the economic advantages of the US and its allies, supply chain disruption and manipulation, and theft of Western military R&D to erode military superiority in key technologies. Disinformation and information manipulation undermine political cohesion in the West, delegitimizing democratic institutions and processes, and harming alliances. Since strategic effects can be achieved through actions short of war, authoritarian states and non-state actors will continue to experiment in this cyber competitive space, whether we respond or not. The bottom line is that cyberspace competition is strategically consequential, not because it could be a step toward escalation to armed conflict. Thinking about competition principally as a step toward war misses how actions in competition can secure strategic victory before ever approaching the war-fight.
2. In cyberspace, gains are cumulative. Any single action, hack, or incident alone might not be strategically consequential, but cumulatively the results can be of great strategic impact. It is insufficient to concentrate on preventing significant incidents or catastrophic attacks during ongoing campaigns comprised of activities whose individual effects never rise to the level of a significant incident, and therefore rarely elicit a timely response, yet which cumulatively produce strategic gains.
3. Cyberspace campaigns against US and allied interests are continuous and ongoing across space and time, so too must our approach be to thwarting them. There is no operational pause. This does not mean being everywhere all the time; it does mean that the struggle to retain the initiative in cyberspace is enduring. As General Nakasone explained, "Superiority in cyberspace is temporary; we may achieve it for a period of time, but it's ephemeral. That's why we must operate continuously to seize and maintain the initiative in the face of persistent threats." This requires a campaigning mindset that recognizes security and stability in cyberspace flow from deliberate, cumulative action, not the threat of prospective action.

4. Being assertive and active does not mean being aggressive or offensive. Much of the activity associated with defend forward allows the US to be anticipatory about resilience, in other words defending forward in time. It often employs defensive measures undertaken with consent of the system or device owner and/or the state in whose territory cyber infrastructure resides. Yet enhancing resilience—as necessary as it is—is insufficient by itself. Action does not undermine stability; rather, restraint in the face of continuous aggression is destabilizing because it incentivizes aggressors to continue to operate with impunity and leads to de facto norms antithetical to our interests and values. Unlike nuclear weapons, the strategic effect of cyber capabilities comes from their use, not their mere possession.
5. Fears about escalation have not materialized. We have yet to see escalation out of the cyber competition space into armed conflict. Adversaries have been emboldened—arguably, by our restraint—but emboldened behavior within the cyber competition space is not the same as escalation out of competition and into armed conflict. We have demonstrated that we can preclude and disrupt cyber aggression without escalating to armed conflict.
6. Cyberspace operations have become a standard tool in diplomacy and competition between states. Restraint above the armed attack threshold occurs alongside routinization below that threshold in continuous campaigns of non-violent operations. And what works to deter catastrophic or armed-attack equivalent cyber-attacks has not dissuaded adversaries from routinely operating in and through cyberspace for strategic influence. Cyber aggression below armed conflict is not an anomaly but rather signals the emergence of a new competitive space where agreement over the substantive character of acceptable and unacceptable behaviors is immature. The lens of persistent engagement views as normal occurrences what many policymakers describe as deterrence strategy failures.
7. What matters most in cyber strategic competition short of armed conflict is not that capabilities are forward, but that cyber forces are engaging and seizing initiative. Defend forward is not synonymous with "forward defense" or "forward positioning" as practiced by the US and NATO during the Cold War, when troop presence near international borders signaled readiness and enhanced deterrence. Defend forward is not about messaging through force posture and disposition. It is about actively operating and engaging to shift the balance of initiative in one's favor, and upon gaining initiative (i.e., defending forward in time), to structure the playing field and force the opponent to play on a field that better suits your strengths.
8. The reflexive use of impose cost in cyberspace strategy and policy is misplaced. Because of the strategic imperative to be active in cyberspace, our energy and resources would be better spent precluding adversary options for exploitation rather than trying to alter

their cost-benefit calculus to act. The objective should be to shift the composition of the adversary's portfolio of cyber activities in a manner that benefits us.

9. Redlines are notoriously difficult to define in cyberspace. Adversaries have been adept at designing their intrusions and disruptions around the redlines we defined only after we endured earlier intrusions and compromises. Calls for setting redlines leaves us one step behind and always reacting while opponents set the timing, tempo, and terms of competition.

10. Metrics designed for the coercion/conflict space do not fully apply in competition. The metric of success for defend forward and persistent engagement is not the absence of action, but rather sustained initiative that constrains the adversary's freedom of maneuver and renders their actions strategically inconsequential. We should be anticipating how we will be exploited, taking away exploitation opportunities from the adversary that are likely to result in strategically consequential effects, and setting the conditions of security in cyberspace to support our interests and values.

Principles of Cyberspace

Paradigms reflect deeply held, taken-for-granted assumptions about how the world works, which can cause lessons to remain unlearned for some time. Outdated paradigms are difficult to change—despite mounting evidence that their utility has declined. Sanctions, indictments, expulsions, designations, and naming and shaming can all in principle constrain an adversary's freedom of maneuver by exposing bad behavior, but they are not likely to impose sufficient costs to deter (prevent from acting) or compel (stop acting). Response *per se* does not deter; only responses that outweigh benefits can change the perceptions and behavior of an ideologically motivated actor. Labeling every response as "cost imposition" does not make it so. Relying on redlines and responding to incidents after-the-fact have not stemmed malicious cyberspace activity, and there is no reason to believe such measures will suddenly dissuade authoritarian sponsors of cyber misbehavior. More of the same will not produce different results—no matter how often senior leaders call for a coherent deterrence strategy for cyberspace.

The cyber strategic environment with its dynamic terrain, regenerating capabilities, low entry costs, anonymity, pervasive vulnerabilities, and prospect of cumulative gains rewards continuous action, initiative-seeking, and sustained exploitation. From this list, we can derive key principles to guide cyberspace policy, strategy, and operations, thus implementing the key lessons-to-be-learned. In this case, seven principles borne of experiences are now readily available.

- Superiority in cyberspace is temporary and advantage favors those with initiative; thus, we must operate to seize and maintain initiative.
- One-off cyber operations are unlikely to defeat adversaries; thus, we must compete continuously.

- Continuous campaigns of non-violent operations in and through cyberspace can have strategic effects; thus, we must compete now as well as prepare for future crisis and armed conflict.
- If we are defending inside our networks, we have lost initiative; thus, we must defend forward, outside our system boundaries, as close as practicable to the source of malicious activity.
- Toeholds must not become beachheads; thus, we must hunt on our networks rather than wait for intrusions to become compromises.
- Gains in cyberspace are cumulative; thus, we must employ a campaigning mindset rather than treat incidents and intrusions as discrete events.
- The strategic value of cyber capabilities lies in their use, not their possession; thus, we must act with precision and be risk informed, not risk averse.

In sum, the overarching lesson to be learned is to persevere with persistence across all seven principles.

The views expressed in this article are those of the author and do not reflect official positions of the Department of Defense or any U.S. government entity. More extensive development of the core arguments and lessons appears in Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, Cyber Persistence: Redefining National Security in Cyberspace, (forthcoming, Oxford University Press, 2022).