Rough and Ready:
Frameworks to Measure Persistent Engagement and Deterrence[1]

Jason Healey and Neil Jenkins

The 2018 U.S. Department of Defense (DoD) Cyber Strategy marked a significant departure from previous policy regarding the United States' use of force in cyberspace. The new strategy seeks to "persistently contest malicious cyber activity in day-to-day competition" by "defending forward to intercept and halt cyber threats."[2] The goal of this strategy is to reduce the effectiveness of nation state adversaries and deter them from further malicious cyber activity against the United States. The strategy seeks deterrence through cost imposition, both by offensive cyber activity and by outside means such as sanctions and indictments.

While this strategy will, by design, result in increased U.S. offensive cyber operations, the Trump administration contends that this is a necessary component of efforts to deter adversaries in cyberspace. National Security Advisor John Bolton emphasized this when he noted that the administration has approved increased offensive cyber operations "precisely to create the structures of deterrence that will demonstrate to adversaries that the cost of their engaging in operations against us is higher than they want to bear."[3]

The Debate Over Persistent Engagement and Deterrence

This emphasis on the use of cyber capabilities instead of simply the possession of capabilities and the implied or overt threat of their use is a significant aspect of this strategy. General Paul Nakasone, the commander of U.S. Cyber Command and the Director of the National Security Agency, argued in a recent interview that "in cyberspace it's the use of cyber capabilities that is strategically consequential. The threat of using something in cyberspace is not as powerful

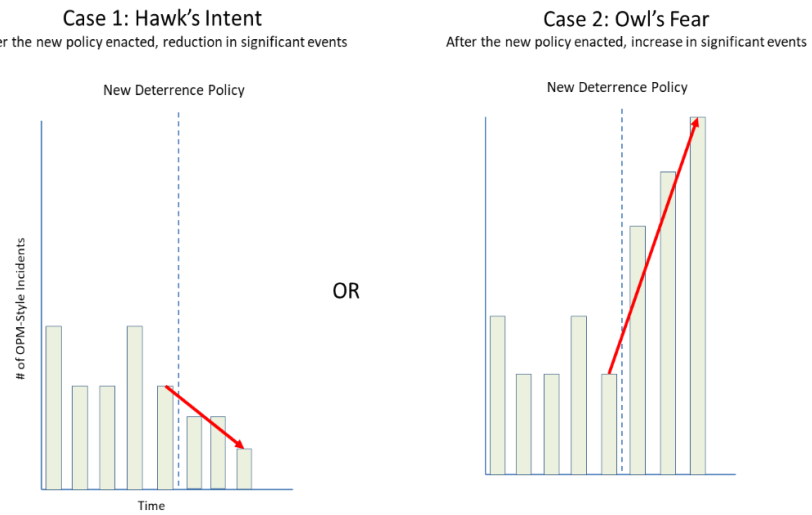
[1] This whitepaper is based on a paper presented at the 11th International Conference on Cyber Conflict: J. Healey and N. Jenkins, "Rough-and-Ready: A Policy Framework to Determine If Cyber Deterrence Is Working or Failing," in *2019 11th International Conference on Cyber Conflict (CyCon)*, vol. 900, 2019, 1–20, https://doi.org/10.23919/CYCON.2019.8756890.

[2] "Summary: Department of Defense Cyber Strategy" (U.S. Department of Defense, September 2018), 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[3] John Bolton, "Transcript: White House Press Briefing on National Cyber Strategy," September 20, 2018, https://news.grabien.com/making-transcript-white-house-press-briefing-national-cyber-strateg.

as actually using it."[4] The mere possession of cyber capabilities is not enough, Nakasone argues, because adversaries are actively engaging the U.S. in cyberspace every day.[5] If an adversary is actively stealing U.S. data, merely possessing the capability to disrupt them, but not using it, does nothing to improve the U.S. position. The use of cyber capabilities allows the U.S. to both demonstrate its capability and directly impose costs on an adversary.

Those who support the new DoD policy, who we dub "hawks," argue that a more forceful approach in cyberspace will lead to deterrence and tamer adversaries. Those who question the policy, who we dub "owls," are concerned that increased offensive cyber operations will backfire and lead to increased attacks in response. Hawks therefore argue that increased offensive cyber operations to counter adversary activity introduces "negative feedback," shepherding adversaries back to previous, more stable norms and decreasing potentially de-stabilizing incidents. On the other hand, owls recognize that there is no evidence either way, but fear that that U.S. counter-offensives will result in "positive feedback," amplifying current trends and increasing reckless and potentially de-stabilizing incidents.[6]



[4] Paul Nakasone, "An Interview with Paul M. Nakasone," *Joint Forces Quarterly*, no. 92 (2019): 4.
[5] Nakasone, 4.

[6] Healey and Jenkins, "Rough-and-Ready," 9.

Three Frameworks to Measure Cyber Deterrence and Persistent Engagement

Whether the new policy results in positive or negative feedback requires metrics that allow the U.S. to objectively measure the results of this new policy on adversary activity. The clandestine nature of most cyber operations, as well as the inherent difficulties of measuring deterrence, makes a conclusive determination of the success or failure of this new U.S. cyber strategy impossible. However, "rough-and-ready measurements of the scope and number of cyber incidents can suggest the impact of persistent engagement and deterrence."[7]

Framework 1: USG Incident Severity System

The U.S. government already classifies cyber incidents using a five-tier system. Those incidents classified as a level 3 or above are considered "significant cyber incidents," and such incidents could simply be tallied over time to determine trends.[8]

The strengths of this approach include that the five-tier system is already used by the U.S. government and thus could be immediately and easily implemented; it would include non-public incidents known to the government, but not openly acknowledged; and it could be correlated with classified U.S. government actions and operations. However, the results may be classified, limiting its utility for researchers and the private sector and provides little insight into causation of any observed changes.

Framework 2: Tracking of Significant Incidents

A second framework would involve tracking particularly significant incidents that meet a certain threshold, as by Bolton, who said the goal of the new policy was to deter incidents like the 2015 Office of Personnel Management (OPM) data exfiltration. This statement can be taken literally, so that to be a success, the number of OPM-style incidents should ideally decrease. This framework would require (1) a description of the characteristics of an "OPM-

[7] Healey and Jenkins, 7.
[8] "NCCIC Cyber Incident Scoring System | CISA," n.d., https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System.

style incident," (2) the classification of past incidents that fit that description, and (3) tracking of any new incidents that also meet this threshold.[9]

Compared to the first framework, this approach is directly tied to policy goals and allows for more analytical transparency since most "OPM-style" incidents would be disruptive and likely to be publicly known. If the number of "OPM-style" incidents decreases over time this suggest that perhaps the policy is imposing negative feedback and is therefore working as intended. If rather the number goes up, then it may be actually a far stronger signal that the policy is not working, as the proponents of persistent engagement and deterrence argue that they should be uniquely successful, perhaps the most important defensive step the United States has ever taken. Therefore, anything other than a correspondingly sharp decrease puts the new policy in trouble.

Framework 3: Deep Dive on Particular Adversary/Goal Pairings

The first two frameworks focus on tracking overall cyber incidents, which limits their utility for determining the effects of a policy on particular adversaries or particular types of incidents. A framework that focuses on tracking incidents or campaigns attributed to a specific adversary allows for metrics more readily tied to policymaker goals. For example, such a framework could track the trend of Chinese cyber activity against the U.S. after the 2015 Obama-Xi agreement.[10]

This deep dive framework allows for more detailed metrics and more analytical specificity. However, once again, it is difficult to correlate incident trends with specific U.S. actions, and this approach requires significantly more effort to track campaigns than the first two, more general, frameworks.

Shortcomings of the Three Frameworks

Measurements Swamped by Technical Developments: A significant challenge in measuring the effect of actions in cyberspace is that it is difficult to distinguish between the effect of

[9] Healey and Jenkins, "Rough-and-Ready," 8.
[10] Healey and Jenkins, 9.

those actions and the effect of technical developments. Technical improvements in either offensive or defensive capabilities could result in increases or decreases in cyber incidents that have nothing to do with changes in U.S. policy or actions. Such technical effects can be limited by comparing incident trends of various adversaries and by referencing the assessments of cyber intelligence analysts who are tracking both adversary and technical developments.

Difficulties of acquiring data: Another significant challenge is that cyber incidents and their impacts are often unknown, at least publicly. Adversaries usually go to great lengths to obfuscate their operations and their motivations. This makes it particularly difficult to determine whether changes in adversary behavior are the result of U.S. actions or other geopolitical events. However, the measurement does not need to be exact and the general direction and magnitude of incidents should give to have a rough indication of the strategy's success or failure.

Methodological Shortcomings: A third set of challenges deal with methodological issues which will stymie the determination of causation and correlation. The system is chaotic so cause and effect may be indistinguishable and there may be significant time lags between cyber incident and their discovery. There may be so few truly dangerous attacks that an increase or decrease of a small number of incidents leads to an enormous percentage increase or decrease. These factors would inhibit any assessment of the success of nearly any adversary-centric cyber strategy. The best we can do is to structure the data and frameworks as appropriately as possible … or to give up trying any measurement.

Conclusion

The debate over the merits of persistent engagement cannot be resolved through conjecture. The frameworks presented here would provide some rough metrics to allow policymakers to objectively assess the impact of this new cyber strategy and therefore determine whether the admittedly more aggressive U.S. posture is worth the accompanying risks.