INSTITUTE FOR DEFENSE ANALYSES

The Cyberspace Solarium Report and Persistent Engagement: A Response to Ben Jensen

Michael P. Fischerkeller, *Project Leader*

Final
March 2020

IDA Non-Standard
NS D-13141

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-14-D-0001, Project C5107, "Cyberspace Operations Working Group," for the IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For More Information

Michael P. Fischerkeller, Project Leader
mfischer@ida.org, 703-845-6784

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Copyright Notice

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Non-Standard NS D-13141

The Cyberspace Solarium Report and Persistent Engagement: A Response to Jensen

Michael P. Fischerkeller, *Project Leader*

The Cyberspace Solarium Commission Report and Persistent Engagement:

A Response to Ben Jensen

Michael P. Fischerkeller

In the recently released Cyberspace Solarium Commission (CSC) report, the Congressional commission re-affirmed Congress' ongoing support for the Department of Defense's (DoD) Defend Forward (DF) strategy as operationalized through persistent engagement (DF/PE) by U.S. Cyber Command (USCYBERCOM). Indeed, Pillar Six (Preserve and Employ the Military Instrument of Power) of the proposed CSC national strategic approach for cyberspace—layered deterrence—focuses entirely on DF/PE within the context of the military instrument's contribution to CSC's proposed approach. And yet, shortly after the release of the CSC report, Ben Jensen, a staff member with the Commission, questioned the strategic approach of persistent engagement. There is a glaring disconnect between the Jensen essay and the CSC report supporting PE, as well as the related CSC essays authored by Erica Borghard and Mark Montgomery and Laura Bate, Phoebe Benich, Val Cofield, Kerrie Jefferson, Ainsley Katz, and Sang Lee, which followed the report's release. If we are to gain maximum benefit from the work of the CSC, there must be accurate discussion of it and, importantly, accurate understanding of its components, including DF/PE and how it complements the construct of layered deterrence.

The Jensen essay's disconnects are many. First, he makes reference to a "false promise" of "persistent offensive cyber operations" for, presumably, providing security. The reference to PE may appear slightly obtuse here but, redirecting to the hyperlink he provides, one sees a report critical of PE, which he authored, not the CSC report itself. The characterization of PE as comprising "persistent offensive operations" and being "more offensive than defensive" is not consistent with how the CSC report describes DF/PE in Pillar Six, how PE is described in USCYBERCOM's Command Vision, nor how Harknett and I describe it in our work. Moreover, Borghard and Montgomery state that the layered deterrence strategic approach "should explicitly and deliberately clarify the fact that defend forward is an inherently defensive strategy—despite the fact that there are offensive components at the tactical and operational levels." Additionally, Jensen's claim of a "false promise" of security is not supported by the empirical record. There are three open-source reported cases of specific and successful USCYBERCOM efforts enabled by the strategic approach of DF/PE: securing the U.S. 2018 mid-term elections from external interference, generating cyber-enabled effects against Iranian ship tracking capabilities in response to Iran's kinetic attack on a U.S. RQ-4 Global Hawk drone, and Operation GLOWING SYMPHONY. Importantly, these represent efforts across the full spectrum, from competition short of armed conflict through militarized crises and into armed conflict. Also, Borghard and Montgomery and Bate, et al. note that DF/PE contributes to security by supporting norms construction, a position Harknett and I have maintained in our published articles. They state, respectively, "to be meaningful, norm-building initiatives must be coupled with consistent (and, when possible, collective and transparent) action to support and enforce them when they are violated. In addition to law enforcement, sanctions, and collective attribution efforts after norms are violated, defend forward cyber operations can help establish norms the U.S. seeks to promote in the first place" and "U.S. norms-based international engagement and military activities under defend forward don't just serve the shared goal of deterrence; in fact, they complement one another." The CSC report is aligning with, not disregarding, the writings on and application of DF/PE.

The essay seemingly argues for the superiority of layered deterrence over DF/PE by noting the former is a "whole of nation" approach, but Harknett and I have previously published that a "whole of nation +" approach is necessary to blunt adversary strategic gains in and through cyberspace and that PE could be an anchor for a national strategy for cyberspace. Again, the CSC report's proposed strategic approach actually aligns with our perspective. Although the report positions DF/PE in layer 3, it notes in section 6.1.2 that USCYBERCOM's contribution to VirusTotal of malware discovered through DF/PE supports the broad objective of layer 2 (deny benefits) and, more specifically, Pillar Five (operationalize cyber collaboration with the private sector). Providing this service, the report states, allows the private sector an opportunity to develop response plans and potentially inoculate their systems to avoid harm. Additionally, as referenced previously, Borghard and Montgomery and Bate et al. concur with our views that DF/PE also contributes to the broad objective of layer 1 (shape behavior) by supporting norms construction and reinforcement and, more specifically, Pillar Two (strengthen norms and non-military tools).

PE's fundamental strategic principle of seizing the initiative could (and should, in my view) be the basis of a national cyber strategy and a national framework for strategic competition short of armed conflict. Indeed, upon reviewing the 2019 National Defense Authorization Act language calling for the Cyberspace Solarium Commission, some, myself included, shared an expectation that one of the task forces would explore those very notions, but that did not come to pass. That said, PE's strategic principle is reflected in the CSC report, albeit through an elevation of aspects of the DoD DF strategy to a national strategic concept of Defend Forward, a concept the CSC report argues should be a core element of a new national cyber strategy. To wit, the CSC report says "Defend Forward posits the United States must shift from responding to malicious behavior after it has already occurred to proactively observing, pursuing, and countering adversary operations and imposing costs to change adversary behavior." This aligns nicely with the USCYBERCOM Vision's view of PE's strategic principle as seizing the initiative to set the conditions of security. Indeed, the CSC report argues that "This posture [Defend Forward] implies persistent engagement with adversaries as part of an overall integrated effort to apply every authority, access, and capability possible (e.g., laws, financial regulation, diplomacy, education) to the defense of cyberspace in a manner consistent with international law." And so it seems that, as a matter of fact, PE's core strategic principle of seizing the initiative is the very heart of the DIMEFIL-focused, Defend Forward concept, where DIMEFIL represents all national sources of power (Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement).

To build on the work of the CSC, let's push harder for greater clarity. For example, although the PE-spawned construct of DF takes a higher profile in the CSC report, we might benefit from more thinking about "big DF" (the national-level concept) and "little DF" (the DoD strategy). Borghard and Montgomery argue "big DF" is represented by "forces and capabilities … forward-positioned, both geographically and virtually. This is analogous to historical strategies of forward defense, which was the foundation for the U.S. and NATO grand strategy during the Cold War." If this frame is applied across the DIMEFIL, it is easy to argue that most, if not all, instruments of U.S. national power are already positioned forward—U.S. embassies house diplomatic, economic, and other capabilities; the Federal Bureau of Investigation has offices overseas; intelligence capabilities are deployed globally both physically and virtually; and so on. What primarily matters in cyber strategic competition short of armed conflict (and the larger strategic competition, as well) is not that the U.S. has assets forward, it's that its

assets are seizing the initiative (this applies to aspects of national instruments of power not forward as well.)

There is a bounty of evidence that several United States agencies and departments embodying national instruments of power are, in fact, seizing the initiative to stem the tide of strategic effects of adversary campaigns in, through, and from cyberspace and will, hopefully, eventually gain the upper hand. The matter of China's licit and illicit efforts to acquire U.S. intellectual property is a case in point. Over the past few years, Congress (and now the CSC) has proposed strengthening the capabilities of the Committee on Foreign Investment in the United States; the Department of Justice stood up the China Initiative to combat IP theft; and the National Security Agency stood up the Cybersecurity Directorate to "eradicate threats to national security systems and critical infrastructure, with an initial focus on the defense industrial base and the improvement of our weapons' security"; USCYBERCOM operationalized the DoD's established construct of DF through a strategic approach of persistent engagement; and the Department of State, after having to accept the resounding defeat of its nominee to China's preferred candidate for leading the United Nation's (UN) Food and Agriculture Organization, seized the diplomatic initiative through an aggressive diplomatic campaign to help ensure Darren Tang of Singapore prevailed over China's nominee to lead the UN's' World Intellectual Property Organization. To build on this momentum, even though the horse has just now left the barn, I encourage the CSC Commissioners and its former staff to consider adopting as the core concept of a national cyber strategy the language of the strategic principle that Defend Forward actually represents—seizing the initiative.

In sum, by arguing in Pillar Six for the continued execution of DF/PE and through other report references and essays highlighting the positive contributions DF/PE makes independently and to a national cyber strategy, the CSC report and key commission staff acknowledge that both DF/PE and the strategic principle it embodies are effective anchors and touchstones for a national cyber strategy. Let's move forward and effectively grasp the new opportunities found in the CSC by building on those acknowledgments and not go backwards before the ink is dry on the report.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-03-20	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Cyberspace Solarium Report and Persistent Engagement: A Response to Ben Jensen	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michael P. Fischerkeller	C5107
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-13141

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Institute for Defense Analyses 4850 Mark Center Dr., Alexandria, VA 22311	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Michael P. Fischerkeller

14. ABSTRACT

The Cyberspace Solarium Commission report aligns well with the core strategic principle of persistent engagement, as well as with the range of contributions it makes to national cyber security. This short essay offers an overview of touchpoints serving as evidence of complementarity.

15. SUBJECT TERMS

Cyberspace solarium commission, persistent engagement, layered deterrence

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Institute for Defense Analyses
Unclassified	Unclassified	Unclassified	Unlimited	3	19b. TELEPHONE NUMBER (Include Area Code)