INSTITUTE FOR DEFENSE ANALYSES

Persistent Engagement and Cost Imposition: Distinguishing between Cause and Effect

Michael P. Fischerkeller, *Project Leader*

Richard J. Harknett, *University of Cincinnati*

January 2020

IDA Non-Standard
NS D-11013

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 C5209, "Cyberspace Solarium Commission," 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.

Acknowledgements

Laura A. Odell

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

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Non-Standard NS D-11013

Persistent Engagement and Cost Imposition: Distinguishing between Cause and Effect

Michael P. Fischerkeller, *Project Leader*

Richard J. Harknett, *University of Cincinnati*

Persistent Engagement and Cost Imposition: Distinguishing between Cause and Effect

Michael P. Fischerkeller – Institute for Defense Analyses

Richard J. Harknett – University of Cincinnati

Introduction

The term "cost imposition" is deeply engrained in U.S. nuclear and conventional strategic theory and in policy discussions of strategy. The term is core to the conceptualization and application of coercive strategies intending to produce security by influencing the strategic decision calculus of an opponent during times of crises and armed conflict. The threat of or actual imposition of costs has become the principal causal mechanism to deter or compel behavior to achieve U.S. strategic ends. Given its centrality in U.S. strategic practice and discourse, it is not surprising that policymakers default to the concept of cost imposition when discussing approaches to the cyber strategic environment. But should they? We argue the term should be used cautiously, if at all.

Cost imposition is integral to strategies of coercion, yet recent cyber strategic guidance concludes that those strategies have failed to secure U.S. national interests in a re-emergent, great-power cyber strategic competition short of armed conflict.[1] Set against the operational reality of cyber strategic competition, the focus on traditional cost imposition leads to confusion within the U.S. government and with allies and partners. To reduce or eliminate this confusion, we propose cost imposition should be reconceptualized in a manner that aligns with the realities of cyber strategic competition. Specifically, we contend that although the threat or actual imposition of costs is the key causal mechanism of coercion strategies in the cyber strategic space of armed conflict, in the cyber competitive space short of armed conflict, cost imposition is best understood as an effect resulting from the causal mechanism associated directly with a strategy of persistent engagement.

Scoping the "traditional" conception

The phrase "impose costs" has its roots in coercion theory and strategies applied to the strategic space of crises and armed conflict. The success of coercive strategies in producing security is premised on threatening or imposing costs on adversaries with the principal objective to influence their strategic calculus to attack or cease attacking (strategic approaches of deterrence and compellence, respectively). We've argued that, in the cyber strategic environment, coercion theory and strategies align well with the cyber strategic space of crises and armed conflict—an argument supported by the empirical record and noted in U.S. strategic guidance.[2] Therefore, we also argue that a conception of imposing costs in and through this cyber strategic space should be consistent with how it has been traditionally conceived for crises and armed conflict. That is, in the context of crisis management and war, cost imposition is the

[1] Department of Defense Cyber Strategy (Department of Defense, 2018).

[2] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare* (November 9, 2018), https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

central causal mechanism through which *to influence an adversary's strategic decision calculus to not attack or to cease attacking*.

However, we've also argued that coercion theory and associated strategies are not well aligned with the cyber strategic competitive space short of armed conflict, a perspective also supported by the empirical record and argued in U.S. strategic guidance.[3] Others have made related arguments by noting that cyber operations to-date have not been primarily coercive in intent nor action.[4] If coercion is not the dominant dynamic in cyber strategic competition, we should question continuing to cite its central causal mechanism (cost imposition) in discussions of security strategy for the cyber strategic competitive space. Thus, to advance greater clarity in strategic thought about cyber strategic competition, cost imposition should be uncoupled from coercion theory and reconceptualized to align with the realities of cyber operations and campaigns short of armed conflict.

Reconceptualizing cost imposition in cyber strategic competition

As noted, theories and strategies of coercion are focused on the goal of influencing the strategic decision calculus of opponents by signaling to them the consequences of proceeding. Strategic approaches of deterrence and compellence embrace cost imposition as the central mechanism for coercing shifts in decision calculus. The fundamental problem with applying this conceptualization of cost imposition to the cyber strategic environment is both structural and strategic. First, cyberspace's core structural feature of interconnectedness and the resulting condition of constant contact combine with the nature of the technology itself to produce a structural imperative to act persistently—states do not have a choice but to act if they want to secure their national interests in, through, and from cyberspace. Ceding the initiative to act (i.e., operational restraint) ensures that one is always playing catch-up. Second, a strategic incentive also exists for states to act persistently short of armed conflict because strategic gains can be realized through operations and campaigns that minimize the risk (and justification) of armed attack responses to the same. Together, the structural imperative and strategic incentive lead to a critical prescriptive and planning assumption: *in, through, and from cyberspace, adversaries will act persistently short of armed conflict*.

Thus, the planning assumption intended to produce security in the crisis and war-fighting environment—that an adversary's strategic decision calculus to act can be influenced through threats or actual cost imposition —is precluded in the cyber strategic competitive environment in which there is both a structural imperative and strategic incentive to act persistently. Consequently, cost imposition as

---

[3] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation," *Cyber Defense Review – Special Edition* (2019), https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf and Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* (Summer 2017), 61:3, pp. 381–393; *Department of Defense Cyber Strategy*, op. cit.

[4] See, for example, Erick Gartzke and John R. Lindsay, "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace," *Security Studies* (24:2), pp. 316–348, http://deterrence.ucsd.edu/_files/Weaving%20Tangled%20Webs_%20Offense%20Defense%20and%20Deception%20in%20Cyberspace.pdf; John R. Lindsay, "Cyber Espionage," in *The Oxford Handbook of Cyber Security*, ed. Paul Cornish (New York: Oxford University Press, (forthcoming), https://drive.google.com/file/d/0B7IN_AGAVuy-WFFFX04yNVVjM3c/view, and Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* (26:3), pp. 452–481, https://www.tandfonline.com/doi/pdf/10.1080/09636412.2017.1306396.

conceptualized in coercion theory and practice provides us with little analytic or prescriptive purchase in the cyber competitive space.

We argue that "cost imposition" should, instead, be understood in the competitive space as an effect of the strategy of persistent engagement's causal mechanism (i.e., seizing the initiative in setting the conditions for security (and insecurity) in the cyber strategic environment). Specifically, cost imposition effects derive from the continuous activities, operations, and campaigns comprising a strategy of persistent engagement that aims to set the conditions for security in the United States' favor by exploiting adversary cyberspace vulnerabilities and reducing the potential for exploitation of its own. Cost imposition effects resulting from this continuous, conditions-setting effort manifest as constraints on adversary cyber behavior across the dimensions of how, when, for what duration, against what national interests, and toward what gains they are directed. Therefore, cost imposition should be understood as a result or consequence of a persistent engagement strategy.[5] Persistent engagement proponents often speak of reducing adversaries' confidence in their cyber capabilities, causing friction in adversaries' political, military, or intelligence organizations, and shifting adversary focus and efforts to the defense in cyberspace. These are examples of cost imposition effects that may result from an adversary's realization that security conditions have shifted.[6] Not all persistent engagement campaigns, operations and activities will result in cost imposition effects. When such efforts shift conditions without an adversary's awareness, for example, the result or consequence is better understood as an effect of benefit gained by the United States, rather than an effect of costs imposed on the opponent.

Distinct from coercion theory, we argue cost imposition in cyber competition is a derived effect of persistent engagement's causal mechanism and not a causal mechanism itself, because security is produced not by prospective threats to impose costs, but by rather by seizing the initiative in exploiting cyberspace's underlying condition of vulnerability with the aim of changing the reality "on the ground" in ways that favor U.S. security. The three operational concepts of a strategy of persistent engagement—anticipatory resilience, defend forward, and contest—have been described as serving this very purpose. To wit, U.S. Cyber Command's 2018 Command Vision describes persistent engagement as operating globally and continuously—shaping the battlespace to create operational advantage for the U.S. while denying the same to its adversaries.[7] More recently, General Paul Nakasone, Commander, U.S. Cyber Command, argued the operational purpose of the "defend forward" concept is "to limit the cyber terrain over which the enemy can gain influence or control."[8]

An intentionally visible manifestation of this approach is USCYBERCOM's practice of uploading malware samples to the VirusTotal website that are discovered through persistent engagement's routine

---

[5] *DoD Dictionary of Associated Military and Associated Terms*, (Department of Defense, October 2019).

[6] United States Senate Committee on Armed Services – Subcommittee on Cybersecurity Hearing, "Department of Defense's Role in Protecting Democratic Elections," February 13, 2018, https://www.armed-services.senate.gov/hearings/18-02-13-department-of-defenses-role-in-protecting-democratic-elections; *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (U.S. Cyber Command, February 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010; Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation," op. cit.

[7] *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,* op. cit.

[8] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* (92, 1st quarter 2019), pp. 10–14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

operations and campaigns. USCYBERCOM describes this activity as "an enduring and ongoing information-sharing effort, and it is not focused on any particular adversary."[9] Stated differently, it is a continuous activity (initiative-seeking) centered on shifting the condition of security through simultaneously enabling the cyber community to improve defenses, while undermining the effectiveness of malware likely populating cyber arsenals across the globe. Information security company threat analysts have noted that although such global uploads may not immediately render the malware totally ineffective, "it is likely to at least cause the attacker to adapt".[10] This observation is illustrative of the ways adversaries can respond to cost imposition effects derived from changing the conditions of security in cyberspace. In this example, an attacker seeking to regain initiative and set new conditions must devote additional energy and resources toward developing a new malware variant. The broader point of this example is that security is produced by taking the initiative in changing the conditions of security (through global sharing which blunts or mitigates the effects of known malware), not through seeking to change the strategic decision calculus of the attacker. This practice by USCYBERCOM, while unique because it is supported by a strategic approach of persistent engagement, relates, through a shared objective of remediation and mitigation, to earlier and ongoing efforts by various coalitions of non-profit, public sector, private industry, academia, and law enforcement agencies including, for example, the DNSChanger Working Group and the Conficker Working Group. Taken together, these efforts represent a step toward a "Whole of Nation+" approach to cyber security that leverages the unique capabilities of a diverse set of actors.[11] Critically, all of this activity has to be seen through a persistent engagement lens as not reactive patching, but institutionalizing pathways through which anticipatory resilience can be achieved.

Based on open source reporting, USCYBERCOM's effort to defend the 2018 U.S. mid-term elections can be understood similarly. Reportedly, USCYBERCOM took an initiative to exploit vulnerabilities in the cyber infrastructure of the Internet Research Agency (IRA) in Russia. This campaign changed the conditions of security in favor of the United States in this space, resulting in an initial effect of a benefit gained. The United States could have opted to covertly persist in this infrastructure, in a limited intelligence gain posture, to learn about IRA capabilities or intentions and feed that information back to improve U.S. cyber defenses (and perhaps it did so for a period), but, instead, it chose to make its presence known. When Russia became aware of a change in security conditions, cost imposition effects then manifested as the IRA experienced organizational friction, and Russia shifted focus and efforts toward defense, both of which served a U.S. objective of taking Russia's focus off of cyber-enabled information operations directed at U.S. elections.[12] Once aware of a U.S. presence, IRA operators likely

---

[9] Joseph Cox, "The US Military Just Publicly Dumped Russian Government Malware Online," *Motherboard*, November 9, 2018, https://www.vice.com/amp/en_us/article/8xpa7k/us-military-cybercom-publicly-dumped-russian-government-malware-fancy-bear-apt28.

[10] Catlin Cimpanu, "US Cyber Command Starts Uploading Foreign APT Malware to VirusTotal," *Zeroday*, November 8, 2018, https://www.zdnet.com/google-amp/article/us-cyber-command-starts-uploading-foreign-apt-malware-to-virustotal/.

[11] Michael P. Fischerkeller and Richard J. Harknett, "A Response on Persistent Engagement and Agreed Competition," *Lawfare* (June 27, 2019), https://www.lawfareblog.com/response-persistent-engagement-and-agreed-competition.

[12] United States Senate Committee on Armed Services Hearing, "Review Testimony On United States Special Operations Command and United States Cyber Command in Review on the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program," February 14, 2019, https://www.armed-services.senate.gov/imo/media/doc/19-13_02-14-19.pdf.

and hastily sought to re-examine security practices, discern where else the United States might be in IRA infrastructure, and determine what information or capabilities the United States might have ascertained or ex-filtrated by leveraging its exploitation. As in the previous example, the broader point is that security was produced through following persistent engagement's prescription to seize initiative in setting the conditions of security (through exploiting vulnerabilities, in this example) and not through seeking to change the strategic decision calculus of the attacker. This was not a traditional coercive signaling moment. Rather, any IRA plans to launch cyber-enabled disinformation were thrown off balance as USCYBERCOM captured the initiative in setting security conditions. Cost imposition effects against Russia derived from this initiative should be understood for what they were—a result or consequence of seizing the initiative away from Russia in setting those conditions.

Managing expectations and measuring effectiveness

How does this reconceptualization have analytic utility? Coercion strategies and their central causal mechanism of cost imposition focus policymakers and analysts alike on identifying thresholds, ensuring effective signaling and assessing if the strategic decision calculus of an adversary has been influenced. If coercive strategies are not aligned with the cyber competitive space, as U.S. strategic guidance and scholars have argued, adopting the same foci in that space will lead to misaligned efforts, unrealistic expectations, and illogical measures of effectiveness. Regarding the latter, a core challenge of measuring the effectiveness of coercion strategies in the conventional strategic environment has been cited by many—namely *a dearth of empirical data* of whether an adversary actually intended to attack.[13] Assessing the effectiveness of a persistent engagement strategy brings different challenges, but interestingly, challenges that may be overcome *due to an abundance of empirical data*. This abundance is an empirical consequence of accepting the planning assumption that states will act persistently in, through, and from cyberspace short of armed conflict. The challenge, then, becomes synthesizing numerous sources of threat data gathered by both the private sector and the government to measure, for example:

- whether an adversary's presence on U.S. critical infrastructure is fleeting or enduring, but not if adversaries have been coerced to not have a presence at all;
- whether adversaries are constrained or not in the set of U.S. national interests that they can engage in, through, and from cyberspace, but not if adversaries have been coerced to not target any interests at all;
- and whether the effects adversaries generate in, through, and from cyberspace are inconsequential vice being independently or cumulatively strategic, but not if adversaries are coerced to not generate any effects at all.

This latter measure, whether cyber campaigns cumulatively produce a shift in the relative balance of national sources of power, is a key strategic focus of a persistent engagement strategy. To be sure, these examples represent a different mindset than expectations associated with the traditional conception of cost imposition, but it is one far more tightly aligned with realties of the cyber strategic competitive

[13] See, for example, Paul Huth and Bruce Russett, "Testing Deterrence Theory: Rigor Makes a Difference," *World Politics* (42:4), July 1990, pp. 466–501, https://www.jstor.org/stable/pdf/2010511.pdf?refreqid=excelsior%3A7d1309bcd6eda1bf948ca4fe5c85fdf2.

space and the strategic approach of persistent engagement and therefore should be seen as an advancement in our understanding of cyberspace strategic competition.

Conclusion

If the U.S. is able to shift the balance of initiative in its favor in setting the security conditions under which the cyber strategic competition is played, adversaries will find themselves primarily playing catch-up and will have to take into account U.S. efforts and/or try to anticipate them. This is not because the United States will have imposed or threatened to impose costs in the "traditional" sense—rather, cost imposition effects on adversaries would derive from U.S. efforts to set the conditions of security in cyberspace.

Thomas Kuhn argued that when there is a paradigm shift in a scientific discipline, scientists see familiar objects in a different light and come to understand unfamiliar ones, as well.[14] This can take some time, however, so consensus on a new paradigm tends not to be achieved quickly or broadly. We've argued elsewhere that the advent of the cyber strategic environment necessitates a cyber strategy paradigm shift to account for new strategic realities—specifically, away from deterrence and to persistent engagement in the cyber competitive space short of armed conflict.[15] Consistent with Kuhn's arguments, we also recommend the term "cost imposition" be seen not as a causal mechanism for coercion strategies in this space but as an effect derived from the casual mechanism of a strategy of persistent engagement. We think this reconceptualization postures the notion of cost imposition to be more relevant in strategic discussions of this space, can reduce the potential for policymaker and warfighter misunderstandings and better align expectations, and can, hopefully, hasten the advancement of strategic thought and consensus.

[14] Thomas S. Kuhn, *The Structure of Scientific Revolutions* (University of Chicago: Chicago, IL, 2012).
[15] Brad D. Williams, "Meet the Scholar Challenging the Cyber Deterrence Paradigm," *Fifth Domain*, July 19, 2017, https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-01-20	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Persistent Engagement and Cost Imposition: Distinguishing between Cause and Effect	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michael P. Fischerkeller, Richard J. Harknett	C5209
	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-11013

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

For the last 70 years, the term "cost imposition" has been deeply engrained in U.S. nuclear and conventional strategic theory and policymaker discussions of strategy. The term has anchored the conceptualization and application of coercive strategies seeking to influence an adversary's strategic decision calculus in crises and armed conflict. The threat of or actual imposition of costs has been the central causal mechanism to achieve those U.S. strategic ends, primarily through deterrence or compellence. Given the centrality of the term in decades of strategic practice and discourse, it's not surprising that it is invoked today in discussions of strategy for the cyber strategic environment. But many scholars have argued it has little to no relevance in cyberspace. In an effort to bridge this gap, this product offers a reconceptualization of "cost imposition" to better align it with the core features and dynamic of the cyber strategic environment.

15. SUBJECT TERMS

Persistent engagement, cyber strategy, cyberspace, strategy, coercion, cost imposition

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	6	19b. TELEPHONE NUMBER (Include Area Code)