NIU
NATIONAL INTELLIGENCE UNIVERSITY
Ann Caracristi Institute For Intelligence Research

**What this is:**

This report is the product of academic research. As the IC's university, NIU is uniquely positioned to use academic approaches to research—and report on—subjects of interest to the community.

**What this is not:**

This is not finished intelligence. The opinions expressed in this report are solely the author's and not those of National Intelligence University, or any other US Government agency.

# RESEARCH SHORT

**INSIGHT** Sharing academic research September 17, 2024

IMAGE FROM SHUTTERSTOCK

# Does Academic Theory Sway US Cyber Strategy Implementation?

**LTC Amanda C. Current**

The evolution of US cybersecurity strategy since 2015 illustrates how academic debate can guide practitioners managing operations in the cyber domain. The shift from an emphasis on deterrence toward an operational approach rooted in Cyber Persistence Theory suggests that, for the first time, the public manifestation of a theory—in its embryonic form—did not lag behind strategy development. This *Research Short* examines the shift in strategic language as an indicator that theorizing about the unique structural characteristics of cyberspace drove a policy shift for US cybersecurity. If theory can drive practice, how does that relationship affect cyber operators' downstream strategy implementation in a dynamic security environment?

After attending a talk by the authors of *Cyber Persistence Theory*, *Redefining National Security in Cyberspace*, a senior tactician at US Cyber Command remarked, "It was interesting, but has nothing to do with what operators are actually doing in the domain." This comment revealed an assumption that appears to permeate much of the practitioner community: Academic debate and theory development have little impact on how strategists manage conflict and competition, or how tacticians operate in cyberspace. The evolution of national strategic guidance for cybersecurity during the past decade, however, indicates otherwise. A 19-page report published by President Barack Obama's White House in 2015 articulated a cyber policy centered on deterrence, but the Biden Administration's "2023 National Cybersecurity Strategy" did not mention deterrence a single time. Instead, a "defend forward" strategy* rooted in Cyber Persistence Theory emerged as the preferred operational approach.[1] Not only do strategies of deterrence and operational restraint yield fundamentally different tactics and operations than strategies of forward defense and persistent engagement; this shift in strategic posture between the Obama and Biden administrations implies a realignment between theory and practice in the cyber domain that signals the beginning of a paradigm shift away from coercion theory and the resultant "deterrence default" of the national security enterprise.[2]

## The Theory-Practice Gap

> The most promising way to bridge the gap between the academician and the policy maker…is to focus on the relationship between knowledge and action in the conduct of foreign policy.[3] – Alexander George

The question of theory's relevance to practice is not new. Alexander George's *Bridging the Gap: Theory and Practice in Foreign Policy* explored the disconnect between those studying foreign policy and those practicing it.[4] He determined that a weak knowledge base undercut the effectiveness of five of six attempts at US coercive diplomacy in Iraq in 1988-91. His theory-practice gap framework identified three kinds of knowledge needed in policymaking:

- *Abstract conceptual models of strategies* that can identify "the critical variables of a strategy and the general logic associated with successful use of that instrument of policy."[5] The abstract model is not the strategy itself, but a starting point for constructing a strategy.
- *General or generic knowledge* that can compensate for the limitations of abstract conceptual models by providing conditional generalizations based on past experiences that favor success or forecast the failure of a strategy.[6]
- *Actor-specific behavioral knowledge* to provide a "correct image of the opponent."[7]

* "Defend forward" first appeared as strategic guidance in the 2018 Department of Defense (DoD) Cyber Strategy, which directed DoD to "disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." The strategy, however, simultaneously directed DoD to "compete and deter in cyberspace," revealing a bifurcated strategy that straddles two distinct conceptual frameworks. *Source:* US Department of Defense, "Department of Defense Cyber Strategy: Summary (2018)," 2018, 1, 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Together, these three knowledge types constitute what George called *policy-relevant theory,* or "the type of knowledge needed for statecraft."[8] Gaps exist where there is a lack of the knowledge needed for statecraft. The magnitude of the gap between academics and policymakers is proportionate to the lack of policy-relevant knowledge. Put more succinctly, the theory-practice gap can be defined as *a disconnect between substantive theory and published policy proportionate to the absence of policy-relevant knowledge.*

George asserted that theoretical-conceptual knowledge is essential to policymaking, and—consciously or not—all policymakers use some form of conceptual framework, reflecting their assumptions about a theory's core requirements and causal logic. Although the theory-practice gap cannot be eliminated, policy-relevant knowledge can help "bridge" the gap by aiding policymakers in diagnosing and prescribing an effective policy response to a particular problem. Implicit in George's work is the idea that both the work of the scholar and the outcomes of the practitioner would benefit with a better bridge between the two.

Most scholarly work published since George's book maintains that the theory-practice gap is problematic on both sides of the divide.[9, 10, 11, 12, 13, 14,15, 16, 17] Underpinning the majority's consensus is the prevailing assumption that theory-practice alignment (that is, a smaller gap) would lead to better policy. Academic-practitioner Philip Zelikow explicitly states "government would benefit if the vast stores of outside knowledge could somehow be brought to bear on daily policy challenges."[18] In summarizing the growing literature on the theory-practice gap, Stephen Walt asserts "the need for powerful theories that could help policymakers design effective solutions would seem to be apparent."[19]

The assumption that theory-practice alignment yields better policy outcomes is so pervasive among academics that many international relations scholars structure their arguments as though it is a proven fact. While scholars believe theories impact strategy development and implementation, many practitioners question that assumption. They argue that academic debate and theory development is, at best, tangential and, at worst, irrelevant.[20] So, is theory consequential to policy outcomes? Text analyses of the national cybersecurity strategic guidance from 2015 and 2023 indicate theory was neither tangential nor irrelevant to strategy development.

## Cyber Deterrence: An Academic Debate

The theory-practice gap in cybersecurity is most acutely evident in the decades-long debate over mapping traditional deterrence models to the cyber domain.† In 2012, Tim Stevens provided a "genealogy of American cyber deterrence" that traced its roots to the successful use of information

† The detonation of atomic bombs in 1945 caused Bernard Brodie to leave his work as a naval war strategist to become the architect of US nuclear deterrence. His work marked the first of three waves of strategic studies in post-World War II security, as civilian strategists rose to prominence. During the Cold War, the existential threat of the "absolute weapon" drove deterrence strategies rooted in coercion theory, which became the central concept of the strategic studies subfield and continues to impact strategy development today.

warfare during the early stages of Operation Desert Storm in Iraq in 1991. This led to theorizing about an "information-technology Revolution in Military Affairs."[21] No one disputed the differences that existed between nuclear and Information Age conflict, but scholars varied widely in how they treated deterrence in the Information Age and used nuanced arguments to support their claims. Sir Lawrence Freedman, for example, broadened the concept of deterrence by citing non-deterrence strategic options (that is, norms-based approaches) that yield deterrent *effects*.[22] Critics of cyber deterrence, however, argued that the core assumptions underwriting deterrence theory's causal logic do not map to the 21st century security environment.[23, 24, 25, 26, 27, 28, 29, 30, 31] This debate was well underway at the time the Obama administration was drafting its White House Report on Cyber Deterrence Policy—written in response to mounting pressure from Congress.[32, 33]

## Case Comparison: 2015 White House Report on Cyber Deterrence Versus 2023 National Cybersecurity Strategy

> Make no mistake, we are not winning the fight in cyberspace. Our adversaries view our response to malicious cyberactivity as timid and ineffectual. Put simply, the problem is a lack of deterrence.[34] – Senator John McCain, September 2015

### *2015 White House Report on Cyber-Deterrence Policy*

Despite having published the "2011 International Strategy for Cyberspace" during his first term as president, Congress repeatedly denounced President Obama for perpetuating a "deterrence deficit" in the cyber domain.[35] Lawmakers blamed the increase in cyberattacks from China, Iran, North Korea, and Russia on the absence of a definitive US cyber deterrence policy.[36] In December 2015, the White House articulated its cyber-deterrence policy in a report to Congress.[37]

A section titled "Cyber-Deterrence Strategies" defined deterrence in the classical sense:

> "Deterrence seeks to convince adversaries—by means of influence over their decision-making—not to take actions that threaten important national interests. Influence is achieved by credibly demonstrating the ability and willingness to deny benefits or impose costs to convince the adversary that restraint will result in better outcomes than will confrontation."[38]

The report acknowledged that "cyber deterrence in the Information Age is substantially different from Cold War-era concepts intended to deter the use of weapons of mass destruction."[39] These differences include the following:

- Cyber capabilities' asymmetric threat;
- The larger number of players (because of the low cost of entry);
- Cyber tools' dual-use nature;
- Plausible deniability clouding attribution;

- Cyberspace's globally interconnected structure; and
- Cyberspace's privately-owned terrain, where the same tools can be used for both benign and malicious purposes.[40]

Despite identifying these fundamental differences, the document describes a cyber-deterrence policy that remained grounded in defense and resilience. In fact, the document mentioned defense, defend, and defending 60 times in 19 pages—a frequency that matched mentions of deter, deterrence, and deterrent.

This blending of strategic concepts did not go unnoticed by academics, intensifying the ongoing cyber-deterrence debate. Some scholars opined that the strategy was "far from the strategic concept found in classic deterrence literature" and was "actually a strategy of (passive) defense."[41] Cyber-deterrence skeptics panned the policy as the type of muddled national security guidance that results from misaligning strategy with the unique "structural features and operational characteristics of the domain."[42] In short, the "2015 White House Report on Cyber Deterrence Policy" illuminated an Information Age theory-practice gap: a disconnect between substantive theory and published policy resulting from the misapplication of a conceptual framework to a particular strategic environment.

### *2023 National Cybersecurity Strategy*

Seven years later, the Biden administration crafted the "2023 National Cybersecurity Strategy," written by a team of scholar-practitioners appointed to the newly established Office of the National Cyber Director (ONCD).‡ Although many of the staff involved in its drafting had served in the Obama administration and published on cybersecurity topics during the intervening years,§ the deterrence-focused conceptual framework of the 2015 policy was not carried over. In fact, the 2023 strategy did not once use the terms deter, deterrence, or deterrent, marking a significant departure from strategic language dating back to President George W. Bush's "2008 Comprehensive National Cybersecurity Initiative."[43]

Instead, the "2023 National Cybersecurity Strategy" directed DoD to continue a "strategic approach of defending forward" in support of one of the strategy's core pillars: to disrupt and dismantle threat actors.[44] This was an "explicit continuation of some of the priorities outlined in the 2018 Trump administration cyber strategy," including a new "strategic posture" of *persistent engagement* that had slowly overtaken deterrence as the conceptual framework best aligned to structural realities of the virtual domain.[45, 46] In contrast to the operational restraint emphasized in Obama-era strategies, the "core strategic principle of persistence is seizing the initiative to set and maintain the conditions of security in and through cyberspace."[47] The strategy to defend forward through an operational approach of persistent engagement marked the beginning of a paradigm shift from the "legacy of deterrence as the US central security strategy" for the cyber domain.[48]

‡ ONCD was established under the fiscal year 2021 National Defense Authorization Act, on the recommendation of the bipartisan Cyberspace Solarium Commission.

§ The top three officials spearheading the project—Chris Inglis, Robert Knake, and Harry Krejsa—have several published books and articles among them on topics including cyber deterrence, cyber war, cyber resilience, research, and strategy, and the "dual hat" leadership construct of USCYBERCOM and the National Security Agency (NSA).

## Findings and Implications

The authors invited to speak at the above-mentioned USCYBERCOM-hosted book talk[¶] were among the most prolific scholar-practitioners engaged in the cyber deterrence debate between 2015 and 2023 and were instrumental in crafting USCYBERCOM's "2018 Command Vision." They offer an innovative analytic framework for new cyber strategies that responds to the unique structural characteristics of cyberspace. Their Cyber Persistence Theory was informed by the years-long debate over the misapplication of deterrence strategies to prevent or punish malicious activity in a virtual domain. This debate—and the new theory it produced—was not merely scholarly pontification. It drove the shift in strategic thought captured in the "2023 National Cybersecurity Strategy" and DoD's current operational approach of *persistent engagement* through a strategy of *defending forward* in the cyber domain.

The emergent *theory* of cyber persistence is still taking shape, marking a paradigm shift even as the *operational approach* of persistent engagement appears in cyber policy and strategy documents. The concept's increasing appearance in national security blogs, academic conferences, journal articles, and Congressional hearings[49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59] is noteworthy because, for the first time, it appears the public manifestation of theory—in its embryonic form—did not lag behind strategic implementation. Theorizing about the unique structural qualities of the cyber domain drove a monumental policy shift in US cybersecurity. Just as theory informed cybersecurity policies and strategies during the past 10 years, the challenge of securing a virtual domain inspired theoretical innovation in the scholarly literature.

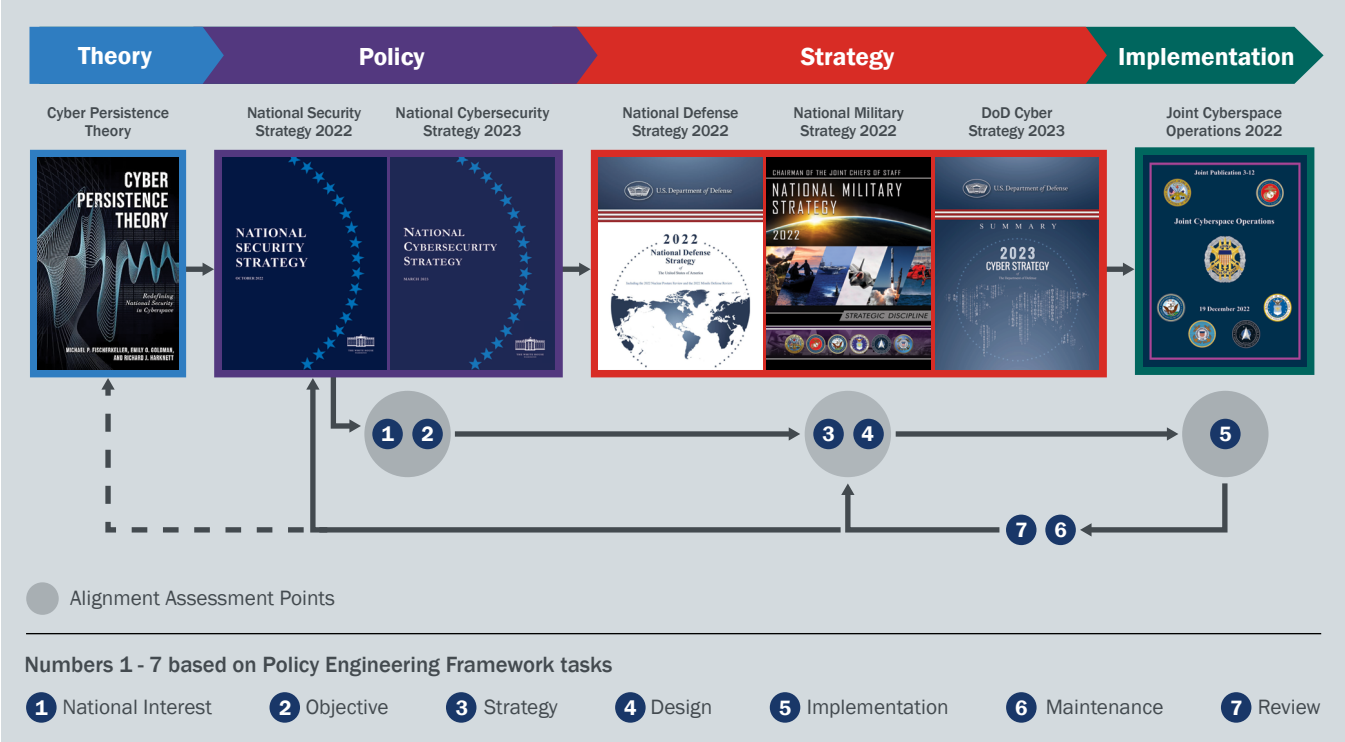
## Future Research

The question now before us is whether the theoretical paradigm shift affected downstream strategy implementation efforts for cyber operators in a dynamic security environment. The cyber domain is a crowded space where intelligence is collected, communications are exchanged, financial transactions are executed, and conflict takes place. National strategies to secure cyberspace must account for multiple stakeholders' equities to prevent strategy implementation from inadvertently undermining missions or activities critical to securing the virtual domain. A study designed to assess alignment along the theory-policy-strategy implementation continuum will illuminate how theory-practice gaps might impact the defense, intelligence, and security enterprise communities' activities and equities.

Applying Philip Zelikow's policy engineering framework to empirical evidence collected through case study analysis will reveal whether theory did, in fact, impact strategy implementation. (See Fig. 1)

¶ Dr. Michael Fischerkeller, a research staff member in the Information, Technology, and Systems Division at the Institute for Defense Analyses, spent 25 years supporting DoD; Dr. Emily Goldman, a strategist at USCYBERCOM, served as a cyber advisor at Department of State after two decades as a Professor of Political Science; Dr. Richard Harknett is Professor and Director of the School of Public and International Affairs at the University of Cincinnati, and served as the first Scholar in Residence at USCYBERCOM and NSA.

**Figure 1**




Zelikow defines policy engineering as "the application of knowledge, principles, and methods to the solution of specific public problems in a given political environment."[60] His framework identifies seven distinct, iterative tasks for the policymaking process that need not occur in chronological order: 1) national interests, 2) objectives, 3) strategy, 4) design, 5) implementation, 6) maintenance, and 7) policy review.[61] Using this framework to conduct a comparative case study will help answer the question: ***How closely aligned were theory, policy, and strategy implementation during US attempts to secure the cyber domain between 2010 and 2023?***

Answering that question requires a descriptive analytic framework that illuminates what a "bridged" theory-practice gap might look like for cybersecurity. Merging the work of the architect (George) and the engineer (Zelikow), this research seeks to offer a framework that provides academics and practitioners greater precision in measuring the existence of a theory-practice gap, how gaps might be managed, and how they might matter for downstream strategy implementation.

**LTC Amanda Current** is a US Army Strategic Intelligence Officer and Research Fellow at NIU's Caracristi Institute for Intelligence Research. She is a Tufts University Cyber Security and Policy scholar and previously served as a nonresident fellow at the Harvard Kennedy School's Belfer Center for Science and International Affairs from 2019 to 2021. This *Research Short* draws on her dissertation research for the Fletcher School of Law and Diplomacy, where she is pursuing her Ph.D. in International Relations.

If you have comments, questions, or suggestions for a *Research Short* topic or article, please contact the NIU Office of Research and Engagement at: **NIPress@niu.odni.gov**.

## Endnotes

1 US Department of Defense, "Department of Defense Cyber Strategy: Summary (2018)," 2018, 1, 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
2 Michael P. Fischerkeller et al., *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford, UK: Oxford University Press, 2022), 5.
3 Alexander L. George, *Bridging the Gap: Theory and Practice in Foreign Policy* (Washington, D.C: United States Institute of Peace, 1993), 16.
4 George, *Bridging the Gap*.
5 George, *Bridging the Gap*, 118.
6 George, *Bridging the Gap*, 120.
7 George, *Bridging the Gap*, 125.
8 George, *Bridging the Gap*, xx.
9 Joseph S. Nye, "Bridging the Gap between Theory and Policy," *Political Psychology* 29, no. 4 (2008): 593–603, https://www.jstor.org/stable/20447146.
10 Joseph S. Nye, "International Relations: The Relevance of Theory to Practice," in *The Oxford Handbook of International Relations*, 2008, https://doi.org/10.1093/oxfordhb/9780199219322.003.0037.
11 Joseph Lepgold and Miroslav Nincic, *Beyond the Ivory Tower: International Relations Theory and the Issue of Policy Relevance* (New York: Columbia University Press, 2001).
12 Michael Desch, "Technique Trumps Relevance: The Professionalization of Political Science and the Marginalization of Security Studies," *Perspectives on Politics* 13, no. 2 (June 2015): 377–93, https://doi.org/10.1017/S1537592714004022.
13 Michael C. Desch, "How Political Science Became Irrelevant: The Field Turned Its Back on the Beltway," *The Chronicle of Higher Education* 65, no. 25 (March 8, 2019): B14–B14, http://go.gale.com/ps/i.do?p=AONE&sw=w&issn=00095982&v=2.1&it=r&id=GALE%7CA579342146&sid=googleScholar&linkaccess=abs.
14 Marc A. Genest, *Review of Beyond the Ivory Tower: International Relations Theory and the Issue of Policy Relevance*, by Joseph Lepgold and Miroslav Nincic, *Perspectives on Politics* 1, no. 2 (2003): 458–458, https://www.jstor.org/stable/3688998.
15 Philip Zelikow, "Foreign Policy Engineering: From Theory to Practice and Back Again," *International Security* 18, no. 4 (1994): 143–71, https://doi.org/10.2307/2539180.
16 Joseph Lepgold, "Is Anyone Listening? International Relations Theory and the Problem of Policy Relevance," *Political Science Quarterly (Academy of Political Science)* 113, no. 1 (Spring 1998): 43, https://doi.org/10.2307/2657650.
17 Robert Jervis, "Bridges, Barriers, and Gaps: Research and Policy," *Political Psychology* 29, no. 4 (2008): 571–92, https://doi.org/10.1111/j.1467-9221.2008.00650.x.
18 Zelikow, "Foreign Policy Engineering," 146.
19 Stephen M. Walt, "The Relationship Between Theory and Policy in International Relations," *Annual Review of Political Science* 8, no. 1 (2005): 23, https://doi.org/10.1146/annurev.polisci.7.012003.104904.
20 Daniel Maliniak et al., *Bridging the Theory-Practice Divide in International Relations* (Washington DC: Georgetown University Press, 2020), 9.
21 Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy* 33, no. 1 (April 1, 2012): 149, https://doi.org/10.1080/13523260.2012.659597.
22 Lawrence Freedman, *Deterrence*, 1st ed. (Cambridge, UK: Polity, 2004).
23 David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010), https://doi.org/10.17226/12997.
24 Nazli Choucri and David D. Clark, *International Relations in the Cyber Age: The Co-Evolution Dilemma* (Cambridge, MA: MIT Press, 2018). 2010
25 Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What To Do About It*, Reprint edition (New York: Ecco, 2011).
26 Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017): 381–93, https://doi.org/10.1016/j.orbis.2017.05.003.
27 Richard J. Harknett and Emily O. Goldman, "The Search for Cyber Fundamentals," *Journal of Information Warfare* 15, no. 2 (2016): 81–88, https://www.jstor.org/stable/26487534.

28 Richard J Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies*, March 4, 2020, 1–34, https://doi.org/10.1080/01402390.2020.1732354.
29 Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," Belfer Center for Science and International Affairs, Fall 2013, https://www.belfercenter.org/publication/myth-cyberwar-bringing-war-cyberspace-back-down-earth.
30 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009).
31 Aaron F. Brantly, ed., *The Cyber Deterrence Problem* (London, New York: Rowman & Littlefield Publishers, 2020).
32 Scott Maucione, "McCain Presses Obama Administration on Cyber Deterrence," *Federal News Network*, November 20, 2015, https://federalnewsnetwork.com/defense/2015/11/mccain-presses-obama-administration-cyber-deterrence/.
33 Scott Maucione, "Lawmakers Want Defense Cyber Policy To Deter, Retaliate," *Federal News Network*, September 29, 2015, https://federalnewsnetwork.com/cybersecurity/2015/09/lawmakers-want-defense-cyber-policy-deter-attacks-retaliate/.
34 Committee on Armed Services, *United States Cybersecurity Policy and Threats* (Washington, DC: Government Publishing Office, 2015), 2, http://archive.org/details/gov.gpo.fdsys.CHRG-114shrg22270.
35 Committee on Foreign Affairs, *Cyber War: Definitions, Deterrence, and Foreign Policy* (Washington, DC: Government Publishing Office, 2015), 2, http://archive.org/details/gov.gpo.fdsys.CHRG-114hhrg96817.
36 Committee on Armed Services, *United States Cybersecurity Policy and Threats*.
37 Scott Maucione, "White House Finally Acquiesces to Congress on Cyber Deterrence Policy," *Federal News Network*, December 29, 2015, https://federalnewsnetwork.com/cybersecurity/2015/12/white-house-finally-acquiesces-congress-cyber-deterrence-policy/.
38 White House, "Report on Cyber Deterrence Policy (for Congress)," December 2015, 4, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://federalnewsnetwork.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf.
39 White House, "Report on Cyber Deterrence," 4.
40 White House, "Report on Cyber Deterrence," 4–5.
41 Michael P. Fischerkeller et al., "The Limits of Deterrence and the Need for Persistence," in *The Cyber Deterrence Problem*, Aaron F. Brantly, ed., 2020, 9.
42 Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," 1.
43 George W. Bush, "National Security Presidential Directive 54/Homeland Security Presidential Directive 23" (The White House, January 8, 2008), 10, https://fas.org/irp/offdocs/nspd/nspd-54.pdf.
44 White House, National Cybersecurity Strategy, March 2023, 14, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
45 Tim Starks, "The Biden National Cyber Strategy Is Unlike Any Before It," *Washington Post*, January 6, 2023, https://www.washingtonpost.com/politics/2023/01/06/biden-national-cyber-strategy-is-unlike-any-before-it/.
46 Michael P. Fischerkeller, et al., *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford, UK: Oxford University Press, 2022), 83.
47 Fischerkeller, et al., *Cyber Persistence Theory*, 128.
48 Fischerkeller, et al., *Cyber Persistence Theory*, 128.
49 Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare* (blog), November 9, 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace. \\uc0\\u8221{} {\\i{}Lawfare} (blog
50 Michael P. Fischerkeller and Richard J. Harknett, "What Is Agreed Competition in Cyberspace?," *Lawfare* (blog), February 19, 2019, https://www.lawfareblog.com/what-agreed-competition-cyberspace.
51 Richard J. Harknett, "SolarWinds: The Need for Persistent Engagement," *Lawfare* (blog), December 23, 2020, https://www.lawfareblog.com/solarwinds-need-persistent-engagement.
52 James N. Miller and Neal A. Pollard, "Persistent Engagement, Agreed Competition and Deterrence in Cyberspace," *Lawfare* (blog), April 30, 2019, https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace.
53 Max Smeets and Herb Lin, "An Outcome-Based Analysis of US Cyber Strategy of Persistence and Defend Forward," *Lawfare* (blog), November 28, 2018, https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward.

54 Max Smeets, "US Cyber Strategy of Persistent Engagement and Defend Forward: Implications for the Alliance and Intelligence Collection," *Intelligence and National Security* 35, no. 3 (2020): 444–53, https://doi.org/10.1080/02684527.2020.1729316.

55 William T Eliason, "An Interview with Paul M. Nakasone," *Joint Force Quarterly*, 92 (January 22, 2019): 6.

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

57 Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (January 22, 2019): 9.

58 Paul M. Nakasone and Michael Sulmeyer, "How To Compete in Cyberspace," *Foreign Affairs*, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

59 "Cyberspace Solarium Commission," accessed August 5, 2020, https://sites.google.com/solarium.gov/cyberspace-solarium-commission.

60 Zelikow, "Foreign Policy Engineering," 144.

61 Zelikow, "Foreign Policy Engineering."