INSTITUTE FOR DEFENSE ANALYSES

Fluidity, not Advantage, Conditions Cyberspace Security: An Alternative to Offense-Defense Theory

Michael P. Fischerkeller, Project Leader

Jay Jacobs

July 2023

IDA Non-Standard D-33534

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

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 Project C5239, "Cyber Offense-Defense Theory," 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

Kevin Garrison (IDA), J.D. Work (National Defense University), Eugene Spafford (Purdue University), Richard J. Harknett (University of Cincinnati)

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

Fluidity, not Advantage, Conditions Cyberspace Security: An Alternative to Offense-Defense Theory

Michael Fischerkeller and Jay Jacobs

Introduction

Since cyberspace's inception, scholars and policymakers have sought to describe and explain state cyber behaviors through the lens of offense-defense theory. Some have claimed that cyberspace is offense dominant,[1] others that it is offense advantaged,[2] while still others argue it is defense advantaged.[3] Additionally, some have claimed that a condition of cyber offense or defense advantage can be measured only dyadically vice systemically, and others have stated it cannot be measured at all.[4] These differing claims harken back to important decades-old debates about prevailing advantages in different epochs of conventional military capabilities and how to operationalize the offense-defense balance.[5]

---

[1] See William J. Lynn III, "Defending a New Domain: The Pentagon's Cyber Strategy," *Foreign Affairs* 89, no. 5 (September / October 2010), https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain; John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 95–112, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-2/Sheldon.pdf; and Jan Van Tol, Mark Gunzinger, Andrew Krepinevich, and Jim Thomas, *Airsea Battle: A Point-of-Departure Operational Concept* (Washington, D.C., Center for Strategic and Budgetary Assessments, 2010), 35. Additionally, Gen. (Rtd.) Michael Hayden, a former director of the Central Intelligence Agency and of the National Security Agency, argues that "the cyber domain gives near-crushing advantage to the offense." Michael Hayden, "To Defend against Hostile Nations, America Needs Fierce Cyberpower," *The Hill*, March 12, 2018, http://thehill.com/opinion/national-security/377876-america-needs-to-step-up-cyber-combat-against-hostile-nations.

[2] See The White House, *National Cybersecurity Strategy, March 2023*, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, 1; David Cattler, North Atlantic Treaty Organization (NATO) assistant secretary general for Intelligence and Security, quoted in Maggie Miller, "NATO Prepares for Cyber War," *Politico*, December 3, 2022, https://www.politico.com/news/2022/12/03/nato-future-cyber-war-00072060; Anne Neuberger, "The U.S. Government's Global Cyber Initiatives," U.S. Department of State, November 17, 2022, https://www.state.gov/briefings-foreign-press-centers/global-cyber-initiatives; Jason Healey, "Understanding the Offense's Systemwide Advantage in Cyberspace," *Lawfare*, December 22, 2022, https://www.lawfareblog.com/understanding-offenses-systemwide-advantage-cyberspace; Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review* 3, no. 4 (Fall 2020): 31–53, 44, https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/; New York Cyber Task Force, *Building a Defensible Cyberspace* (Columbia School of International and Public Affairs, 2017), https://www.sipa.columbia.edu/sites/default/files/2022-09/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (Fall 2013): 7–40, http://www.jstor.com/stable/24480929; Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S-China Relations* (Washington, D.C,: Brookings, 2012), 14, https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf; Martin C. Libicki, *Cyberdeterrence* and Cyberwar (Santa Monica, CA: Rand Corporation, 2009), 32, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf; and Joseph F. Nye, Jr., *Cyber Power* (Belfer Center for Science and International Affairs: Cambridge, MA, 2010), 5, https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf.

[3] See Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013), 73, 168; Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal* 157, no. 1 (February / March 2012): 6-13, 12, https://doi.org/10.1080/03071847.2012.664354; and Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no.3 (2013): 365–404, https://doi.org/10.1080/09636412.2013.816122,

[4] See, respectively, Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?" *International Security* 41, no. 3 (Winter 2016/17): 72–109, https://www.jstor.org/stable/10.2307/26777791 and Brandon Valeriano, "The Failure of Offense/Defense Balance in Cyber Security," *The Cyber Defense Review* 3, no. 3 (Summer 2022): 91–99, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/08_Valeriano_CDR_V7N3_Summer_2022.pdf?ver=7MCo6VFl2ITu0SiNBMFWvg%253d%253d.

[5] A series of articles is presented in Michael E. Brown, Owen R. Cote, Jr., Sean M. Lynne-Jones, and Steven E. Miller, eds, *Offense, Defense, and War* (Boston: MIT Press, 2004), https://mitpress.mit.edu/9780262523165/offense-defense-and-war/.

From a theoretical and policy perspective, the cyber debates have been distracting rather than enlightening. An alternative theory—*cyber persistence theory*—argues that core structural features of cyberspace designate a systemic condition of offense-defense fluidity as opposed to offense or defense advantage/dominance.[6] The cyber debate (and analyses), therefore, ought to center on whether the condition designated by cyberspace's core structural features is advantage/dominance or fluidity. The policy salience of this debate cannot be overstated as structural theorists have convincingly argued that a failure to recognize prevailing conditions and align one's strategy with them increases the likelihood of strategic losses and elevates increasing international tensions.[7]

We proceed by briefly reviewing offense-defense theory with an emphasis on its structural form and by offering a limited review of cyber persistence theory's claim of a cyber systemic condition of offense-defense fluidity.[8] We then review how scholars and policymakers have applied offense-defense theory to cyberspace and conclude that, with one exception, micro-vulnerability/macro-resilience and mutability are implicated as core structural features associated with offense or defense advantage/dominance. Cyber persistence theory argues that these same structural features actually designate a condition of offense-defense fluidity.

Based on these core features, we offer a proof-of-concept for identifying a systemic condition of offense-defense fluidity or offense or defense advantage/dominance by analyzing the life cycles of actively exploited, publicly known vulnerabilities over a one-year period (2019). Findings from these analyses support the claim that the prevailing condition designated by cyberspace over this period was offense-defense fluidity.

We offer further evidence in support of structural theorists' general argument that strategic misalignment with structural conditions can lead to strategic losses and increased international tensions by presenting a brief history of U.S. cyber policy and strategy from 2010 through 2017, and we conclude by proposing new avenues of research based on our empirical findings.

Offense-Defense Theory

The underlying premise of offense-defense theory "properly specified" is that a core structural feature of the prevailing pool of technologies available to states designates a condition of offense or defense advantage/dominance that impacts the efficacy of a state's security strategy.[9] This condition acts as an

[6] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford: Oxford University Press, 2022).

[7] Kenneth Waltz argues, for example, that structure punishes states that fail to recognize the conditions it designates, and Jack Levy summarizes a number of historical cases highlighting the consequences of states misperceiving the prevailing offense-defense condition. Kenneth N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979) and Jack S. Levy, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis," *International Studies Quarterly* 28, no. 2 (June 1984): 219–238, http://links.jstor.org/sici?sici=0020-8833%28198406%2928%3A2%3C219%3ATOBOMT%3E2.0.CO%3B2-1. Fischerkeller, Goldman, and Harknett also argue that states not aligned to the structure of the cyber strategic environment increase their likelihood of suffering strategic losses.

[8] We do not address the debate regarding the application of offense-defense theory as applied to conventional capabilities. Although this is an important component of international relations and security studies scholarship, the focus in this article is on how the theory applies to cyberspace.

[9] On "properly specified" offense-defense theory, see Sean M. Lynn-Jones, "Offense-Defense Theory and Its Critics," *Security Studies* 4, no. 4 (1995): 660–691, https://doi.org/10.1080/09636419509347600. Lynn-Jones refers to "offense-defense theory"

intervening systemic variable that influences the outcomes of states' responses to the anarchic nature of the international system.[10] When applied to the pool of technologies composing conventional capabilities, it is argued that the pool determines the relative costs of offensive and defensive strategies at any given time. This may be understood as a structural feature that, in turn, designates a condition of either offense or defense advantage/dominance. Offense and defense advantage may be understood in terms of the amount of resources that a state must invest in offensive technologies to offset an adversary's investment in defensive technologies. A condition of offense advantage is designated when an investment in offensive technologies produces a military force that can defeat the force deployed by a state that has invested an equal amount in defensive technologies.[11] Advantage shifts toward the offense when innovation heralds a new type of weapon that makes it possible to pursue a given type of strategy at lower cost or by reducing the costs of producing a particular type of weapon. The velocity of shifts, themselves, has been measured in decades and centuries.[12]

Whereas a condition of offense and defense advantage/dominance impacts the efficacy of states' warfighting strategies, scholars argue that perceptions of the condition influence states' foreign policies. This notion has been studied in efforts to shed light on the causes of war,[13] arms races and arms control,[14] and alliance formation.[15]

Cyber Persistence Theory

---

as a collection of hypotheses about variations in the effects of the offense-defense balance. Additionally, Jack Levy and Keir Lieber note that most hypotheses relating to the offense-defense balance treat that concept as a systemic-level attribute. See Levy, "The Offensive/Defensive Balance of Military Technology" and Keir A. Lieber, "Grasping the Technological Peace: The Offense-Defense Balance and International Security," *International Security* 25, no. 1 (Summer 2000): 71–104, https://www.jstor.org/stable/2626774. For a discussion of how structural features designate conditions, see Waltz, *Theory of International Politics*, 69, 73.

[10] See Lynn-Jones, "Offense-Defense Theory and Its Critics," Glaser, "Realists as Optimists," and Jack Snyder, *Myths of Empire* (Ithaca, N.Y.: Cornell University Press, 1991).

[11] Lynn-Jones, "Offense-Defense Theory and Its Critics," 665–666. For similar definitions of the offense-defense balance, see Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 167–214, https://www.jstor.org/stable/2009958, and Charles L. Glaser, "Realists as Optimists: Cooperation as Self-Help," *International Security* 19, no. 3 (Winter 1994–1995): 50–90, https://www.jstor.org/stable/2539079. For a discussion of changes in the offense-defense balance over time, see Levy, "The Offensive/Defensive Balance of Military Technology," 230–234.

[12] This "relative cost of strategy" structural feature is discussed in Lynn-Jones, "Offense-Defense Theory and Its Critics," Glaser, "Realists as Optimists," Jervis, "Cooperation Under the Security Dilemma," and Charles L. Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" *International Security* 22, no. 4 (Spring 1998): 44–82, https://www.jstor.org/stable/2539240. Robert Gilpin references the same structural feature, but only for offense advantage. Robert Gilpin, *War and Change in World Politics* (Cambridge: Cambridge University Press, 1981), 62–63. For a discussion of changes in the offense-defense balance over time, see Levy, "The Offensive/Defensive Balance of Military Technology," 230–234.

[13] See Jervis, "Cooperation Under the Security Dilemma," 188–190, and Steven Van Evera, *Causes of War: Power and the Roots of Conflict* (Ithaca: Cornell University Press, 1999).

[14] George H. Quester, *Offense and Defense in the International System* (New York: John Wiley & Sons, 1977), chapter 17; Robert Powell, "Guns, Butter, and Anarchy," *American Political Science Review* 87, no. 1 (March 1993): 115–132, https://www.jstor.org/stable/2938960; and, Charles L. Glaser, "Political Consequences of Military Strategy: Expanding and Refining the Spiral and Deterrence Models," *World Politics* 44, no. 4 (July 1992): 497–538, https://www.jstor.org/stable/2010486.

[15] On alliances, see Stephen M. Walt, *The Origins of Alliances* (Ithaca: Cornell University Press, 1987), and Thomas J. Christensen and Jack Snyder, "Chain Gangs and Passed Bucks: Predicting Alliance Patterns in Multipolarity," *International Organization* 44, no. 2 (Spring 1990): 137–168, https://www.jstor.org/stable/2706792.

Cyber persistence theory, a structural theory of cyberspace security, argues that core structural features of the pool of technologies composing cyberspace—micro-vulnerability/macro-resilience and mutability—designate a condition of offense-defense fluidity, a condition that impacts the efficacy of a state's cyber security strategy. This argument rests on a review of numerous seminal, historical primary source documents offering discussions, descriptions, or concerns of core structural features of cyberspace. For example, David Clark's 1988 review of the design philosophy of the Internet highlights macro-resilience as a goal.[16] Willis Ware's 1970 *Security Controls for Computer Systems* highlights micro-vulnerability when stating "By their very nature, computer systems bring together a series of vulnerabilities" including "[h]ardware vulnerabilities [that] are shared among the computer, the communication facilities, and the remote units and consoles" and "software vulnerabilities at all levels of the machine operating system and supporting software."[17] And the *Computers at Risk* volume published by the National Research Council in 1991 states that "[t]he inherent mutability of software conflicts with the requirements for achieving security."[18]

To be clear, cyber persistence theory does not argue that cyber actors cannot hold a defensive or offensive advantage for some limited period of time; rather, it argues that such a circumstance is analytically distinct from defense or offense advantage/dominance as a structural condition.

Offense-Defense Theory in the Context of Cyberspace

Numerous scholars and policymakers have referenced, applied, or considered offense-defense theory in the context of cyberspace. This section highlights arguments that are consistent with the "properly specified" structural theory as described above—arguments that implicate, directly or indirectly, that a core structural feature of the prevailing pool of technologies composing cyberspace designates a condition of either offense or defense advantage/dominance. We cast a wide net to differentiate arguments that are structural from those that clearly are not. Most sources trace the systemic condition of offense or defense advantage/dominance to cyberspace's core structural features of either *micro-vulnerability/macro-resilience* or *mutability*. Micro-vulnerability/macro-resilience encapsulates the notion that vulnerabilities are abundant but do not affect macro-system integrity even when exploited at scale. This has been described as the "paradox of cyberspace" and is an apt descriptor of cyberspace that is empirically supported by its resilience in spite of relentless exploitation.[19] Mutability captures the notion that the prevailing pool of technologies composing cyberspace is liable to change.

---

[16] David D. Clark, "The Design Philosophy of the DARPA Internet Protocols," *Proceedings: SIGCOMM '88 Symposium Proceedings on Communications Architectures and Protocols* (Stanford: Stanford, CA, August 16–18, 1988), 106–114 and David D. Clark, *The Design Philosophy of the DARPA Internet Protocols: Version 1.2 of March 14, 2013* (Massachusetts Institute of Technology: Cambridge, MA, 2013), https://www.cs.princeton.edu/courses/archive/fall14/cos561/papers/ARPAdesign-revisited13.pdf

[17] Willis H. Ware, ed., *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security* (Santa Monica, CA: Rand Corporation, 1970), 3, https://www.rand.org/pubs/reports/R609-1.html.

[18] National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington D.C.: National Academies Press, 1991), 120, https://nap.nationalacademies.org/catalog/1581/computers-at-risk-safe-computing-in-the-information-age.

[19] The "paradox of cyberspace" is described by David Fahrenkrug when noting that any given node—a server, a router, a user's laptop or phone—is highly vulnerable, but when it is tied together in an overall network, a system can be incredibly resilient because the nature of networks is to be decentralized and redundant with multiple nodes and pathways and because civilian investment has created a thriving ecosystem with multiple options for most services. See Sydney J. Freedberg, Jr., "Cyber Lessons from Ukraine: Prepare for Prolonged Conflict, Not a Knockout Blow," *BreakingDefense,* May 1, 2023, https://breakingdefense.com/2023/05/cyber-lessons-from-ukraine-prepare-for-prolonged-conflict-not-a-knockout-blow/.

Micro-vulnerability/Macro-resilience

When announcing cyberspace as a new domain of warfare, then-U.S. Deputy Secretary of Defense William Lynne III stated that the offense is dominant in cyberspace for "structural" reasons, noting that an abundance of vulnerabilities are a consequence of a lower priority for security and identity management in the design of the Internet.[20] This view recurs in the 2023 U.S. National Cybersecurity Strategy, which states that advantage must be shifted to cyber defenders who are frustrated by the underlying "structural dynamics" of the digital ecosystem, the components of which are vulnerable to exploitation.[21] Unmentioned but understood in Lynne's statement and the 2023 Strategy is that the primary operational goal of the Internet's underlying architecture, upon which the viability of cyberspace rests, is that Internet communication must continue despite sub-systemic disruptions. That is, it must be macro-resilient.[22]

John Sheldon echoes an offensive advantage orientation by arguing that the defense is reliant on "vulnerable protocols" and "open architectures."[23] Joseph Nye, Jr., offers a similar rationale for offense advantage in noting that the Internet was designed for ease of use rather than security.[24] Kenneth Lieberthal and Peter Singer argue that the offense is advantaged because most of the products and systems that link into "this network of networks" are not designed with embedded security and that "there are many vulnerabilities that can be exploited."[25] Finally, Lucas Kello says that the offense is advantaged because systems increasingly rely on "off-the-shelf and offshore manufacturers for components, introducing vulnerabilities into the supply chain."[26] These arguments for offense advantage share the view that the prevailing pool of technologies composing cyberspace is fraught with an abundance of vulnerabilities but that cyberspace itself is macro-resilient.

Bruce Schneier argues that a primary reason that cyberspace favors the offense is the complexity of modern-day computer systems.[27] This is repeated in the New York Cyber Task Force's (NYCTF) 2017 report, which states that attackers are advantaged because "increasing complexity increases cost [for

---

[20] Lynn III, "Defending a New Domain." Various definitions of what cyberspace comprises abound. This article adopts Nazli Choucri's definition: a system composed of the physical foundations and infrastructure that enable the cyber playing field; the logical building blocks that support the physical platform and enable services; the information content stored, transmitted, or transformed; and the actors, entities, and users who participate in this arena. Nazli Choucri, *Cyberpolitics and International Relations* (Cambridge, MA: MIT Press, 2012), 8. For other definitions, see Slayton, "What Is the Cyber Offense-Defense Balance?", 74; Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 70, and David Clark, "Characterizing Cyberspace: Past, Present, and Future," https://ecir.mit.edu/sites/default/files/documents/%5BClark%5D%20Characterizing%20Cyberspace-%20Past%2C%20Present%20and%20Future.pdf.

[21] The White House, *National Cybersecurity Strategy, March 2023*, 1. Also see Anne Neuberger (Deputy National Security Advisor on Cyber and Emerging Technologies), "The U.S. Government's Global Cyber Initiatives."

[22] See Clark, "The Design Philosophy of the DARPA Internet Protocols" and Clark, *The Design Philosophy of the DARPA Internet Protocols: Version 1.2 of March 14, 2013*. For a discussion of systemic cyber risk, including case studies highlighting macro-resilience, see David Forscey, Jon Bateman, Nick Beecroft, and Beau Woods, *Systemic Cyber Risk: A Primer* (Carnegie Endowment for International Peace and the Aspen Institute, 2022), https://carnegieendowment.org/files/Bateman_et_al_Cyber_Risk_final_1.pdf.

[23] Sheldon, "Deciphering Cyberpower," 98.

[24] Nye, Jr., *Cyber Power*, 5.

[25] Lieberthal and Singer, "Cybersecurity and U.S.-China Relations," 13.

[26] Kello, "The Meaning of the Cyber Revolution," 29.

[27] Bruce Schneier, "Attack vs. Defense in Nation-State Cyber Operations," *Schneier on Security*, April 13, 2017, https://www.schneier.com/blog/archives/2017/04/attack_vs_defen.html.

defenders]" and "decreases the predictability of new costs."[28] Kello makes the same argument for offense advantage, noting that the complexity of the defense surface increases costs for defenders.[29] This rationale also appears in the 2023 U.S. National Cybersecurity Strategy, which argues that software and systems are growing more complex, "increasing our collective insecurity."[30] While these arguments appear to suggest that complexity is a structural feature that designates a condition of advantage, there is more to this argument than meets the eye. When associating complexity with offense advantage, the U.S. National Research Council (NRC) states that, regarding software systems, "as complexity and size increase, the probability of serious vulnerabilities increases more than linearly" and that "what correlates most strongly with lack of vulnerabilities in software is simplicity."[31] Martin Libicki similarly argues that "complexity is the source of much vulnerability."[32] Likewise, the NYCTF report notes that software complexity and "the massive scale of the Internet" aids attackers, as the combination results in "more doors left unlocked."[33] Thus, complexity itself is not a structural feature of cyberspace—rather, it is an antecedent to a core structural feature of micro-vulnerability/macro-resilience.

Schneier also proposes that a principal reason the offense is advantaged in cyberspace is that an attacker has an ability to choose the time and method of the attack, whereas a defender must necessarily secure against every type of attack.[34] Kello refers to this predicament as "offense unpredictability," where "the universe of unknown and manipulable weaknesses renders a cyberattack difficult to predict, complicating the design of measures to repulse it."[35] When the same argument is described by the U.S. NRC, however, it takes on a vulnerabilities-based orientation. The Council describes this predicament as follows: "the attacker must find but one of possibly multiple vulnerabilities in order to succeed; the security specialist must develop countermeasures for all."[36] Similar to complexity, these arguments treat offense unpredictability as a consequence of micro-vulnerability/macro-resilience.

Finally, some cyber scholars' attribute offense advantage to the relative cost of offensive or defensive strategies, adopting arguments made about conventional technologies. For example, Libicki argues that "another dollar's worth of offense requires far more than another dollar's worth of defense to restore prior levels of security."[37] But he also argues that "cyberattacks are possible only because systems have flaws" and "every information system has vulnerabilities—some more serious than others."[38] Thus, the relative cost of strategies is not the systemic feature but a consequence of cyberspace's core structural feature of micro-vulnerability/macro-resilience. Thomas Rid argues that the defense is advantaged in cyberspace because the offense has higher costs relative to the defense, given its shorter half-life after

---

[28] New York Cyber Task Force, *Building a More Defensible Cyberspace*, 9.
[29] Kello, "The Meaning of the Cyber Revolution," 28–29.
[30] The White House, *National Cybersecurity Strategy, March 2023*, 2.
[31] National Research Council, *Computers at Risk*, 121.
[32] Libicki, *Cyberdeterrence and Cyberwar*, 167.
[33] New York Cyber Task Force*, Building a Defensible Cyberspace*, 18.
[34] Bruce Schneier, "Attack vs. Defense in Nation-State Cyber Operations," *Schneier on Security*, April 13, 2017, https://www.schneier.com/blog/archives/2017/04/attack_vs_defen.html. Conversely, it has also been argued that *fingerprinters* (defenders seeking to track offender infrastructure) perpetually maintain a cyber advantage over offenders because fingerprinters only have to find *one* commonality among infrastructure, while offenders have to ensure *no* commonality is findable. See Bill Marczak, "Triangulation: Did "the NSA" Fail to Learn the Lessons of NSO?" *Medium*, June 3, 2023, https://medium.com/@billmarczak/triangulation-did-the-nsa-fail-to-learn-the-lessons-of-nso-5f36d251d02e.
[35] Kello, "The Meaning of the Cyber Revolution," 27.
[36] National Research Council, *Computers at Risk*, 14.
[37] Libicki, *Cyberdeterrence and Cyberwar*, 32.
[38] Ibid, xiii, 28.

discovery.[39] Rid's argument is not centrally about relative costs, but rather brings to the fore a second core structural feature of cyberspace that contributes to the designation of a condition of offense or defense advantage/dominance: mutability.

Mutability

Rid argues that the higher cost associated with a shorter half-life of the offense is a consequence of a defender's ability to discover and mitigate a vulnerability that has been exploited.[40] While presented in terms of cost, Rid makes clear in other statements that mutability, not cost, is a core structural feature of cyberspace that designates an offense-defense condition. He argues that, once discovered, vulnerabilities that enable an exploit will likely be patched or otherwise mitigated, and both he and Peter McBurney argue that even if a potent cyber-weapon could be launched successfully once, it would be highly questionable if an attack could be repeated to achieve a political goal.[41] Libicki also notes that discovering a specific vulnerability does not mean it will be there when the time comes to exploit it as the target, or a vendor may discover and mitigate the exploit in ways that are known or unknown to the attacker.[42] This is especially true, he argues, where serial reapplication of an exploit is desired:[43]

> Computer systems are mutable; indeed, when people say that cyberspace is the only man-made medium, what they are also saying is that it is the only man-alterable medium as well. Such alteration can take place rapidly. If the patch level of a system determines a target's susceptibility for attack, such a target may transition from vulnerability (to a particular attack) to invulnerability in, literally, minutes.[44]

Eviatar Matania and Eldad Tal-Shir argue that mutability advantages defenders because it enables them to "alter the state and composition of any assets over which cyberattackers and defenders contend."[45] Chris Bartos highlights mutability as a primary factor impacting the perishability and obsolescence of exploit code and, as a direct consequence, offense dominance/advantage.[46] The NYCTF's report claims that the offense is advantaged due to "rapid technological change," the consequence of which is an ever-expanding attack surface.[47] And the North Atlantic Treaty Organization's *Allied Joint Doctrine for Cyberspace Operations* says that "Cyberspace is not limited to, but at its core consists of, a computerised

---

[39] Rid, *Cyberwar Will Not Take Place*, 168.
[40] Ibid.
[41] Rid, *Cyberwar Will Not Take Place*, 168, and Rid and Peter McBurney, "Cyber-Weapons," 12. For an argument on why this is not always be the case, see Jay Healey, "The Lingering Power of Cyber Brandishing," *Lawfare*, January 18, 2022, https://www.lawfareblog.com/lingering-power-cyber-brandishing.
[42] Consider, for example, the software updating model of "continuous deployment," a software engineering practice of deploying many small incremental software updates into production, leading to a continuous stream of tens, hundreds, or even thousands of deployments per day. Firms including Facebook, Amazon, Google, LinkedIn, Adobe, Tesla, Netflix, Flickr, and Etsy have embraced this update model. Tony Savor, Mitchell Douglas, Michael Gentili, Laurie Williams, Kent Beck, Michael Stumm, "Continuous Deployment at Facebook and OANDA," *ICSE 2016: 38th IEEE Conference on Software Engineering*, https://research.fb.com/publications/continuous-deployment-at-facebook-and-oanda/.
[43] Libicki, *Cyberdeterrence and Cyberwar*, 55–56.
[44] Martin C. Libicki, "Second Acts in Cyberspace," *Journal of Cybersecurity* 3, no. 1 (March 2017): 29–35, https://doi.org/10.1093/cybsec/tyw014.
[45] Eviatar Matania and Eldad Tal-Shir, "Continuous Terrain Remodelling: Gaining the Upper Hand in Cyber Defence," *Journal of Cyber Policy* 5, no. 2 (2020): 285–301, https://doi.org/10.1080/23738871.2020.1778761.
[46] Captain Christopher A. Bartos, "Cyber Weapons are Not Created Equal," *Proceedings Magazine* 142, no. 6 (June 2016), 30–33, https://www.usni.org/magazines/proceedings/2016-06/cyber-weapons-are-not-created-equal.
[47] Healey, "The Attacker Has the Advantage in Cyberspace."

environment, artificially constructed and constantly under development."[48] These arguments share the view that mutability is a structural feature of cyberspace that contributes to the designation of a condition of offense or defense advantage.

Non-Structural Arguments

Some arguments regarding advantage are not structural. For example, Rid argues that as systems (targets) become more complex, the knowledge required to exploit them also becomes more complex, thus resulting in a tenuous security advantage for the defender.[49] Jon Lindsay makes a similar claim couched in a larger argument that a "more precise specification of scope conditions of offense dominance in cyberspace is much needed."[50] Both Rid and Lindsay's arguments do not view complexity as a structural feature of cyberspace, nor do they imply that offense-defense advantage is a systemic condition. Rather, Rid and Lindsay consider complexity and advantage as narrowly scoped and call for additional scoped analyses. This is consistent with Rebecca Slayton's argument, the latter part of which is challenged by this article, that "[o]ne can assess the offense-defense balance of cyber operations between two adversaries, but not of cyberspace."[51]

Finally, the NYCTF's report argues that cyberspace is offense advantaged because attackers have incentives to attack, such as profit motives (cybercrimes), sanctuary they could be offered by certain nations, and weaknesses in national laws.[52] But, to paraphrase Jack Levy, arguing that the incentive to act increases the likelihood that technology favors the offense is a tautology and hence has no explanatory power.[53] Focusing attention on the incentive to attack ignores the more basic question of what conditions create an incentive to attack. While the Task Force offers a set of rationales that incentivize attacking, they do not speak to structural features of the prevailing pool of technologies composing cyberspace.

A Proof of Concept

All the arguments supporting claims of a condition of offense advantage in cyberspace directly or indirectly implicate micro-vulnerability/macro-resilience as a core structural feature that contributes to the designation of that condition. With one exception, all of the arguments supporting claims of a condition of defense advantage directly or indirectly implicate mutability as a core structural feature that contributes to the designation of that condition. But in his former role as Deputy Director of the US. National Security Agency, Chris Inglis succinctly described the consequence of the co-existence of both of these structural features (in the context of offense-defense theory):

[48] North Atlantic Treaty Organization, *Allied Joint Publication 3-20: Allied Joint Doctrine for Cyberspace Operations*, January 2020, 1, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.
[49] Rid, *Cyberwar Will Not Take Place*, 73.
[50] Lindsay, "Stuxnet and the Limits of Cyber Warfare," 396.
[51] Slayton, "What Is the Cyber Offense-Defense Balance?" 74.
[52] New York Cyber Task Force Report, *Building a Defensible Cyberspace,* 8.
[53] Levy, "The Offensive/Defensive Balance of Military Technology," 228.

> It's almost impossible to achieve a static advantage in cyberspace—*whether that's a competitive [offensive] advantage or a security [defensive] advantage*—when things change every minute of every hour of every day. And it's not just the technology that changes; it's the employment of that technology; the operations and practices.[54]

Inglis' comment suggests that a static condition of advantage lasting decades or centuries, as has been documented by historians of the conventional technology offense-defense balance, does not hold in cyberspace because the systemic offense-defense balance is continuously in flux.[55] It is in flux because cyberspace's core structural features designate a condition of offense-defense fluidity. In the next section, we introduce an approach for evaluating the offense-defense and cyber persistence theories' competing propositions of offense or defense advantage/dominance and offense-defense fluidity, respectively.

Measuring Cyber Systemic Conditions of Offense-Defense Fluidity and Offense or Defense Advantage/Dominance

The condition designated by cyberspace's core structural features of micro-vulnerability/macro-resilience and mutability may be identified by analyzing the life cycles of actively exploited, publicly known vulnerabilities. Vulnerability life cycles are records of the manifestations of micro-vulnerability/macro-resilience and mutability within subsets of the pool of technologies composing cyberspace. Analyzing how these core structural features manifest in vulnerability life cycles provides a measure of the prevailing condition in these subsets that, when amalgamated, indicates the prevailing cyber systemic condition, whether it be fluidity or advantage/dominance.

A vulnerability's life cycle is defined as the period from first discovery through the spread of exploitation attempts across the Internet to when the vulnerability eventually becomes widely remediated.[56] Many vulnerabilities are publicly enumerated in the Common Vulnerabilities and Exposures (CVE) List.[57] A study by Kenna Security and the Cyentia Institute focused on the more than 18,000 vulnerabilities published to the CVE List in 2019 and tracked their life cycles through the first half of 2020 as, for this time period, they have "solid data sources" for vulnerability scanning and remediation across hundreds of organizations and data on "exploitation in the wild" of these vulnerabilities for over 100,000 organizations.[58] From the 2019 List, 473 unique CVEs were identified that were subject to exploitation-

---

[54] Chris Inglis as quoted in Amber Corrin, "Is Government on the Wrong Road with Cybersecurity?" *FCW: The Business of Federal Technology*, May 21, 2013, https://fcw.com/articles/2013/05/21/csis-cybersecurity.aspx. Inglis' reference to operations and practices highlights that cyberspace is a socio-technological system, not merely a technological system. This does not, however, undermine arguments regarding micro-vulnerability/macro-resilience and mutability. Instead, it merely identifies another layer atop the physical and logical layers of cyberspace, in and through which vulnerabilities (weak passwords and configuration errors) and mutability (reconfigurations, policies, and security practices) are introduced.

[55] Levy, "The Offensive/Defensive Balance of Military Technology," 230–234.

[56] *Prioritization to Prediction, Volume 6: The Attacker-Defender Divide* (Cyentia Institute, 2020), 3. For a similar definition, see William A. Arbaugh, William L. Fithen, and John McHugh, "Windows of Vulnerability: A Case Study Analysis," *IEEE Computer* 33, no. 12 (2000): 52–59, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=889093.

[57] See https://cve.mitre.org/. It should not be assumed that the CVE List contains an exhaustive and complete compilation of every unique, known vulnerability as not every vendor and vulnerability researcher submit vulnerabilities and vendors may fix vulnerabilities "quietly." For a discussion of what the CVE List comprises and what it does not, see Eugene H. Spafford, Leigh Metcalf, and Josiah Dykstra, *Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us* (Boston: Addison-Wesley, 2023), 215–217.

[58] See *Prioritization to Prediction, Volume 6*. In *Volume 6*, exploitation data were aggregated from a total of six independent sources. Five of these were compiled by Kenna Security, including two intrusion detection services, two open source threat

in-the-wild attempts—approximately 2.5 percent.[59] Analyses of exploitation-in-the-wild attempts within a six-month window following the publication of each CVE identified more than 228 million observed instances (assets) in the top 10 most prevalent vendors.[60] These data support a proof-of-concept for measuring a cyber systemic condition of fluidity and advantage. The proof-of-concept finds that such a condition can indeed be measured and that the prevailing condition in the sample is offense-defense fluidity, thus refuting claims of cyberspace offense or defense dominance/advantage as well as assertions that scholars cannot measure a systemic condition of fluidity or advantage.[61]

To measure a cyber systemic condition of fluidity or advantage, we first define ideal-type defensive and offensive baselines—that is, vulnerability life cycles that represent ideal-type sequences of life-cycle milestones for defenders and offenders. These ideal-type sequences may be considered the left and right boundaries of the spectrum of all potential permutations of life-cycle milestones. A systemic condition of fluidity or advantage/dominance may then be measured relative to these baselines at any given time for the population of publicly known and actively exploited vulnerabilities enumerated in the CVE List. Moreover, the systemic condition could conceivably be tracked over time.

intelligence services, and one malware analysis service. The sixth source was Fortinet. Additional, smaller-scale studies that provide relevant insights are also referenced in this article. Note that exploitation "in the wild" distinguishes exploit code in controlled laboratory cyber environments from exploit code spreading among unwilling or unsuspecting users' devices in the course of the ordinary operation of those devices. Additionally, the phrase refers to both attempts at exploitation and successful exploitation. See https://thecyberwire.com/glossary/wild-the.

[59] This 2.5 percent finding is consistent with findings of other studies. For example, of 94,597 vulnerabilities published in the CVE List from 1999 through 2017 (where 1999 marks the inception of the List), the Cyentia Institute found that only 2% of this population of CVEs has been actively exploited in the wild. See *Prioritization to Prediction, Volume 3: Analyzing Vulnerability Remediation Strategies* (Cyentia Institute, 2018), 7. Additionally, of the 12,243 unique CVEs listed from June 1, 2016, to December 31, 2022, the Institute observed 6.4% had been exploited. See Jay Jacobs, Sasha Romanosky, Octavian Suciu, Benjamin Edwards, Armin Sarabi, "Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights," *arXiv:2302.14172* (2023), https://doi.org/10.48550/arXiv.2302.14172.

[60] *Prioritization to Prediction, Volume 6*, 3.

[61] See, respectively, Brandon Valeriano, "The Failure of Offense/Defense Balance in Cyber Security," *The Cyber Defense Review* 3, no. 3 (Summer 2022): 91–99, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/08_Valeriano_CDR_V7N3_Summer_2022.pdf?ver=7MCo6VFl2ITu0SiNBMFWvg%253d%253d and Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?" *International Security* 41, no. 3 (Winter 2016/17): 72–109, https://www.jstor.org/stable/10.2307/26777791. Valeriano's argument that a condition (he uses the term "balance") cannot be measured is largely based on the structural feature that is proposed in scholarship on offense-defense theory in the context of conventional technologies (i.e., the relative costs of offensive and defensive strategies). As the literature review presented in this article illustrates, most cyber scholars do not view that feature as a designator of cyber offense or defense advantage/dominance. Slayton argues that only a dyadic condition of offense or defense advantage/dominance is measurable.

A defender's ideal-type sequence of life-cycle milestones for its own vulnerabilities is as follows:[62] a patch being made available,[63] vulnerability scanning by asset owners,[64] remediation efforts by asset owners,[65] a CVE being published, publicly disclosed proof-of-exploit code,[66] and exploitation in the wild (see Figure 1). Several of these milestones are technological actions (manifestations of mutability) that present opportunities for defenders and offenders to seize or sustain the initiative over the course of the life cycle.[67] For example, patch availability, vulnerability scanning, and remediation are opportunities for defenders, whereas exploit code disclosure and exploitation in the wild are opportunities for offenders.[68] Alternatively, the publication of a CVE offers opportunities simultaneously for both

[62] This is not to suggest this is the only ideal-type for defenders. Any CVE life cycle that begins with a combination of the three milestones that seize or sustain the initiative solely for defenders, that is, strictly favors defenders, could be an ideal-type. For example, remediation may be a possible initial milestone if the vulnerability can be addressed via compensating controls (rather than patching), and defenders may receive insights on malware signatures that enable vulnerability scanning for a CVE before a patch is released.

[63] Note that, whereas a vulnerability life cycle was previously described as originating with discovery, data for the date of discovery is often not publicly shared, thus making it an unreliable life-cycle milestone measure. The same holds for CVE reservation, as a reservation is not consistently associated with the discovery date of a vulnerability. Inconsistencies may arise, for example, from the fact that numerous CVE naming authorities, those authorized to assign CVE identifications to vulnerabilities, reserve blocks of identifications in advance of actual vulnerability discovery. See Stephen Watts, "What Is CVE? Common Vulnerabilities and Exposures Explained," *bmc blogs*, May 21, 2020, https://www.bmc.com/blogs/cve-common-vulnerabilities-exposures/#:~:text=CNAs%20are%20given%20a%20block%20of%20CVE%20numbers,national%20and%20industry%20CERTS%3B%20and%20bug%20bounty%20programs. Conversely, reliable data on patches (or vulnerability scanning or remediation) can be collected by directly looking up vendors' sites and vendor-neutral websites. See Guido Schryen, "Is Open Source Security a Myth?" *Communications of the ACM* 54, no. 5 (May 2011): 130–140, https://dl.acm.org/doi/10.1145/1941487.1941516.

[64] Vulnerability scanners are able to identify a variety of systems running on a network, such as laptops and desktops, virtual and physical servers, databases, firewalls, switches, and printers. Identified systems are probed for different attributes: operating system, open ports, installed software, user accounts, file system structure, system configurations, and more. This information is then used to associate known vulnerabilities to scanned systems. Vulnerability scanners perform this association by using a vulnerability and exploit database that contains a list of publicly known vulnerabilities. See "Vulnerability Management Process, *Rapid 7*, https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/.

[65] Remediation may include deploying updates, patching, modifying system configurations, implementing compensating controls, or otherwise addressing a vulnerability so that it is no longer an exposure. For examples of remediation based on modifying system configurations, see Zeljka Zorz, "PoC Exploit for Recently Patched Microsoft Word RCE is Public (CVE-2023-21716)," *Help Net Security*, March 6, 2023, https://www.helpnetsecurity.com/2023/03/06/cve-2023-21716-poc/ and Cisco Security Advisory, "SNMP Remote Code Execution Vulnerabilities in Cisco IOS and IOS XE Software," June 29, 2017, https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp. For a discussion of compensating controls, see Rick Kaun, "Compensating Controls in ICS Security," Verve, January 14, 2021, https://verveindustrial.com/resources/blog/compensating-controls/.

[66] Also known as a proof-of-concept exploit, proof-of-exploit code is a non-harmful attack against a computer or network. Such exploits are not meant to cause harm, but to show security weaknesses within software. Although, when proof-of-exploit code is publicly shared before a weakness is patched, it leaves software and networks vulnerable to exploitation. See "Proof-of-concept Exploit," *TechTarget*, https://www.techtarget.com/searchsecurity/definition/proof-of-concept-PoC-exploit. For a case study highlighting how rapidly offenders act on the publication of a proof-of-concept exploit, see Ryan Barnett, "The Race to Patch: Attackers Leverage Sample Exploit Code in Wordpress Plugin," Akamai Blog, May 11, 2023, https://www.akamai.com/blog/security-research/attackers-leverage-sample-exploit-wordpress-plugin.

[67] Technological actions may be understood as actions performed through, or mediated by, some kind of technology. See Asle H. Kiran, "The Concept of a Technological Action," May 29, 2009, https://www.academia.edu/2095093/The_Concept_of_a_Technological_Action.

[68] There is evidence that offenders are, at times, able to reverse engineer exploit code from a patch. However, reverse engineering requires an additional step, and thus patch availability presents a first opportunity to defenders, not offenders. See https://www.techtarget.com/searchsecurity/feature/An-introduction-to-binary-diffing-for-ethical-hackers. Additionally, some argue that publishing exploit code presents opportunities to defenders. However, there is empirical evidence that publishing exploit code before a patch is released is far more likely to enable offenders to seize and sustain the initiative. For an argument that it favors defenders, see Robert Lemos, "Attackers Crib Exploit Code, But Net Benefit for Defenders," *DarkReading*, October 30, 2013, https://www.darkreading.com/attacks-breaches/attackers-crib-exploit-code-but-net-benefit-for-defenders. For an

defenders and offenders.[69] Figure 1 is an ideal-type life cycle for defenders because the defender has the first opportunities to seize and sustain the initiative. Should they do so, any first opportunities that emerge for the offender will have few, if any, non-remediated vulnerabilities to exploit.

Figure 1: A Defender's Ideal-Type Sequence of Life-cycle Milestones

Alternatively, the initial milestones in an offender's ideal-type (Figure 2) would include exploitation in the wild and exploit code being available, followed by CVE publication, patch availability, vulnerability scanning, and remediation. The dynamic in this ideal-type differs from the defender's ideal-type as offenders have the first opportunity to seize and sustain the initiative, and defenders can only begin to seize the initiative from offenders as milestones come to pass that offer them opportunities to do so.

Figure 2: An Offender's Ideal-Type Sequence of Life-cycle Milestones

With this understanding, we can evaluate the hypothesis that micro-vulnerability/macro-resilience and mutability designate a condition of offense or defense advantage/dominance. The null hypothesis—that these features do not designate a condition of offense or defense advantage/dominance—serves as a test of the condition of offense-defense fluidity.

If a majority of life cycles (51%) of actively exploited CVEs aligns with the defender's ideal-type sequence of life-cycle milestones or in any other way favors the defender *for a sustained period*, it could be argued that the systemic condition designated by micro-vulnerability/macro-resilience and mutability is defense dominance and advantage, respectively. Using the color coding in Figures 1 and 2, defense advantage would appear graphically as a list of life-cycle permutations with milestones that all started with a light

empirical analysis that it favors offenders, see *Prioritization to Prediction, Volume 7: Establishing Defender Advantage* (Cyentia Institute, 2021).

[69] This is because after a CVE is published, all of the information regarding the vulnerability that could support offensive or defensive technological actions is publicly known. At this time, most security vendors start developing their vulnerability signature and protection strategy, and this is also the time that many adversaries begin seeking to exploit the vulnerability. Regarding the latter, in a three-month study of 50 global enterprises, Palo Alto Networks reported that, on a typical day, defenders' Internet-facing assets were scanned for vulnerabilities every hour by potential offenders. However, after the disclosure of a CVE, potential offenders scan even more frequently—within 15 minutes or less. See *2021 Cortex Xpanse Attack Surface Threat Report* (Palo Alto Networks, 2021), https://start.paloaltonetworks.com/asm-report. Also, see Jay Chen, "The State of Exploit Development: 80% of Exploits Publish Faster than CVEs," Unit 42: Palo Alto Networks, August 26, 2020, https://unit42.paloaltonetworks.com/state-of-exploit-development/. Scanning by offenders has been described as the first step in their funnel of opportunity, which comprises the following steps: scanning for IPs and open ports, crawling for specific services, moving on to test for specific CVEs, and, finally, executing remote code to gain access to a system. See Verizon, *Data Breach Investigation Report, 2008–2022*, https://www.verizon.com/business/en-gb/resources/reports/dbir/, 31.

shade and gradually transitioned to a dark shade. If a majority of life cycles of actively exploited CVEs aligns with the offender's ideal-type *for a sustained period*, the condition is one of offense dominance and advantage. This would appear graphically with the initial milestones having darker shades and shifting to lighter shades.

The null hypotheses of offense-defense fluidity would be supported when a majority of life-cycle permutations differ from the defensive and offensive ideal-types. The greater the number of permutations, the greater the systemic offense-defense fluidity.

Figure 3 shows three groupings of life-cycle permutations selected from the top, middle, and bottom of the full list of 148 observed permutations of the 473 actively exploited CVEs in the sample. Three subsets are offered to illustrate the numerous permutations observed across the breadth of total observations.

Figure 3: Three Groupings of Life-cycle Milestone Permutations of Publicly Known, Actively Exploited Vulnerabilities (Top, Middle, and Bottom Five)

In the top five life cycles, the first permutation of milestones nearly matches the defender's ideal-type—patch available, vulnerability scanning, remediation, CVE published, and exploitation in the wild—and was observed in 10.8% of the total sample of CVE life cycles analyzed. Summing the percentages of life-cycle permutations where the first three milestones strictly favor defenders (i.e., any combination of patch available, vulnerability scanning, and remediation) results in a value of 20% of the total sample. This percentage falls well short of a majority of permutations (51%) required to support the hypothesis that cyberspace's core structural features designate a condition of defense advantage/dominance. Note that no permutation approximating an offender's ideal-type is evident in the top five life cycles. On the other hand, summing the percentages of life-cycle permutations where the first two milestones strictly

favor offenders (i.e., exploited in the wild and exploit code available) results in a value of 1.2% of the total sample. This small percentage suggests little empirical support for a condition of offense advantage/dominance.

For some of the remaining CVEs in Figure 3, CVE publication precedes patch availability, exploitation in the wild is the initial action, and exploit code is published prior CVE publication.[70] Additionally, not all life cycles comprise all of the milestones—exploit code may never be published or it may be published without being associated with a published CVE. Further, there are "ties" where some milestones are realized simultaneously (these are represented through asterisks in the figure). Of the 148 distinct permutations observed in the sample of 473 vulnerability life cycles, those that deviate from defender's and offender's ideal-types comprise over 79% of the sample.[71] They appear graphically as a checkerboard pattern in Figure 3 (rather than transitioning from light to dark or dark to light). This 79% is evidence that micro-vulnerability/macro-resilience and mutability designate a systemic condition of offense-defense fluidity.

Offense-defense fluidity becomes even more apparent when applying different lenses to analyze the course of life cycles over the 18-month period accounted for in the sample.[72] Figure 4 offers two different lenses. First, from January 1 to July 1, 2019, milestones that enable defender and offenders to seize/sustain the initiative occurred simultaneously across CVE life cycles. This is illustrated in the first five life cycles (viewed top to bottom) displayed in Figure 4. Additionally, not all of the initial milestones for the 148 life-cycle permutations in the sample were observed on January 1, 2019. CVEs are published on a rolling basis and thus life-cycle milestones across the CVEs, some of which enable the offense and some the defense to seize/sustain the initiative, overlap over time.[73] This is illustrated in the last five life cycles displayed in Figure 4. All of these observations reinforce the finding from Figure 3 that the prevailing systemic condition in this sample is offense-defense fluidity.

[70] For CVE case studies in which exploitation and patching were the initial actions, see Kathleen Metrick, Jared Semrau, and Shambavi Sadayappan, "Think Fast: Time Between Disclosure, Patch Release and Vulnerability Exploitation—Intelligence for Vulnerability Management, Part Two," *Mandiant Threat Research*, April 13, 2020, https://www.mandiant.com/resources/blog/time-between-disclosure-patch-release-and-vulnerability-exploitation.
[71] *Prioritization to Prediction, Volume 3*, 7.
[72] Whereas the CVE sample itself is from the 12-months composing 2019, a minimum of six months was allowed for every CVE life cycle to play out. Thus, for CVEs listed in December 2019, data regarding their life cycles were gathered through June 2020, thereby making the overall period of analysis 18 months.
[73] In 2019, roughly 1,100 new CVEs were published each month. See https://www.cvedetails.com/browse-by-date.php. Of those, roughly 40 CVEs per month were actively exploited.

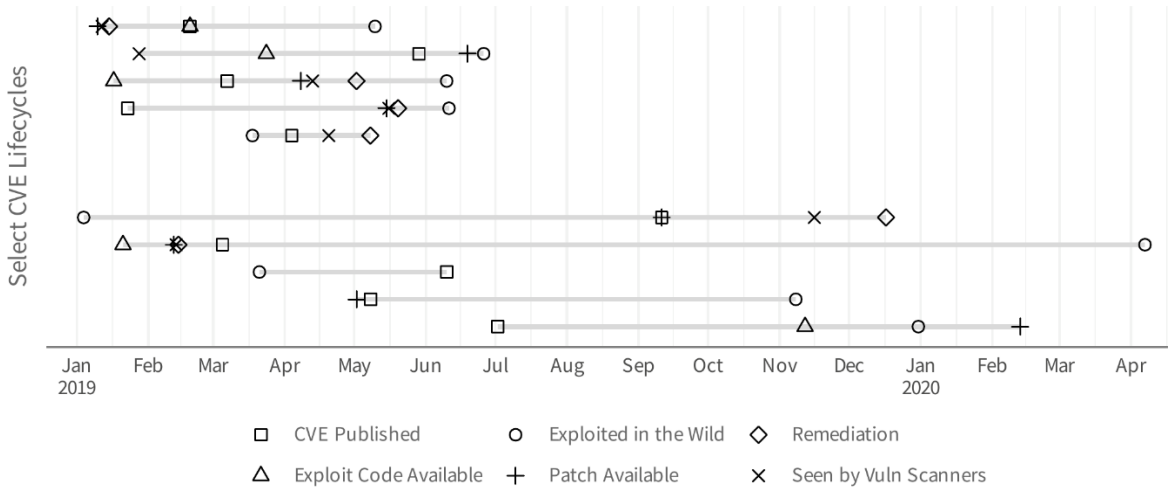

Figure 4: Concurrent and Chronologically Overlapping Life Cycles

The findings presented in Figures 3 and 4 support our claims that a cyber systemic condition of offense-defense fluidity or offense and defense advantage/dominance can be measured and that the prevailing condition in 2019 was offense-defense fluidity. Life-cycle milestone sequences favoring the defense or offense never represent the majority of the sample, either at a single point of time or over a sustained period. For the foreseeable future, there is little reason to expect the 2019 prevailing condition of offense-defense fluidity to be supplanted by one of enduring advantage or dominance.[74] This empirical evidence suggests that cyber persistence theory, not offense-defense theory, offers more descriptive and explanatory power for analyzing state cyber behaviors. Importantly, it also suggests that cyber persistence theory is the aligned framework upon which to derive conditions-based strategy and policy prescriptions, whereas offense-defense theory misdirects from understanding, measurement, and management of the fundamentals of cyberspace security.

An Opportunity-based Analysis versus an Execution-based Analysis

Although Figure 3 presents life-cycle milestones as a series of discrete, chronological actions, they may often overlap. The technological actions (milestones) that life cycles comprise present opportunities for defenders and offenders to seize and sustain the initiative, but they are not always seized, seized in a timely manner, or seized at once by the entire population of actors seeking to either remediate or exploit vulnerable assets.[75] Any one of these three factors can disrupt the integrity of a CVE life-cycle

[74] Even if "secure-by-design" and "secure-by-default" networks, systems, and devices begin to gradually populate the cyber strategic environment, their impact on the condition of fluidity will likely not be notable for years given that cyberspace comprises billions of assets. Regarding these design and development concepts, see Cyber Security and Infrastructure Security Agency, *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default*, April 13, 2023, https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf. For a specific example of how a development choice can reduce vulnerabilities, see Thomas Claburn, "Microsoft Is Busy Rewriting Core Windows Code in Memory-safe Rust," *The Register*, April 27, 2023, https://www.theregister.com/2023/04/27/microsoft_windows_rust/ and Thomas Claburn, "Memory Safety is the New Black, Fashionable and Fit for Any Occasion," *The Register*, January 26, 2023, https://www.theregister.com/2023/01/26/memory_safety_mainstream/.

[75] For an analysis of patching opportunities not being seized at once by the entire population of actors seeking to secure vulnerable assets, see Bill Toulas, "15 million Public-Facing services Vulnerable to CISA KEV Flaws," *Bleeping Computer*, March

milestone sequence defined by emergent opportunities. For example, at the asset-owner level of analysis, should a life cycle's initial milestone be a patch made available but not immediately deployed, offenders could seize the initiative by reverse-engineering an exploit from the patch and exploiting the vulnerability in the wild before the asset owner engages in vulnerability scanning and/or remediation.[76] Similarly, should the initial milestone for a CVE life cycle be the publication of exploit code, an offender may not act in a timely enough manner and miss the opportunity to exploit an asset owner's vulnerable assets before a patch is made available and remediation commences. Increasing the scope of CVE life-cycle analysis beyond a single asset defender and offender to include the total population of asset owners (and their vulnerable assets) and offenders elevates the impact of these factors to the systemic level. At this level, the times to remediation by asset owners and to exploitation by offenders will vary across the total population, potentially from hours to weeks, months, or even years, until, and if, the vulnerability eventually becomes widely remediated.[77]

This reality aligns with the general core logic of cyber persistence theory, so the theory would benefit from an additional specification that more precisely captures this aspect of the cyber systemic condition of offense-defense fluidity. We describe this as an execution-based analysis of fluidity. Figures 3 and 4 represent opportunity-based analyses, which are determined by analyses of unique milestone sequences that represent first opportunities to seize and sustain the initiative for offenders and defenders over the course of a CVE life cycle. Execution-based analyses are informed by these data but also include data and analyses of when these opportunities actually are seized upon and how well the effort is sustained.

At present, data exists to support opportunity-based analyses but not execution-based analyses. This is not to argue that execution-based analyses are out of reach. There are analytical techniques, such as survival analysis, that can be applied to estimate, for example, the probability of vulnerability instances surviving (i.e.,, still being available for exploitation) after a certain period of time of interest has elapsed (think of the speed and spread of remediation).[78] This is illustrated in Figure 5, which presents the top five, middle five, and bottom five life-cycle permutations from the sample where remediation (renamed

---

31, 2023, https://www.bleepingcomputer.com/news/security/15-million-public-facing-services-vulnerable-to-cisa-kev-flaws/amp/.

[76] For case studies of this phenomenon, see Kathleen Metrick, Jared Semrau, and Shambavi Sadayappan, "Disclosure, Patch Release and Vulnerability Exploitation—Intelligence for Vulnerability Management, Part Two," Mandiant (now a part of Google Cloud), April 13, 2020, https://www.mandiant.com/resources/blog/time-between-disclosure-patch-release-and-vulnerability-exploitation and Ian Beer, "Mind the Gap," *Project Zero*, November 22, 2022, https://googleprojectzero.blogspot.com/2022/11/mind-the-gap.html.

[77] For a longitudinal analysis of the prevalence of exploitation in the wild, see *Prioritization to Prediction, Volume 6*, 15–16.

[78] Generally speaking, *survival analysis* is a branch of statistics for analyzing the expected duration of time until an event occurs, such as death in biological organisms and failure in mechanical systems. In regard to vulnerability remediation, if one assumes that an organization observes 100 live/open vulnerabilities within its assets today (Day Zero) and manages to remediate 10 of them, leaving 90 to live another day, the survivability rate on Day Zero would be 90% with a 10% remediation rate. As time passes and vulnerabilities continue to be remediated, that proportion will continue to change. Tracking this change over time allows one to estimate at what future point in time all vulnerabilities (or a percentage of interest that is less than 100%) will be remediated by that organization. The same approach can be taken where the entity of interest is not an organization's remediation velocity, but rather the velocity at which a specific CVE is remediated across all organizations in a sample. That is the approach we have taken in this article, and we used the Kaplan-Meier curve to account for challenges to estimation posed by, for example, new and vulnerable systems/devices being added the sample after the initial instance of a vulnerability is catalogued, existing vulnerable systems being retired before the end of the period of analysis, and vulnerability instances not being remediated before the end of the period of analysis. For a review of survival analysis, see John P. Klein, Hans C. van Houwelingen, Joseph G. Ibrahim, and Thomas H. Schieke, eds., *Handbook of Survival Analysis* (Routledge, 2020). For an example of how survival analysis may be applied to vulnerabilities, see *Prioritization to Prediction, Volume 3: Winning the Remediation Race* (Cyentia Institute, 2019).

Remediation Half-Life in the figure) is located in the life cycles (and, therefore, in time) based on survival analyses estimates of when the majority (greater than 50 percent) of the CVE's vulnerability instances would be remediated (or less than 50 percent could be exploited).[79]

Figure 5: Three Groupings of Life-cycle Milestone Permutations of Publicly Known, Actively Exploited Vulnerabilities Incorporating Remediation Survival Analysis (Top, Middle, and Bottom Five)[80]

Unlike the first row of Figure 3, the first row of Figure 5 does not approximate a defender's ideal-type, as the first three milestones do not strictly favor defenders. Life-cycle permutations where the first three milestones strictly favor defenders comprise 0.6% of the total sample. As in Figure 3, this falls well short of 51% of the overall sample, and so these data do not support the hypothesis that the prevailing condition in this sample is defense advantage/dominance. In the fourth row of Figure 5, the life-cycle permutation nears but does not satisfy the ideal-type requirement for strictly favoring offenders. Life-cycle permutations where the first two milestones strictly favor offenders comprise 1.6% of the total sample and, thus, do not support claims that the prevailing condition is offense advantage/dominance. The remainder of the rows, nearly 98% of the total sample, appear as a checkerboard pattern, which is indicative of a condition of offense-defense fluidity.

A closer comparison of Figures 3 and 5 reveals additional noteworthy findings. In the first row of Figure 5, which certainly includes some of the sample that populates the first row of Figure 3, the Remediation

[79] The value of 51% was selected based on the logic that defenders have seized the initiative after remediating more than half of the instances of a publicly known, actively exploited vulnerability.

[80] Data indicating vulnerability survival rates for CVEs were tracked from 2019 to 2021 (40 months). This differs from the 18-month period used to generate Figure 3, because the larger the sample size for survival curve analyses (i.e., the more data points indicating remediation events), the more one can be confident that the curve approaches the true survival function. Were the survival analyses truncated at 18 months, we would be less confident in these findings.

milestone has shifted to the right. This reveals that CVEs were published before a remediation half-life was realized in these vulnerability life cycles. This 'defender's lag' allowed offenders to seize the initiative from defenders (as published CVEs aid both defenders and offenders). This likely occurred in other life-cycle permutations as well; a claim that is supported by the fact that the total percentage of life-cycle permutations favoring defenders decreased from 20% to 0.6% in Figures 3 and 5, respectively.[81] Additionally, note that the summed percentages of the top five in Figure 3 (25.5%) exceed the summed percentages of the top five in Figure 5 (18.6%). This suggests that the execution-based analyses generated more distinct permutations than did the opportunity-based analysis. This, indeed, is the case as the execution-based analyses generated 188 unique permutations—40 more than the opportunity-based analysis. Recall that the greater the number of permutations that deviate from defender and offender ideal-type life cycles, the greater the offense-defense fluidity. Clearly, execution-based analyses can reveal insights that opportunity-based analyses cannot. However, these additional insights do not challenge our conclusion that cyberspace designates a condition of offense-defense fluidity.

It is important to note that Figure 5 tells only half of the execution-based story as exploitation in the wild also occurs over time, so survival analysis ought to also be applied to the exploitation-in-the-wild milestone to create an exploitation-in-the-wild half-life. Doing so likely would alter the location of exploitation-in-the-wild milestones in numerous CVE life cycles, just as it did for remediation (as shown in Figure 5). Unfortunately, this is not possible at this time, as no large dataset of publicly known and actively exploited vulnerabilities distinguishes between attempted (opportunity) and successful (execution) exploitation. For example, the Cybersecurity and Infrastructure Security Agency's (CISA's) Known Exploited Vulnerabilities Catalog defines active exploitation as comprising both "attempted exploitation," which occurs when an offender executes code on a target system but the code does not execute due to the system not being vulnerable (or the system being a honeypot), and "successful exploitation," which occurs when an offender successfully exploits vulnerable code on a target system and is then able to perform additional, unauthorized actions on that system or network.[82] A more comprehensive execution-based analysis requires that these actions be distinguished in a dataset.[83] The security consequences of being able to better estimate a condition of offense-defense fluidity or offense and defense advantage/dominance ought to motivate the construction of such a dataset, as more precision would lead to a better-informed strategy.

The Consequences of Strategic Misalignment

Like offense-defense theory, cyber persistence theory argues that strategic misalignment with the prevailing condition can lead to a crisis and armed conflict through significant strategic losses and increased international tensions. When identifying a source of misalignment, offense-defense theory focuses its gaze on a gap between state's perceptions of the prevailing advantage and the objective

[81] Beyond the top five rows/life cycles, Figures 3 and 5 are not to be compared row-by-row as the survival analyses that informs the list in Figure 4 generates an increased number of permutations. Therefore, the mid-five in Figure 3 represent rows 72–76 of the 148 permutations generated by the opportunity-based analysis, whereas the mid-five in Figure 5 represent rows 92–96 of the 188 permutations generated by the execution-based analyses. The same argument applies to the bottom five rows.
[82] See https://www.cisa.gov/known-exploited-vulnerabilities-catalog.
[83] This is not to suggest that insights cannot be gained from survival analyses of the combination of exploitation in the wild attempts and successes. For example, survival analyses of the combination would give insights on the level of effort being expended by offenders, whether or not that effort leads to successful exploitation.

advantage.[84] Cyber persistence theory identifies a different source of strategic misalignment—failing to recognize that the structural condition designated by cyberspace's core structural features is a condition of fluidity rather than one of advantage. Case studies of U.S.-China and U.S.-Russia cyber interactions between 2010 and 2020 serve as examples of the negative consequences that may follow.

In 2010, then-U.S. Deputy Secretary of Defense Lynn described the prevailing condition in cyberspace as offense dominance, as opposed to offense-defense fluidity, and then-U.S. Secretary of Defense Leon Panetta expressed this view by painting a scenario of a cyber Pearl Harbor, where an aggressor state intent on generating cyber armed-attack equivalent effects would target U.S. critical infrastructure facilities, including chemical, electrical, and water treatment.[85] In reflecting this understanding of a prevailing condition of offense dominance, U.S. cyber security policy centered on defending against and deterring potentially catastrophic cyberattacks.[86]

Despite being targeted by strategically significant adversary cyber campaigns whose effects were short of threats and uses of force from 2010 to 2015, the U.S. adhered to its "doctrine of restraint," even as allowing this adversary activity to go largely unchallenged appeared to embolden and incentivize adversaries to continue experimenting and operating with impunity.[87] This reality of state behavior and interaction in cyberspace by others departed markedly from U.S. views of offense dominance and the model of war, catastrophic attack, coercion, and escalation upon which U.S. cyber strategy and policy was based. This divergence was unquestionably a source of increased tension between the U.S. and its great-power adversaries.

In 2012, years of unbridled Chinese cyber-enabled illicit acquisition of intellectual property (IP) prompted then-Commander of U.S. Cyber Command General Keith Alexander to describe the strategic consequence as the "greatest transfer of wealth in history."[88] U.S. diplomatic efforts in 2012 and 2013 to abate China's IP-theft campaigns resulted in no notable progress, despite the fact that, as then-White House National Security Advisor Thomas Donilon noted, "From the President on down, this has become a key point of concern and discussion with China at all levels of our governments."[89] The tension between the governments was further heightened in May 2014, when the U.S. Department of Justice charged five members of China's military with cyber-enabled illicit IP acquisition for the purpose of

---

[84] Levy, "The Offensive/Defensive Balance of Military Technology, 233.

[85] Secretary Leon Panetta on Cybersecurity, *C-SPAN*, October 11, 2012, https://www.c-span.org/video/?308750-1/secretary-leon-panetta-cybersecurity.

[86] See, for example, U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace, July 2011*, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf and The White House, *International Strategy for Cyberspace, May 2011*, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[87] Regarding a "doctrine of restraint," at the 2013 retirement ceremony of then-Commander, U.S. Cyber Command General Keith Alexander, then-Secretary of Defense Chuck Hagel commented that "DoD will maintain an approach of restraint to any cyber operations outside the U.S. government networks. We are urging other nations to do the same." Garrett M. Graff, "The Man Who Speaks Softly—and Commands a Big Cyber Army," *Wired*, October 13, 2020, https://www.wired.com/story/general-paul-nakasone-cyber-command-nsa/. For policy documents reflecting this doctrine, see U.S. Department of Defense, *The DoD Cyber Strategy, April 2015*, https://nsarchive.gwu.edu/document/21384-document-25 and The White House, *White House Report to Congress on Cyber Deterrence Policy*, https://federalnewsnetwork.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf.

[88] Josh Rogin, "NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History," *Foreign Policy*, July 9, 2012, https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

[89] Thomas Donilon quoted in Eric Chabrow, "U.S. Asks China to Probe, Stop Cyber-Intrusions," *Bankinfosecurity*, March 11, 2013, https://www.govinfosecurity.com/us-asks-china-to-probe-stop-cyber-intrusions-a-5594. Also see Eric Chabrow, "Obama Raises IP Theft with New China Leader," *Bankinfosecurity*, March 14, 2013, https://www.bankinfosecurity.com/obama-raises-ip-theft-new-china-leader-a-5610.

realizing commercial advantage, the first time such charges had been publicly brought against state-sponsored cyber actors.[90] Beijing called the charges "purely fictitious, extremely absurd" and pulled out of cybersecurity talks scheduled for July of that year.[91] In August 2015 it was reported that, as a consequence of continued intransigence on the part of China, the Obama administration was also considering "a package of unprecedented economic sanctions against Chinese companies and individuals" who had benefitted from cyber-enabled theft of U.S. intellectual property.[92]

In August 2016, when then-Central Intelligence Director John Brennan spoke with Alexander Bortnikov, the head of Russia's Federal Security Service, and shared that the U.S. government was aware that Russia had been interfering in the US election process as early as the year before.[93] Brennan further pointed out that Americans would be enraged to find out Moscow was seeking to subvert the election and that there would be a price to pay if Russia continued this information warfare.[94] In September 2016, tensions were further elevated when, during the G-20 summit in Hangzhou, China, President Obama privately confronted President Putin in what a senior White House official described as a "candid" and "blunt" talk. The president informed his aides he had delivered the message he and his advisers had crafted: We know what you're doing, and if you don't cut it out we will impose onerous and unprecedented penalties. One senior U.S. government official briefed on the meeting was told that the president said to Putin, in effect, "You fuck with us over the election, and we'll crash your economy."[95] On December 29, 2015, the Obama administration took a range of economic and diplomatic actions against Russia "in response to the Russian government's aggressive harassment of U.S. officials and cyber operations aimed at the U.S. election."[96] Michael Flynn, the national security advisor-designate for the incoming Trump administration, expressed concern that these actions could lead to an escalatory response by Russia. In a December 29, 2015, call with then-Russian Ambassador Sergey Kislyak, Flynn, anticipating that Russia would respond to U.S. actions regarding "the cyber stuff," urged Kislyak to

---

[90] U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage: First Time Criminal Charges Are Filed Against Known State Actors for Hacking," May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[91] Ellen Nakashima, "Indictment of PLA Hackers Is Part of Broad U.S. Strategy to Curb Chinese Cyberspying," *The Washington Post*, May 22, 2014, https://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html.

[92] Ellen Nakashima, "U.S. Developing Sanctions against China over Cyberthefts," *The Washington Post*, August 30, 2015, https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html. The sanctions would have been based on Executive Order 13694, signed on April 1, 2015. See Federal Register, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 2, 2015, https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities.

[93] David Korn and Michael Isikoff, "Why the Hell are We Standing Down?" *Mother Jones*, March 9, 2018, https://www.motherjones.com/politics/2018/03/why-the-hell-are-we-standing-down/. Russia had allegedly compromised the networks and systems of the Democratic National Committee. For background on that activity, see Eelco Bosch van Rosenthal, "Dutch Intelligence First to Alert U.S. about Russian Hack of Democratic Party," *NOS*, January 25, 2018, https://nos.nl/nieuwsuur/artikel/2213767-dutch-intelligence-first-to-alert-u-s-about-russian-hack-of-democratic-party.

[94] Korn and Isikoff, "Why the Hell Are We Standing Down?"

[95] Ibid.

[96] The actions included sanctioning 11 entities and individuals: the GRU, the FSB, two Russian intelligence services, four individual officers of the GRU, and three companies that provided material support to the GRU's cyber operations. In addition, the Secretary of the Treasury designated two Russian individuals for using cyber-enabled means to cause misappropriation of funds and personal identifying information. In addition, the Department of State shut down two Russian compounds in Maryland and New York used by Russian personnel for intelligence-related purposes, and declared 35 Russian intelligence operatives "persona non grata". The White House, "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment," December 29, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.

"Make it reciprocal. Don't…don't make it…don't go any further than you have to. Because I don't want us to get into something that has to escalate, on a, you know, on a tit for tat."[97]

These two cases highlight two points. First, when a state 's cyber strategy is misaligned with the cyber systemic condition of offense-defense fluidity, the state's chances of suffering strategic losses increase. During the period of these Chinese and Russian cyber campaigns, U.S. views that the prevailing condition designated by cyberspace's core features was offense dominance produced cyber strategies centered on defense and deterrence, ceding the initiative to adversaries as the U.S. prepared to respond with coercive cyber threats to concerns of catastrophic cyber operations.[98] These strategic approaches were largely ineffective against Chinese and Russian non-coercive and non-destructive cyber campaigns whose cumulative effects resulted in U.S. strategic losses. Second, "winning too much" through campaigns short of threats and uses of force in and through cyberspace, either because your opponent fails to recognize the prevailing condition of offense-defense fluidity or because they are unable to successfully execute a strategy that is aligned with that condition, may increase the likelihood of igniting a crisis. States that are subject to strategic losses resulting from such cyber campaigns may, as a result of elevated tensions, conclude that escalation using non-cyber military capabilities and/or other instruments of national power is their best recourse for returning the international distribution of power to its prior state. Cyber persistence theory argues that if states align correctly to the initiative persistent nature of cyberspace, the likelihood of strategic losses decreases appreciably and an unstable cross-domain escalation dynamic is replaced with a stabilizing agreed-competition dynamic.[99]

The 2018 U.S. National Cyber Strategy marks a notable shift in cyber threat assessment and, arguably, a recognition that cyberspace designates a condition of offense-defense fluidity. It argues that "that the United States is engaged in a continuous competition against strategic adversaries … [who] use cyber tools to undermine our economy and democracy, steal our intellectual property, and sow discord in our democratic processes" and concludes that these "[n]ew threats and a new era of strategic competition demand a new cyber strategy that responds to new realities."[100] This assessment is consistent with the U.S. 2017 National Security Strategy, which notes that "adversaries and competitors became adept at operating below the threshold of open military conflict and at the edges of international law" thus requiring the U.S. to "rethink the policies of the past two decades" and develop "new operational concepts and capabilities to win without assured dominance in air, maritime, land, space, and cyberspace domains, including against those operating below the level of conventional military conflict."[101] DoD's 2018 defend forward cyber strategy took up the call for change, arguing that, in addition to deterring significant cyber events, it is necessary to "persistently contest malicious cyber activity in day-to-day competition" short of armed conflict.[102] The central mechanism for this change is described in U.S. Cyber Command's 2018 *Command Vision*: persistence in seizing and maintaining the initiative in and through cyberspace based on new cyber operational concepts of anticipatory resilience,

[97] Eric Tucker, "Read the Transcripts of Michael Flynn's Calls with Russian Diplomat," *PBS*, May 29, 2020, https://www.pbs.org/newshour/politics/read-the-transcripts-of-michael-flynns-calls-with-russian-diplomat.
[98] Schelling notes that deterrence "often depends on getting into a position where the initiative is up to the enemy …" Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1995), 44.
[99] Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*, 48.
[100] The White House, *National Cyber Strategy of the United States of America,* September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[101] The White House, *National Security Strategy of the United States of America,* November 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
[102] U.S. Department of Defense, *Summary: Department of Defense Cyber Strategy, 2018.*

defend forward, and contest.[103] The assessment behind this strategic prescription also appears in the *Command Vision*: "Cyberspace is a fluid environment of constant contact and shifting terrain," or, to be more analytically precise, core structural features of cyberspace designate a condition of offense-defense fluidity.[104] This substantive pivot is explained by the logic of cyber persistence theory; it is not explained by the assumptions of offense-defense theory. The pivot has been further advanced in the March 2023 U.S. *National Cybersecurity Strategy* with its emphasis on connecting disruption campaigns with defense and resiliency outcomes and with the DoD 2023 cyber strategy update.[105]

New Areas of Study

Policymakers have implemented numerous policies over the past couple of years that are consistent with cyber persistence theory's strategic prescription of initiative persistence though exploitation, so they should be encouraged by our empirical support for the theory's claim that core features of cyberspace designate a condition of offense-defense fluidity Scholars should reflect on this finding, as it suggests that research efforts ought to be directed away from offense-defense theory in the cyber context and toward a better understanding of cyber persistence theory, its claims of condition of offense-defense fluidity, and its strategic prescription. For example, the cyber community would benefit from greater understandings of the relationship between an enduring systemic imbalance in initiative persistence and stability/instability between states, the consequences of offense-defense fluidity for cyber strategic windows of opportunity, and whether an enduring imbalance increases or decreases incentives to engage in explicit negotiations.[106] While these research questions are similar to many studied by offense-defense theorists, the central mechanism being researched differs. Additionally, novel questions that flow from micro-vulnerability/macro-resilience and mutability should come to the fore. As many cyber vulnerabilities and remediation actions can be associated with specific cyber technology developers, studies on the relative impact of developers on the condition of offense-defense fluidity could provide key security insights that inform strategy.[107] Additionally, the application of survival analyses to vulnerability life cycles could provide insights into how much security the U.S. Cybersecurity and Infrastructure Security Agency generates by posting alerts and advisories. Further, the dynamic character of the condition of offense-defense fluidity suggests that it has an attribute of velocity—that is, a measure of the speed and direction of the prevailing condition toward or away from the ideal-type milestone sequences that favor offenders and defenders. Further research considering how artificial intelligence tools may impact the velocity of remediation and exploitation in the wild could provide key security insights for strategy.

---

[103] U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority*, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

[104] Ibid, 4. Cyber persistence theory also argues that cyberspace's core structural feature of interconnectedness designates a second condition of constant contact. When considered in tandem, offense-defense fluidity and constant contact prescribe a strategic approach of initiative persistence through exploitation.

[105] See The White House, *National Cybersecurity Strategy, March 2023*, and U.S. Department of Defense, Fact Sheet: *2023 DoD Cyber Strategy*, https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF.

[106] Consider, for example, the hypothesis that strategic windows of opportunity are likely far more frequent but fleeting as a consequence of the fluid character of cyberspace's initiative persistence condition than they are as a consequence of the less dynamic conventional capabilities' offense-defense condition. See Richard Ned Lebow, "Windows of Opportunity: Do States Jump Through Them?" *International Security* 9, no. 1 (Summer 1984): 147–186, https://www.jstor.org/stable/2538638.

[107] For example, research could ascertain which technology developers (and products) tend to introduce relatively more vulnerabilities into the cyber ecosystem and developers' relative times for supporting remediation once a vulnerability is discovered. For an example of such research, see *Prioritization to Prediction, Volume 7: Establishing Defender Advantage* (Cyentia Institute, 2021).

Conclusion

Many policymakers and scholars have referenced, applied, or considered offense-defense theory in the context of cyberspace. Some have argued that a dyadic but not systemic condition of offense-defense balance can be measured, and alternatively, others have argued that no measure, systemic or dyadic, is possible. Those who argue that cyberspace designates an offense or defense advantage implicate, directly and indirectly, characteristics of cyberspace that are core structural features: micro-vulnerability/macro-resilience and mutability. Cyber persistence theory argues that these structural features designate a condition of offense-defense fluidity, not a condition of offense or defense advantage. We treated these competing perspectives as hypotheses and tested them empirically through a proof-of-concept centered on vulnerability life-cycles analyses.

Vulnerability life cycles, and the technological actions they comprise, are sub-systemic indicators of cyberspace's systemic offense-defense condition. Analyses of life-cycle data from 2019 found little support for the hypothesis that micro-vulnerability/macro-resilience and mutability designate a condition of offense or defense advantage. Conversely, strong support was found for the hypothesis of offense-defense fluidity. Additionally, a consideration of the latency in life cycles between a defender's and offender's initial opportunities to seize and sustain the initiative and actually doing so suggested that two measures of offense-defense fluidity be considered -- one opportunity-based and another execution-based, although not all data required for generating the latter are currently being systemically gathered. Nonetheless, analyses of the data on hand strongly supported cyber persistence theory's claim of offense-defense fluidity, whereas offense-defense theory's claim of advantage found little support. There are numerous ways in which this proof-of-concept can be improved upon, including increasing the pool of source data and scope and scale of the analysis. Expanding the size of the CVE sample beyond one year and increasing the number of sources of data for several of the milestones could increase, or potentially decrease, confidence in the claim that the systemic condition designated by cyberspace's core structural features is offense-defense fluidity.

Similar to claims made by offense-defense theorists focusing on conventional capabilities, cyber persistence theory posits that strategic misalignment with the condition designated by cyberspace's core structural features increases the likelihood of strategic losses and may raise international tensions. Two case studies and a brief review of U.S. cyber strategy over the last decade reveal failure and then learning in this regard and highlight the risks that failure poses for suffering strategic losses and escalating into crisis or armed conflict.

It is our hope that empirical support for cyber persistence theory's claim of offense-defense fluidity will inspire additional confidence in policymakers and encourage cyber scholars to investigate long-standing questions, such as the significance of windows of opportunity, from the perspective of offense-defense fluidity and address new questions, such as the relative impact of technology developers on the condition of offense-defense fluidity and the concept of offense-defense velocity.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-06-23	Non-Standard	

4. TITLE AND SUBTITLE

Fluidity, not Advantage, Conditions Cyberspace Security: An Alternative to Offense-Defense Theory

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)

Michael P. Fischerkeller, Jay Jacobs

5d. PROJECT NUMBER

C5239

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES

Institute for Defense Analyses
730 East Glebe Road
Alexandria, VA 22305

8. PERFORMING ORGANIZATION REPORT NUMBER

NS D-33534

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
730 East Glebe Road, Alexandria, VA 22305

10. SPONSOR'S / MONITOR'S ACRONYM

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

Cyberspace scholars and policymakers claim that cyberspace is offense dominant, offense advantaged, and defense advantaged. Further, they claim that an offense-defense condition can be measured only dyadically vice systemically and, alternatively, that it cannot be measured at all. These claims, based on numerous approaches to assessing an offense-defense condition, are all dubious. In fact, core structural features of the technologies that cyberspace comprises designate a measurable systemic condition—one that, using the offense-defense taxonomy, is aptly named offense-defense fluidity. Further, this condition prescribes a cyber strategy of initiative persistence, which, in turn, argues for reformulating offense-defense theory as applied to cyberspace to reflect the strategic realities of the same. Importantly, reformulation does not undermine for cyberspace the core propositions of "properly specified" offense-defense theory that a core structural feature of the prevailing pool of technologies available to states designates a condition that impacts the efficacy of a state's security strategy, that perceptions of the prevailing condition influence states' foreign policies, and that misperceptions can lead to strategic losses and/or increased international tensions.

15. SUBJECT TERMS

Cyber strategy, cyberspace, offense-defense theory

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	23	19b. TELEPHONE NUMBER (Include Area Code)