The Failure of Offense/Defense Balance in Cyber Security

Dr. Brandon Valeriano

ABSTRACT

The idea of offensive advantage dominates the cyber security field, a framework originating from research on the offense/defense balance in conventional warfare. The basic theory is that the balance of offensive and defensive forces determines what kind of strategy will be most effective. The field of cyber security consistently tries to build on offense/defense balance frameworks with little awareness of the inherent problems of the theory. If the offense is dominant, then the defense would supposedly never win against an aggressive adversary due to the compounding nature of failure. The only solution would be going on the offensive in return. This article identifies three core problems with applying the offensive/defensive balance to cyberspace: (1) the inability to distinguish between the two frames, (2) the failure to understand the impact of perceptions, and (3) the inaccuracy of measurement. The pathology of offensive advantage and being under siege as a defender can only continue to lead to strategic malaise and constant attacks as the defender fails to shore up vulnerabilities due to the mistaken belief in the ascendancy of the offense.

DOES THE CYBER OFFENSE HAVE THE ADVANTAGE?

There is a simple conjecture that is quite common in all aspects of society: the best defense is a good offense. The idea, offered by no less a luminary than George Washington in a letter to John Trumbull, shapes how many think about engaging any adversary. Washington wrote, “It is unfortunate when men cannot, or will not, see danger at a distance [France]...not less difficult is it to make them believe, that offensive

Brandon Valeriano is a senior fellow at the Cato Institute and a distinguished senior fellow at the Marine Corps University and served as senior advisor for the Cyberspace Solarium Commission. Valeriano has published six books and dozens of articles for such outlets as the *Journal of Politics, International Studies Quarterly*, and the *Journal of Peace Research.* His two most recent books are *Cyber War versus Cyber Reality* (2015) and *Cyber Strategy* (2018), both with Oxford University Press. Valeriano has written opinion and popular media pieces for such outlets as the *The Washington Post*, *Slate, Foreign Affairs,* and *Lawfare.* His ongoing research explores conflict escalation, big data in cybersecurity, the cyber behavior of revisionist actors, and repression in cyberspace. Valeriano has a PhD from Vanderbilt University. drbvaler@gmail.com

operations, often times, is the surest, if not the only (in some cases) means of defense."[1]

The basic premise of the idea is historically and theoretically wrong. The US would clearly not have benefited from an offensive war against France in 1799 when the new nation were barely able to handle the Barbary pirate nations a few years later. The perceived utility of the offense persists and promotes the belief that action can trump protection in cyber security because of its simplicity and the general failure in the field to evaluate claims with evidence. Avoiding prudence and restraint in favor of offensive superiority is a notion that continues to pollute the discourse.

The ideal of offensive advantage dominates the cybersecurity field, carried over from research on the offense/defense balance (hereafter the O/D balance) in warfare. [2] The basic framework offered by Lynn-Jones is that "there is an offense-defense balance that determines the relative efficacy of offensive and defensive security strategies."[3] Ever since visions of *Wargames* (1982) and thermonuclear war launched by out-of-control computers entered the imagination, conventional wisdom quickly called for offensive action against emergent technological threats.

For some, technology and computers are so vague and unknown that what becomes conventional wisdom often lacks basic logic. Strategists believe cybersecurity is offense-dominant, attacking first and sorting out the damage later becomes the guiding star for cyber strategy. Understanding exactly what the cyber offense is would be helpful; the basics would be a focus on attack and maneuver. There is an idea of going forward and operating outside of one's networks to deny options to the adversary. The defense is simple to explain in this context. It is about protections and ensuring the homeland infrastructure is secure to prevent the worse abuses of cyberspace.

The benefit of prioritizing offense in cyber operations is a critical question. Belief in the utility of aggression is dangerous; it is also likely a reaction to the threat inflation pervasive in the discourse. Employees of the US government are fond of saying that they are taking fire from all sides in cyber operations. This pathology of offensive advantage and being under siege as a defender, reinforced by patterns promoted by the media and the Twitter discourse of constant cyber barrage, can only continue to lead to strategic malaise and constant attacks as the defender fails to shore up vulnerabilities due to the mistaken belief in the ascendancy of the offense.

In this article, I review the foundations of the dominant idea of cybersecurity offense being the best defense. I demonstrate the flawed logic of this framework and push for ideas that break the limits of it. Why does the community waste its time with a research program the security studies field already discarded?

FAILURE OF AN IDEA: THE OFFENSE/DEFENSE BALANCE

Origins and Failure of an Idea

The basic premise of the O/D balance is that “when defense has the advantage over offense major war can be avoided.” This simple conjecture has created a field of research that seeks to unlock the mysteries behind war and peace by focusing on the nature of operations and perceptions of advantage.[4] That so many gravitate to the O/D balance in cyberspace demonstrates a failure to understand the history of the discipline and the lessons learned by those who came before. While research on the O/D balance exploded in the 1980s and 1990s, mainly due to early work by Snyder and Van Evera, it was on life support by the time Van Evera’s book *Causes of War* appeared in 1999.[5] Proposing a solution to the problem of war and peace, instead the literature became confused over how to measure the phenomenon and even what the central variables were. Van Evera (1999) laid out five hypotheses ranging from false optimism for creating the conditions for war to war being likely when conquest is easy. The paradigm stuttered and moved toward different versions of realism that were more parsimonious and not based on subjective perceptions of offensive power.

A theorist's belief that offense is best is, at best, an outcome after the fact and, at worst, an outcome dependent on rational perceptions of the O/D balance. The ideal of the O/D balance, even if accepted that it is empirically accurate and measurable, is both doubtful and fails to motivate action clearly. States assuming a systemic offensive advantage might be deluded in their perspective, as happened during World War I, or they will go on the offense anyway due to the power of other motivating variables, such as a desire for a territorial claim.[6]

Levy notes that “the concept of the offense/defense balance is too vague and encompassing to be useful for theoretical analysis.”[7] Three core problems emerged on top of the issue of uncontrollable outcomes not being impacted by post hoc reasoning. The first is that offense and defense are indistinguishable, or at least an observer cannot tell which is which. The second problem is that the foundation of theory is based on the rational perception that there must be an advantage to offense or defense, either dyadically or systemically. This is based on the premise that leaders will make optimal choices. The final issue is how to measure the factor of offense/defense empirically.

The Cyber Balance

A misguided focus on the balance between offensive and defensive operations clouds understandings of cyber strategy and forces practitioners toward language that does not describe the nature of cyber operations. It is nearly impossible to distinguish cyber actions between offense and defense and even more so difficult to measure said actions. To assume that the balance between offense and defense can be accurately measured and perceived by leaders requires the theorists to comport themselves into so many leaps of logic that the mental gymnastics become impossible.

The developing field of cybersecurity quickly gravitated toward examining the O/D balance in cyber interactions due to the simplicity of the framework. For Healey (2021), it is not important to understand who has the advantage, but under what conditions the framework operates. Such a view presumes that there is an advantage in the first place and that perceptions of the adversary can be known.

The field of cyber conflict continues to build on early ideas by some such as Buchanan (2016), who noted that the offense is ascendant over the defense. Fischerkeller and Harknett have advocated for the strategic doctrine of cyber persistence because the enemy is persistent and the only way to counteract an adversary's offensive cyber actions is to take even earlier offensive action.[8] Healey notes, "Since the beginnings of the internet, the offense often has *seemed to* have the advantage over the defense."[9]

Unfortunately, there is no evidence that the offense has an advantage or that it is the best course of action in cybersecurity. Some arguments for offense dominance are based on the ubiquity of certain systems and companies, like Microsoft.[10] Since the Internet was never built for security in the first place, it stands to reason that it must then be largely insecure. Healey notes that defensive failures cascade and proper targeting can lead to offensive advantages.[11] The defense supposedly can never win against such adversaries due to their power and reach, the compounding nature of failure, and the specific difficulty of protecting all systems from known and unknown vulnerabilities.

The marketplace of ideas does provide alternative frameworks. Early research on all known cyber interactions demonstrates restraint rather than uncontrollable aggression in cyberspace.[12] In fact, escalation is rare[13] and retaliation nearly non-existent.[14] Early on, Gartzke and Lindsay noted the importance of deception in cyber operations, a form of defense mostly.[15] Slayton notes that the balance between defense and offense is conditional on organizational processes and the cost of the bureaucracy, not the raw impulses of the aggressive actor.[16] The remainder of this article examines three core flaws in theory of the O/D balance as it relates to cybersecurity.

DISTINGUISHING INDISTINGUISHABILITY

The key challenge for the issue of an offense/defense balance, or even simple discussions of the offense or defense in cyberspace, is that it is nearly impossible to distinguish between the two. How do you tell which is which? The fluidity of the concept of offense or defense makes the terms virtually useless, since it is near impossible to operationalize, the terms making the research imprecise. Moves that are said to be defensive involve forward maneuver that can seem offensive in nature. Offensive operations set to impose costs on the opposition are often thought to be defensive in nature, for example, indictments or sanctions against digital aggressors.

Terms on shaky definitional grounding are prone to conceptual stretching. The term "conceptual stretching" was originally coined by Sartori, who connected the idea to the distortion that comes when a concept does not fit new cases.[17] This factor is at play often in cybersecurity where new cases confound observers. Does the US rerouting of server traffic for a ransomware group count as an offensive or defensive operation?[18] Certainly, the operation is proactive and involves foreign network space, but the operation is also not destructive or violent and represents a move to protect the American homeland from ransomware attacks on civilian targets that seemingly plagued the US during the pandemic.

Ideas that defy basic categorization are prone to confirmation bias and the assumption that the measurement is correct when the term itself defies basic measurement. The "offense" and "defense" are terms that are difficult to operationalize. What exactly is an offensive and defensive operation in cyberspace? The problem is any desire to operationalize a difference between offensive and defensive operations is based on an artificial division of the problem. It is not a problem of being precise, but rather distinction. Much like the Dutch ideal of "total football," the best defenders are also the best attackers.[19] They know the weak spots and where to look for vulnerabilities; just as the best attackers are also the best defenders since they know the attack surface so well and can pinpoint weaknesses. The strategic logic between the distinction is empty, yet there is a logic to force allocation and structure that might require a division between defensive and offensive forces, a distinction that remains artificial.

Cyber confusion pervades discussions of the offense and defense. Is a zero-day vulnerability (an unknown flaw) an offensive weapon? Some might suggest any unknown vulnerability can be exploited by the attacker. Yet it is just as likely that basic probes or vulnerability research on other targets will uncover the unknown vulnerability, and allow the defender to become stronger once the weakness is patched. An unknown vulnerability can be both defensive and offensive at the same time, making the idea of distinguishing between the two frames nearly impossible.

What of national cyber forces such as the Cyber Mission Force in the U.S. Cyber Command (USCYBERCOM) or the National Cyber Force in the UK? While these forces can go on the attack against other nation-states, they also can be posted as defensive operators seeking to stop attacks before they happen. The reality is that the active and adaptive nature of modern technology makes the idea of distinction between offense and defense entirely empty, resulting in the basic research question being almost meaningless.

PERCEPTIONS

A key foundation of the offense/defense balance is that perceptions will be optimal. One side will perceive either the offense or defense as having the advantage determining the probability for war. Yet, as critics have pointed out, “It is inherently difficult to assess the impact of weapons technologies, particularly when they have not been employed in war.”[20]

Glaser and Kaufmann note that versions of realism need to introduce a variable that converts power into military capabilities for the theory to be operational.[21] This becomes a key condition to provide a mechanism for how the process of an O/D balance must work to influence the dependent variable, taking territory or winning wars. The remaining question is whether the perceptions of how technology creates military capability accurate?[22] How does a state decide if one is operating in an offensive- or defensive-dominant situation?

Views of cyber power and an emphasis on offensive dominance are really in the eye of the beholder. There is no standardized method of measuring cyber power. In a 2018 book, Valeriano et al. developed a measure of latent cyber capacity measuring digital infrastructure and knowledge capital (engineering graduates and patents).[23] South Korea came out ahead of the US, China, Japan, and Israel, in that order. Clarke and Knake list a ranking of the US, Russia, China, Iran, and North Korea.[24] The Belfer Center National Cyber Power Index of 2020 ranks the US, China, and the UK (a new entry) as the top-three due to the inclusion of a variable for intent, which is coded subjectively based on readings of documents.[25]

For cyber security, converting cyber power into military capabilities is a fraught enterprise. There is little evidence that cyber power is coercive, on either the diplomatic or military battlefield. Kostyuk and Zhukov note there is no impact from cyber capabilities on the battlefield in Ukraine, a finding which appears to be holding strongly during the Ukraine War that began in 2022.[26] In a macro study, Valeriano et al. find little evidence of a coercive impact on international relations, with most cyber events failing to change the behavior of the target.[27] When the target’s behavior changes, it is often as a defensive maneuver to prevent future incursions. If the central mechanism of the O/D balance is the fact of coercive change through technology, cyber options play little role in this process.

The problem is that, for some, cybersecurity is revolutionary, yet there is no evidence that cyber operations affect the battlefield.[28] There are assumptions of a Battlestar Galactica (2004) effect in which the opposition shuts down all weapons and communications making the target’s defenses inoperable to the point of fantasy. This perception of effectiveness, disconnected from the empirical reality of the impact on operations, demonstrates the pervasive power and inapplicability of O/D balance theory to cyberspace. In a domain that operates mostly without empirical evidence, anyone can perceive whatever he/she chooses, often based on fictions, yet the reality is often much different.

The idea that a state's perception of the O/D balance can be accurately known by the opposition is betrayed by the inability of the aggressor even to understand its operations and to optimize their security. That many misperceived the power of the offense on the eve of World War I should suggest that the theory is on shaky ground from the start.[29] Even proponents note "this also means that when states do engage in suboptimal behavior, our ability to determine the offense-defense balance by observing military policies and war outcomes is greatly reduced."[30] Lynn-Jones argues that states which fail to accurately assess the arena and "adopt offensive strategies in a world of a defensive advantage will be punished by the system."[31]

The history of cyber security is a history of suboptimal security behavior since the domain was never developed with security in mind. Of course the policy failures have been constant.[32] Debate over whether the offense or defense has the advantage in cyberspace will never be resolved satisfactorily because security was an afterthought in the creation of the Internet. Hence, one must wonder just how critical the research question is when there are no accurate answers offered.

MEASUREMENT

The water's end for O/D balance is that it is simply impossible to measure the success or failure of the theory given the conditions laid out by its proponents. As Lynn-Jones notes, "The empirical rejection of the framework, plus the more complicated question of just how to measure what an offensive weapon is versus a defensive weapon, and the examined question of how to measure perceptions of these weapons, makes this framework problematic."[33] In examining the efficacy of the theory statistically, Gortzak and Haftel find little empirical support for any of the theoretical propositions.[34]

Absent of measurement, scholars and policymakers are making predictions that can never be falsified. In short, we can never know if one is wrong, or right. In their effort to save the theory of O/D balance in light of penetrating criticisms, Glaser and Kaufmann counter the idea that the theory cannot be measured "as simply incorrect."[35] They note "that the offensive-defensive balance should be defined as the ratio of the cost of the forces that the attacker requires to take territory to the cost of the defender's forces." A line in the sand clearly drawn by scholars, but this point is also degenerative from the earlier grand positions of the O/D balance as the key factor in explaining war and peace.[36]

The reformation of O/D balance as simply the ratio of costs for the attacker versus the costs to defend territory is inoperable for cyber security for one simple reason: there is no territory to take. In its simplest form, cybersecurity is about maintaining networks and protections to ensure that systems operate. One can knock out a system, distract the opponent, or confuse a target but the opposition will always recover at some point. There is rarely a conception of destruction in cyberspace and, although some materials can be destroyed, they can also be quickly restored.[37] While some might use the language of maneuver and gaining ground in cyberspace, there is no ground to take.[38]

The challenge of distinction then returns: how would one measure the costs to defend versus the costs to attack? Glaser and Kaufmann dismiss all these challenges to suggest that "ballpark estimates of the balance may be sufficient," demonstrating how shaky the premise is in operation.[39] Healey supports this notion by writing, "Exact measurements may be difficult but fortunately are not needed, as the scale and magnitude of the trends should be enough to determine the relative advantage over time between offense and defense."[40]

While it might be simple to classify the O/D balance in the abstract, would one classify USCYBERCOM as offensive and the Department of Homeland Security (DHS) as defensive? Failures at such simple distinctions reveal the fluidity of computer network operations and the pace at which bureaucratic organizations operate and share talent. There is also the compound issue of how to measure the cost of a bureaucracy. Operation costs vary by year and often fail to factor in the costs of training and education outside the network security realm. In short, time and the nature of organization matter a great deal in cyber security when considering the measurement of the O/D balance.[41]

While it is difficult to measure O/D balance in any formation based on a dyadic notion of contestation between two entities, it is even more difficult to measure O/D balance in its wider systemic sense. In short, how to do we classify eras exactly? The issue of perceptions returns. How would one know if a set of years under examination is offensive-dominant, especially in light of any objective means of assessment of cyber security operations?[42] Regardless of the academic debates on the nature of the O/D balance, the uncertainty that results from the discussion regarding measurement should give anyone pause in the belief that cyber operations can be classified as offensive or defensive.

FUTURE TASKS

Questions that lack a theoretical grounding or a method of empirical observation to adjudicate outcomes inevitably lead down degenerative pathways, a problem that often pervades the cybersecurity literature. Assuming that there is a distinction between offense and defense ignores the fact that, in practice, the two are impossible to distinguish. Because there is no distinction between the two in practice means that it is impossible to measure the success or failure, which makes the theory indeterminate. Sometimes one must reject the basic premise of a research question if it does not help one understand an issue or provide solutions.

The lessons extracted from this article are very simple. The stopping point for applying O/D balance theory to cyber operations is that it is impossible to distinguish the attack from the defense in cyber security. Effective operationalization of theory is the key consideration. The inability to create a definition that clearly categorizes the two supposed sides of military operations suggests the theory is unworkable in cyber security. It is not that cyber security cannot be measured and operationalized, but that doing so must be done carefully and should be scientifically valid.[43]

There are times when dividing between the offense and defense does make sense. To properly allocate forces, it sometimes becomes necessary to group forces into offense and defense. It might be critical bureaucratically to distinguish between the two sides of offensive and defensive forces, yet this practice is also artificial and often restrains the career paths of defensive operators.

Conflict is a continuum. States build toward conflict; little actions taken can add up and interact with big factors such as territoriality to produce warfare. Distinguishing between offensive and defensive eras has no impact on these actions that lead to war, but it might be able to highlight when a war might occur. This is an interesting proposition but one that requires an accurate reading of perceptions in the domain and the shape of the balance, a near impossibility in cybersecurity.

The premise of O/D balance theory provides poor policy advice, and sometimes leads policymakers to propose offensive operations when these operations might be unsuited for the domain or, worse, ineffective. Ignoring efforts to establish resilience is a certain condition toward instability and further conflict. The reality is that O/D balance theory is troubling because it minimizes the need for defense and focuses on the magic bullet of emergent technology. While some might argue that we have failed to establish effective defense for cyber operations, the reality is that states have rarely tried to do the defense correctly due to bureaucratic issues, money, lack of knowledge, or the pull of the offense. The misapplied and dangerous conjecture that the best defense is a good offense must end. The best defense is a real defense.

NOTES

1. G. Washington, 1799, From George Washington to John Trumbul, June 25, 1799, J. Trumbul, Mount Vernon.
2. J.S. Levy, 1984, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis," *International Studies Quarterly* 28(2): 219-238; G.H. Quester, "Offense and Defense in the International System," Transaction Publishers, 2002.
3. S.M. Lynn-Jones, 1995, "Offense-defense theory and its critics," *Security Studies* 4(4): 660-691.
4. C.L. Glaser and C. Kaufmann, 1998, "What Is the Offense-Defense Balance and Can We Measure It?" *International Security* 22(4): 44-82.
5. J. Snyder, 1984, "Civil-Military Relations and the Cult of the Offensive, 1914 and 1984," *International Security* 9(1): 108-146; S. Van Evera, 1984, "The Cult of the Offensive and the Origins of the First World War," *International Security* 9(1): 58-107.
6. Levy, 1984, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis;"P.R. Hensel and S.M. Mitchell (2017), "From territorial claims to identity claims: The Issue Correlates of War (ICOW) Project," *Conflict Management and Peace Science* 34(2): 126-140.
7. Levy, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis."
8. M.P. Fischerkeller and R. J. Harknett, 2017, "Deterrence is not a credible strategy for cyberspace," *Orbis,* 61(3): 381-393, M.P. Fischerkeller and R.J. Harknett, 2019, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *The Cyber Defense Review*: 267-287.
9. J. Healey, 2021, "Understanding the Offense's Systemwide Advantage in Cyberspace," *Lawfare.*
10. D. Geer, R. Bace, P. Gutmann, and P. Metzger (2007), "Cyberinsecurity: The cost of monopoly."
11. Healey, "Understanding the Offense's Systemide Advantage in Cyberspace."
12. B. Valeriano and R.C. Maness, 2015, Cyber War versus Cyber Realities: Cyber Conflict in the International System, New York, Oxford University Press.
13. B. Valeriano, B.M. Jensen, and R.C. Maness, 2018, Cyber Strategy: The Evolving Character of Power and Coercion, New York, Oxford University Press; S. Kreps and J. Schneider, 2019, "Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics," *Journal of Cybersecurity* 5(1): tyz007; B. Valeriano and B. Jensen, 2021, De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War in "Cyber Peace: Charting a Path Towards a Sustainable, Stable, and Secure Cyberspace. S. Shackelford, F. Douzet, and C. Ankersen (Eds), Cambridge University Press, Forthcoming.
14. B. Valeriano and B. Jensen, 2019, "The Myth of the Cyber Offense: The Case for Cyber Restraint," Cato Institute, *Policy Analysis* (862).
15. E. Gartzke and J.R. Lindsay, 2015, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24(2): 316-348.
16. R. Slayton, 2017, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41(3): 72-109.
17. G. Sartori, 1970, "Concept Misformation in Comparative Politics," *American Political Science Review* 64(4): 1033-1053.
18. E. Nakashima and D. Bennett, 2021, A ransomware gang shut down after Cybercom hijacked its site and it discovered it had been hacked. *The Washington Post*.
19. R. Jensen 2014, "Looking at the extraordinary success of the 'Clockwork Orange': examining the brilliance of total football played by the Netherlands," *Soccer & Society* 15(5): 720-731.
20. S.M. Lynn-Jones, 1995, "Offense-defense theory and its critics." *Security Studies* 4(4): 660-691.
21. Glaser and C. Kaufmann, "What is the offense-defense balance and Can We Measure It?"
22. C. Smythe, 2020, "Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance." *Yale Journal of International Affairs*, 15: 98.
23. Valeriano, Jensen, and Maness, Cyber Strategy: The Evolving Character of Power and Coercion.
24. R. Clarke and R. Knake, 2014). "Cyber war," Tantor Media, Incorporated Old Saybrook.
25. J. Voo, I. Hemani, S. Jones, W. DeSombre, and A. Schwarzenbach, 2020, Reconceptualizing Cyber Power, Belfer Center, Harvard University.
26. N. Kostyuk and Y.M. Zhukov, 2019, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63(2): 317-347.

NOTES

27. Valeriano, Jensen, and Maness, "Cyber Strategy: The Evolving Character of Power and Coercion."
28. L. Kello, 2013, "The Meaning of the Cyber Revolution: Perils to theory and statecraft," *International Security* 38(2): 7-40.
29. Levy, "The offensive/defensive balance of military technology: A theoretical and historical analysis," 219-238.
30. Glaser and Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" 44-82.
31. Lynn-Jones, "Offense-defense theory and its critics," 680.
32. M. Montgomery, B. Jensen, E. Borghard, J. Costello, V. Cornfeld, C. Simpson, and B. Valeriano (2020), Cyberspace Solarium Commission Report, Washington, D.C.
33. Lynn-Jones, "Offense-defense theory and its critics," 660-691.
34. Y. Gortzak, Y. Haftel, and K. Sweeney, 2005), "Offense-defense theory: An empirical assessment," *Journal of Conflict Resolution*, 49(1): 67-89.

Glaser and Kaufmann, "What Is the Offense-Defense balance and Can We Measure It?" 44-82.

35. J. Vasquez, 1997, "The realist paradigm and degenerative versus progressive research programs: An appraisal of neotraditional research on Waltz's balancing proposition," American Political Science Review 91(4): 899-912; S. Van Evera, 1999, "Causes of War: Power and the Roots of Conflict," Cornell University Press.
37. J. Lindsay, 2013, "Stuxnet and the limits of cyber warfare," *Security Studies,* 22(3): 365-404.
38. S. Applegate, 2012, *The principle of maneuver in cyber operations,* 2012 4th International Conference on Cyber Conflict (CY-CON 2012), IEEE.
39. Glaser and Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" 13.
40. J. Healey, 2021, "Understanding the Offense's Systemic Advantage in Cyberspace," *Lawfare.*
41. T. Stevens, 2016, "Cyber security and the politics of time," Cambridge University Press; R. Slayton, 2017, "What is the cyber offense-defense balance? Conceptions, causes, and assessment," *International Security*, 41(3): 72-109.
42. D. Denning, 2015, "Assessing Cyber War" in "Assessing War: The Challenge of Measuring Success and Failure," L. Blanken, H. Rothstein and J. Lepore, Washington, D.C., Georgetown University Press: 266-284.
43. B. Valeriano and R.C. Maness, 2018, "How we stopped worrying about cyber doom and started collecting data," *Politics and Governance*, 6(2): 49-60.