Strategic Impacts of the Cyber Offense/Defense Balance

Wade Huntley and Timothy Shives
Naval Postgraduate School, Monterey, California, USA

wlhuntle@nps.edu

Abstract. This paper examines how the distribution of offensive and defensive cyber operations (OCO & DCO) contributes to the achievement of strategic goals. Drawing on established theories of the relationship of offensive and defensive weaponry in terrestrial conflict domains, the examination develops a methodological framework to assess the relative contributions of OCO and DCO to offensive and defensive cyber strategies and overall multi-domain outcomes. The paper identifies both challenges and opportunities in associating offensive and defensive cyber capabilities with appropriate offensive and defensive strategies. Some challenges are intrinsic to the dynamic effects of specific weapons technologies on conflict outcomes, while other challenges flow from the conditions of the cyber domain. The paper identifies principal complicating factors in associating OCO and DCO selections with strategic outcomes, including the dual-use and indistinguishable nature of some of the most sophisticated cyber weapons; the opacity of operations incumbent to the cyber domain; complexities and data acquisition impediments in calculating precise relative costs associated with developing and utilizing offensive and defensive cyber capabilities; information paucity exacerbation of motivated analytical biases; and the sometimes inverted relationship of OCO and DCO to offensive and defensive strategies, respectively. These findings support the importance of developing a precise and empirical evaluation methodology associating objectives achievement in the distribution and balance of OCO and DCO missions to the underlying operational and strategic objectives of those missions.

Keywords. Cyber offense, Cyber defense, cyber operations, Cyber warfare, Cyber strategy, DCO, OCO, Multi-Domain warfare, Offense-Defense balance, Offense-Defense advantage, Cyber perishability, Cyber obsolescence

1. Introduction

This paper summarizes a longer report on a project assessing whether offensive or defensive strategies prevail in cyberspace, given evolving technologies, and how variance of outcomes based on the nature of cyber capabilities can be utilized to evaluate appropriate distributions of capabilities in specific cyber missions, broader cyber strategies, and overall multi-domain warfare campaigns.

Despite prevalent views favoring offense dominance, recent skepticism suggests a possible overemphasis on offensive operations. This paper applies offense-defense theory from international relations to enable more precise evaluation of the relationship between offensive and defensive cyber operations. The assessment concludes that any judgement of whether offense or defense "dominates" in cyberspace is overly simplistic, which in turn complicates efforts to trace the appropriate balance of offensive or defensive capabilities in any given context, at the tactical, operational or strategic levels.

The following section provides a brief overview of representative claims regarding offensive advantage. To develop a more rigorous evaluation of such claims, the subsequent sections applies Jervis' (1978) two principal variables of the offense/defense balance – differentiation and advantage – to the cyber domain. The discussion also explores specific features of cyber conflict relevant to the offense-defense relationship, such as secrecy, geography metaphors, the transient nature of military cyber capabilities, and the emerging focus on cognitive influence and control as noted by Noel, et al, (2021) and Hutchinson (2022). The paper concludes by mapping these considerations into a multi-domain warfare, drawing overarching conclusions, and considering implications for further research.

2. Assumptions of Offense Dominance

Until recently, most considerations of appropriate military strategies and policies in the cyber domain took the offensive dominance of the domain as a given. The viewpoint that offense dominates in cyberspace drove concerns over vulnerability to a cataclysmic cyber-attack, i.e. a "Cyber Pearl Harbor" (Panetta, 2012; Arquilla, 2012; Clarke & Knake, 2010). In some analyses the need for significant emphasis on offensive cyber operations has functioned as an asserted fact rather than an operating assumption (Sheldon, 2011; Kello, 2013; US DoD, 2011; US JCS, 2013). Often strategists and decision-makers are unequivocal in taking the position that offense is dominant in the cyber domain (Lynn, 2010; Harknett, Callaghan, and Kauffman, 2010; Sterner, 2010; Masters, 2011; Slayton, 2016/17).

Subsequently, the question became more debated, in the context of skepticism over cyber threats in general being "over-hyped" (Rid, 2012; Brito & Watkins, 2011; Libicki, 2013b). But systematic attention to this question in the framework of pre-existing offense-defense theory was slow to emerge (Saltzman, 2013; Lieber, 2014).

Aucsmith (2012) surveys new features of cyber conflict relevant to both offense and defense. Gartzke and Lindsay highlight the important and independent role of deception in cyber activities, and observe that perceptions of offensive advantage rest on mistaking ease of deception for ease of attack (Gartzke & Lindsay, 2015, p.346). In a sophisticated reconceptualization of offense-defense theory, Slayton concludes that the appearance of cyber offense success traces beyond intrinsic technological advantage, necessitating incorporation of factors such as organizational processes and the values of objectives into understandings of the offensive-defense relationship (Slayton, 2016/7, p.75). Gray (2013) offers important logical challenges to the presumption of offensive advantage in cyberspace. Yet most studies fall short of providing a systematic application of the frameworks and variables of offense-defense theory, leading to confusion with theories of deterrence and coercion, and misapplication of offense-defense theory in analysis and in policymaking (Leatherman, 2024:ch.V).

3. Offense-Defense Theory

Offense-defense theory focuses on the impact of the prevailing systemic "balance" between offensive and defensive military technologies on state behaviour and prospects for interstate conflict. Specifically, "offense-defense theory contends that international conflict and war are more likely when offense has the advantage, while peace and cooperation are more probable when defense has the advantage" (Lynn-Jones, 1995, p.661). In Jervis's original formulation, two variables shape the relationship of offense and defense in any given context: "whether defensive weapons and policies can be distinguished from offensive ones, and whether the defense or the offense has the advantage" in preparations and outcomes (Jervis, 1978, pp.186-87). The following two sub-sections examine each of these two factors, with an eye to those features most illuminative of cyberspace conditions.

3.1 Offense-Defense Differentiation

The capacity to distinguish defensive weapons and policies from offensive ones varies over capabilities, applications, context and time. Jervis (1978, p.199) asserts that if "weapons and policies that protect the state" do not "also provide the capability for attack," then "it is possible for a state to make itself more secure without making others less secure." Thus, the feasibility to differentiate offensive and defensive capabilities is central to offense-defense theory. Many capabilities, including cyber capabilities, can be used either offensively or defensively, and some distinctions are only in the intentions of the possessor. Also, defensive weapons may support offensive strategies, and vice versa. For example, some observers consider the nuclear age to be defense-dominant despite the indefensibility of targets under circumstances of "mutually assured destruction" (Morgan, 2010; Jervis, 1978, p.198; Lynn-Jones, 1995, p.667; cf. Schelling, 1966; Morgan, 2003).

Jervis observes that acquisition of offensive capabilities that are unnecessary for defense can be an early indicator of aggressive intentions (Jervis, 1978, p.199). "If procurement of [offensive] weapons cannot be disguised *and takes a fair amount of time, as it almost always does,* a status quo state will have the time to take countermeasures" (Jervis, 1978, pp.199-200; italics added). The italicized addition here is a key observation because, in the cyber domain, this additional factor of the time taken for procurement, and especially the visibility of procurement, loom large in evaluating distinguishability.

3.2 Offense-Defense Balance

Jervis specifies two "aspects" of the offense-defense balance. The first aspect concerns *costs*: whether procuring a defensive capability costs more or less than the offensive capability it is offsetting. If offensive capabilities are relatively cheaper than defensive, states perceive they can "buy more security" per unit cost with offensive rather than defensive expenditures. But in this circumstance the insecurity such procurements generate for other states leads them to increase their own offensive procurements. This makes it difficult to distinguish aggressive versus reactive acquisition of offensive capabilities, and arms races ensue (Jervis, 1978, p.188; cf. Van Evera, 1998, pp.13-14). Conversely, if defensive capabilities are relatively cheaper, status quo states can obtain security with capabilities less threatening to others, and offensive acquisitions more clearly indicate aggressive intentions, leading eventually to a stable security equilibrium (Jervis, 1978, p.188; cf. Lynn-Jones, 1995, p.665).

The second aspect of the offense-defense balance concerns *operations*: whether it is better in a conflict to be attacking or defending, and in particular whether the advantage accrues to the state that strikes first or the state that allows the adversary to expend the first effort. When offense is advantageous in this sense, fear of surprise attack is palpable, periods of crisis encourage states to act precipitously, and short-run instability reigns (Jervis, 1978, pp.188-89). Conversely, when defense dominates, confidence in defensive capabilities allows states not

to fear surprise attacks, incentives for first strikes are greatly reduced, and conflict situations tend toward self-stabilization.

3.3 Geography

Geography is important to offense-defense theory for two reasons. First, it is the ultimate object of major physical conflict. A primary objective of offense-defense theory has been to understand the relationship between the nature of weapons technologies and the causes and outcomes of major wars. Second, geography also can shape how given weapons technologies translate into either offensive or defensive advantage. Historically, geographic factors have offered both natural defenses and natural vulnerabilities, and the military technologies of a given period have functioned to either enhance or obviate these features (Jervis, 1978, p.194-95. Cf. Van Evera, 1998, p. 19).

The cyber domain present novel challenges in applying both these geographic aspects. First, there is the obvious challenge in translating the fundamental criterion of territorial control into the cyber domain, defined by its largely virtual (non-physical) nature. Second, because the main features of the cyber domain evolve under human agency (albeit at varying rates, and with varying intentions), there are few if any static "natural" features. Rather, newly developed technological capabilities interact synergistically with the evolution of the domain's own "geographic" features.

3.4 Perceptions

In offense-defense theory, the characteristics of prevailing weapons technologies at a given time function as a structural feature, shaping the outcomes of the conflict interactions of states independent of states' intentions. Concurrently, in offense-defense theory, how state decision-makers *perceive* the offense-defense relationship of current military technologies plays a decisive role in determining state *behavior*. In one view, the perception of offense dominance raises the same dangers of actual offense dominance, "even without the reality;" "The actual offense-defense balance has marked effects; the effects of the perceived offense-defense balance are even larger" (Van Evera, 1998, p.6).

Research has identified an array of systematic misperceptions and motivated biases favoring offensive doctrines (Lynn-Jones, 1995, p.677; cf. Sagan, 1994, pp.75-6). World War I is widely considered to classically exemplify both how misperception of the offense-defense balance can decisively influence state behavior and how the material realities of the offense-defense balance can decisively shape the outcomes of war despite contrary beliefs (Lieber, 2007; Snyder, 2008; and Lieber, 2008). The disjuncture between perceptions and reality of offense-defense balance complicates the explanatory function of offense-defense theory (Davis, 1998/99, p.180-81, Goddard, 1998/99, p.191, and Van Evera, 1998/99, p.198-99).

The translation of *actual* offensive-defense advantage into *perceived* offensive-defense advantage is a particularly salient feature in the cyber domain, due to the requisites of secrecy that are incumbent to the domain. Secrecy can contribute to the challenge of differentiating offensive and defensive capabilities, and the broader opacity of capabilities leaves empirical gaps that are easy to fill with assumptions influenced by motivated perceptual biases.

4. Offense and Defense in the Cyber Domain

The more structured framework of offense-defense theory offered in the preceding section can provide a robust foundation to improve understanding of the relationship of offensive and defensive capabilities in cyber military conflict. While not determinative, the framework indicates key elements of cyber conflict that require more detailed specification for a thorough systematic application.

4.1 Cyber Power

The concepts of "offense" and "defense" in the cyber domain stem from understandings of the exercise of *power* in the cyber environment. Conceptualizing cyber power can begin from Hans Morgenthau's famous seminal definition: "Power may comprise anything that establishes and maintains the control of man over man" (Morgenthau, 1948; cf. Leatherman, 2024:42). This appreciation of power a relationship between individuals, groups or societies also spotlights Clausewitz's insight that the application of military force is not an end in itself, but rather that strategy is founded in the use of force as a means to ends defined by political objectives (Howard, 1979).

Drawing on this pedigree, Nye defines *cyber power* as "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain." Nye elaborates that this concept

of cyber power has two aspects: achievement of outcomes *within* cyberspace and achievement of outcomes in domains *outside* cyberspace, recognizing directly that strategic purposes for use of cyber power may be obtain from beyond the cyber realm itself (Nye, 2010, pp.3-4; Ackerman, et al, 2024; Briggs 2023). Capturing the interpersonal centerpiece, analysts have elaborated the functions of such forms of power in the realm of information warfare and hybrid warfare (Saressalo & Huhtinen, 2022; Sheikh, 2022; Ormrod, et al, 2023).

4.2 Offense-Defense Differentiation in the Cyber Domain

At first glance, many specific cyber capabilities seem easily distinguishable. But two complications emerge, one recognized in broader offense-defense framework, the other original to this framework's application in cyberspace.

The first complication is the potential for offensive capabilities to serve defensive functions, and vice versa. Examples of use of offensive capabilities for essentially defensive purposes include use of software to deactivate the client computers of an attacking botnet or to detect the parameters of a potentially threatening malware in order to improve network protections (Demchak, 2012, p.66; cf. Belk & Noyes, 2012). The strategic posture of "persistent engagement" and the operational practice of "defend forward" rely upon the ubiquitous use of a range of cyber capabilities for defined defensive purposes. Conversely, robust protection of the cyber systems may support offensively oriented physical military capabilities (e.g. a naval strike group or a nuclear bomber wing).

The second complication in distinguishing offensive and defensive cyber capabilities, unique to cyberspace, stems from the ease with which offensive cyber capabilities can be kept hidden – and the necessity of doing so. Libicki comments that "offensive cyberwar capabilities must be highly classified to remain effective" (Libicki, 2013a, p.22). Concealment is further encouraged by the limited effectiveness of revealing capabilities to achieve essentially defensive deterrent and stabilizing effects (cf. Libicki, 2013a:2; Libicki, 2009:176). As Jervis' noted earlier, the length of time and transparency of the development of offensive capabilities is a crucial factor in evaluating overall impacts. The development and deployment of much offensive cyber software, however, may be concealed. Even if the capability itself is clearly defensive, ease of concealment undercuts the benefits flowing from offense-defense differentiation. Even if differentiation were generally easy, the benefits of differentiation do not obtain when states' capabilities are hidden.

4.3 Offense-Defense Balance in the Cyber Domain

Applying to the cyber domain the two "aspects" of the offense-defense balance, military costs and operational effectiveness, further specifies the nature of the cyber offense-defense relationship.

Several analysts point to cost variations in evaluating whether offense is advantaged in cyberspace (e.g. Saltzman, 2013; Lieber, 2014). Libicki cites U.S. government expenditures on military network security as one reason for offensive advantage (Libicki, 2009, p.32). Malone's accomplished effort to measure and evaluate offensive and defensive cyber costs supports Libicki's and others' general conclusion that offense is less costly, with a heuristic data analysis model generating a 1:1.32 cost advantage for offensive cyber operations and two case studies evincing 1:4.3 and 1:7 advantages (Malone, 2012). Slayton presents an alternative approach to such data that generates a different outcome (Slayton, 2016/7, esp. pp.97-103). Another assessment finds that, regardless of offensive capabilities, the United States is likely to spend more on defense than offense due to the challenges associated with cyber-deterrence (Sakellariadis 2022).

The necessity to conceal development of cyber capabilities presents formidable obstacles to rigorous assessments of costs for offensive and defensive cyber capabilities. Data obstacles include categorizing costs of capabilities with both offensive and defensive traits; bounding costs that might be spent anyway for non-military cyber purposes; incorporating non-governmental costs; and managing budgetary secrecy (Malone, 2012).

Regarding operational effectiveness, scant experience with higher intensity cyber conflict limits evaluation. Throughout history the operational advantages and disadvantages of technological developments often have not been apparent until major conflicts revealed their interaction with other weapons and strategies under real conditions. Moreover, the dynamic evolution of the cyber environment and of exploitation capabilities within it further undercut the value of past experiences as indicators of future cyber utility. Unpredictability is exacerbated when incorporating cyber effects into broader planning for hybrid warfare and multi-domain conflict, as discussed below.

4.4 Geography of the Cyber Domain

The "malleability" of cyberspace presents distinct features relevant to offense-defense evaluation (Leatherman, 2024: 49). No other domain in human history has presented such a dynamic "terrain." Sufficient definitions of the cyber domain include logical and virtual as well as physical dimensions, as in the depiction of cyberspace as three interactive and equally important "layers" – the physical network, logical network, and cyber-persona (U.S. JCS, 2013). Problematically, taking seriously the virtual and persona layers of cyberspace as power projection platforms questions the utility of geographic metaphors at all.

For example, cyberspace is sometimes referred to as a "borderless" realm (Nye, 2010; Lonsdale, 2009). An alternative image is cyberspace as a *border-rich* realm, in which all entities connect, boundaries can emerge and disintegrate in real time, and "distance" is temporal rather than spatial. Attaching meaning to the notion of "taking" or "holding" such cyberspace less resembles charging a hill on a battlefield than winning "hearts and minds" in populations (Meriläinen, 2023). This perspective spotlights the importance of contemporary attention to cognitive warfare (Noel, et. al., 2021; Hutchinson, 2022; Leatherman, 2024: ch.VI). Cognitive warfare focuses attention on the use of cyber capabilities and information networks to influence and control populations on social, political, and military fronts (Buvarp, 2023; Murphy, 2023; Hiltunen & Huhtinen, 2022). Resonant of Morgenthau's definition of power, the "key terrain" in cognitive warfare may consist mainly of ideas, identity affinities, and pivotal civilian communities, rather than routers and undersea cables.

In this imagination of cyber "geography," the questions of offense or defense advantage in the cyber domain are harder to frame. Yet such an effort is essential in the era of information warfare and persistent engagement, given tangible instances of information operations and cognitive warfare, the recent conflicts in Ukraine, and the rising threats in Southeast Asia (Leatherman, 2024; Goldman & Monarez, 2021; Clarke, et al, 2023; Lehto, 2023; Van Niekerk, 2023).

Thus, the concept of geography can be highly suggestive but also obstructive in exploring the roles of offense and defense in cyber conflict. Rather, in cyberspace, the penetrability of boundaries is not by itself an indication of offensive advantage. It may matter more how physical force postures remain resilient and robust (Demchak, 2012), and whether one prevails in the overall outcomes of persistent engagement (Fischerkeller, et. al., 2022).

5. Cyber Operations in Multi-Domain conflict

The propensity of material wars to include cyber components is now empirically established. But cyber capabilities do not present the same kind of war-deciding qualities that other new military technologies have presented (Libicki, 2013b, p.119; Gray, 2013, pp.40, 44-45. Cf. Brodie, 1946). Hence, judging the cyber offense-defense "balance" at any point in time requires evaluating the impact of cyber force projection on overall outcomes of such multi-domain conflict. Importantly, the impacts of the interaction of cyber capabilities with physical capabilities in multi-domain conflict may be the inverse of impacts within the cyber domain only.

For example, an intensified use of cyber weapons could impede or exacerbate crisis escalation (Fischerkeller, et.al., 2022: 51-53). Some strategic implications of cyber operations in crises and early-phase conflicts flow from the novel features of key capabilities that are intrinsic to the cyber domain, including the value of concealment and the uncertainties that imposes. A general dearth of cyber situational awareness broadens the sources of potential strategic surprise. Thus, both offensive and defensive cyber weapons can have indeterminate effects on the crisis behavior of states, depending on the specific configuration of the situation.

6. Conclusion

The preceding application of a more robust framework for evaluating the offense-defense balance in cyberspace leads to several conclusions.

- The indistinguishability of the offensive or defensive nature of sophisticated cyber weapons supports the value of offensive strategies. The secrecy incumbent to the cyber domain exacerbates this influence.
- Relative costs associated with developing and utilizing cyber capabilities may favor the offense, but the secrecy incumbent to the domain impedes more thorough evaluation of relative costs.
- The most indicative measure of the offense-defense advantage, outcomes, is complicated by several factors, including the relation of cyber strategy to multi-domain planning and conduct, and the typically less-than-decisive role of cyber actions in overall conflict outcomes.

Taken together, these findings suggest there is merit to the conventional wisdom that the balance in the cyber domain tips to the offense. But a major factor in this conclusion are novel characteristics of the cyber domain itself, rather than simply the capabilities to project power within it. Additionally, ever-changing technologies continually reshape cyberspace as a medium of warfare, creating an imperative of constant adaptation distinct from other domains. Hence, the application of systematic understandings of offense-defense theory has value but will still leave unanswered important questions rooted in the uniquely dynamic character of the cyber domain (Demchak & Dombrowski, 2011, pp.54-57; Gartzke and Lindsay, 2015, pp. 317-8).

These challenges in some respects underscore critiques of general offense-defense theory's capacity to explain international outcomes. However, the effort to apply offense-defense theory to the cyber domain, in addition to yielding insightful if not definitive findings, can also contribute productively to the further development of offense-defense theory's explanatory power in a twenty-first century context of multi-domain warfare.

Disclaimer: The views expressed here are those of the authors and do not necessarily represent the views of the Naval Postgraduate School, the Department of Defense, or the U.S. Government.

References

Ackerman, G., Sundelson, A., & Wetzel, A. (2024). 'No-one Likes a Cry-Baby": The Effectiveness of Victimization Narratives in External Information Operations. Journal of Information Warfare, 23(1).

Arquilla, J. (2012) "Panetta's Wrong About a Cyber 'Pearl Harbor' - The Internet doesn't work that way," *Foreign Policy* November 19.

Aucsmith, D. (2012) "War in Cyberspace: A Theory of War in the Cyber Domain," *Cyberbelli.com,* May-June 2012.

Belk, R., & Noyes, M. (2012) "On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy," *Belfer Center for Science and International Affairs, Harvard Kennedy School,* March 2012.

Bernard, B., editor. (1946) *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Co.

Briggs, G. (2023). Desperately Seeking Strategic Alignment: Australia's Response to the Informatic Environment as a Global Security Disruptor. Journal of Information Warfare, 22(4), 40–52.

Brito, J. & Watkins, T. (2011) "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard National Security Journal* Vol. 3.

Buvarp, P. M. H. (2023). The Space of Influence: Developing a New Method to Conceptualise Foreign Information Manipulation and Interference on Social Media. Journal of Information Warfare, 22(2), 31–51.

Clarke, R. A. & Knake, R. K. (2010) *Cyber War* (New York: Harper Collins).

Clarke, R., Ormrod, D., Lim, Y., & Slay, J. (2023). The Evolution of Chinese Cyber Offensive Operations and Association of Southeast Asian Nations (ASEAN). Journal of Information Warfare, 22(1), 44–60.

Demchak, C. C. (2012) "Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World," in N. Burns & J. Price (Eds.), *Securing Cyberspace: A New Domain for National Security.* Washington, DC: The Aspen Institute, 2012.

Demchak, C. C. & Dombrowski, P. (2011) "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* (Spring), pp.32-61.

Fischerkeller, M. P., Goldman, E. O., and Harknett, R. J. (2022) *Cyber Persistence Theory: Redefining National Security in Cyberspace*. Oxford University Press.

Gartzke, E. & Lindsay, J.R. (2015) "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace," *Security Studies* Vol. 24.

Goddard, S. E. (1998-1999) "Correspondence: Taking Offense at Offense-Defense Theory," *International Security* 23:3 (Winter).

Goldman, E., & Monarez, E. (2021). Persistent Engagement and the Private Sector. Journal of Information Warfare, 20(2), 107–122.

Gray, C. S. (2013) "Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling," *Strategic Studies Institute and U.S. Army War College Press,* April 2013.

Harknett, R. J., Callaghan, J. P., & Kauffman, R. (2010) "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," *Journal of Homeland Security and Emergency Management,* Vol. 7, No. 1, November 11, 2010.

Hiltunen, E., & Huhtinen, A. (2022). Future of Information Influence Operations: Scifi as a Tool to Imagine the Unthinkable. Journal of Information Warfare, 21(4), 79–99.

Howard, M. (1979). "The Forgotten Dimensions of Strategy," *Foreign Affairs*, Vol. 57, No. 5.

Hutchinson, W. (2022). Strategic Cognition War. Journal of Information Warfare, 21(3), 74–83.

Jervis, R. (1978) "Cooperation under the Security Dilemma," *World Politics,* 30:2 (January 1978), pp. 167-214.

Kello, L. (2013) "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security,* 38: 2 (Fall 2013), pp. 7-40.

Krepinevich, A. (2012) "Cyber Warfare: A 'Nuclear Option'?" *Center for Strategic and Budgetary Assessments,* (2012).

Langner, R. (2013) "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," The Langner Group (Arlington | Hamburg | Munich), November.

Leatherman, A.E. (2024) "Is Offense-Defense Theory Still Relevant in Cyberspace" [Master's Thesis, Naval Postgraduate School].
Lehto, M. (2023). Cyber Warfare and War in Ukraine. Journal of Information Warfare, 22(1), 61–75.
Libicki, M. C. (2009) *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND, 2009.
Libicki, M. C. (2012) "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society,* 8:2 (Fall 2012), p. 325-340.
Libicki, M. C. (2013a) "Brandishing Cyberattack Capabilities," RAND National Defense Research Institute (2013)
Libicki, M. C. (2013b) "Don't Buy the Cyberhype: How to Prevent Cyberwars From Becoming Real Ones," *Foreign Affairs,* August 14, 2013
Lieber, K. A. (2000) "Grasping the Technological Peace: The Offense-Defense Balance and International Security," *International Security,* 25:1 (Summer).
Lieber, K. A. (2005) *War and the Engineers: The Primacy of Politics over Technology* (Ithaca, N.Y.: Cornell University Press).
Lieber, K. A. (2007) "The New History of World War I and What It Means for International Relations Theory," *International Security* 32:2 (Fall).
Lieber, K. A. (2008) "Correspondence: Defensive Realism and the 'New' History of World War I," *International Security* 33:1 (Summer).
Lieber, K. (2014) "The Offense-Defense Balance and Cyber Warfare," in Emily O. Goldman and John Arquilla, *Cyber Analogies*, Technical Report: NPS-DA-14-001, Naval Postgraduate School.
Lonsdale, D. J. (2009) "The Impact of Cyberspace on Strategy," *High Frontier*.
Lynn-Jones, S. M. (1995) "Offense-Defense Theory and its Critics," *Security Studies* 4:4 (Summer).
Lynn, W. J. III (2010) "Defending a New Domain," *Foreign Affairs,* 89:5 (September 2010), pp. 97–108.
Malone, P. J. (2012) "Offense-Defense Balance in Cyberspace: A Proposed Model" [Master's Thesis, Naval Postgraduate School].
Masters, J. (2011) "Confronting the Cyber Threat," *Council on Foreign Relations,* May 23, 2011.
Meriläinen, N. (2023). "Information operations do not worry me" – The Role of Credible Information on Digital Platforms. Journal of Information Warfare, 22(4), 93–112.
Morgan, P. M. (2003) *Deterrence Now* (Cambridge University Press).
Morgan, P. M. (2010) "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (National Research Council).
Morgenthau, H. J. (1948). *Politics Among Nations: The Struggle for Power and Peace*. New York: Alfred A. Knopf
Murphy, B. (2023). Evaluating the Ambiguous Cognitive Terrain: A Framework to Clarify Disinformation. Journal of Information Warfare, 22(3), 9–27.
Noel, G., & Reith, M. (2021). Cyber Warfare Evolution and Role in Modern Conflict. Journal of Information Warfare, 20(4), 30–44.
Nye, J. S. Jr. (2010) "Cyber Power," *Belfer Center for Science and International Affairs,* May 2010.
Panetta, L. E. (2012) Secretary of Defense, "Defending the Nation from Cyber Attack," Speech to Business Executives for National Security, New York, New York, Thursday, October 11, http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1728.
Rattray, G. J. (2009) "An Environmental Approach to Understanding Cyberpower," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (National Defense University Press).
Rid, T. (2012) "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1 (February).
Sagan, S. D. (1994) "The Perils of Proliferation: Organization Theory, Deterrence Theory, and the Spread of Nuclear Weapons," *International Security*, Vol. 18, No. 4 (Spring).
Sakellariadis, J. (2022). "Extending the 'Attribution Problem': Why Who-Based Attribution Is Insufficient to Deterring Cyberattacks," *Journal of Information Warfare,* 21(2), 64–76.
Saltzman, I. (2013) "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* 34/1.
Saressalo, T., & Huhtinen, A. (2022). Information Influence Operations: Application of National Instruments of Power. *Journal of Information Warfare*, *21*(4), 41–66.
Schelling, T. (1966) *Arms and Influence* (Yale University Press).
Sheikh, H. (2022). AI as a Tool of Hybrid Warfare: Challenges and Responses. *Journal of Information Warfare*, *21*(2), 36–49.
Sheldon, J. B. (2011) "Deciphering Cyberpower Strategic Purpose in Peace and War," *Strategic Studies Quarterly,* Summer 2011.
Slayton, R. (2016/17) "What is the Cyber Offense-Defense Balance?" *International Security* 41/3 (Winter).
Snyder, J. (2008) "Correspondence: Defensive Realism and the 'New' History of World War I," *International Security* 33:1 (Summer).
Sterner, E. (2010) "Stuxnet and the Pentagon's Cyber Strategy," Arlington, Va.: George C. Marshall Institute, October 13, 2010.
Turner, B., Ryan, R., Karie, N., & Guidetti, O. (2024). The Theory of Transitional Target Defence: A New Approach to Enhancing Cyber Deception. Journal of Information Warfare, 23(1).
U.S. Department of Defense (DoD) (2011) "Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934," November.

U.S. Joint Chiefs of Staff (JCS). (2013) "Joint Publication 3-12 (R): Cyberspace Operations," 5 February 2013. [Online] Available at: www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf .

Van Evera, S. (1998) "Offense, Defense, and the Causes of War," *International Security,* 22:4 (Spring, 1998), pp. 5-43.

Van Evera, S. (1998/99) "Correspondence: Taking Offense at Offense-Defense Theory," *International Security,* 23:3 (Winter, 1998-1999), pp. 195-200.

Van Niekerk, B. (2023). The Evolution of Information Warfare in Ukraine: 2014 to 2022. Journal of Information Warfare, 22(1), 10–31.