The Offense-Defense Balance in Cyberspace

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

*(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.)

wlhuntle@nps.edu
timothy.shives@nps.edu

Abstract: The study of cyber strategy and its implications for international security has become increasingly crucial, necessitating an examination of the unique challenges posed by the dynamic and stealthy nature of the cyber domain. This paper addresses whether offensive or defensive strategies prevail in cyberspace, especially in light of evolving technological landscapes and debates over cyber threats. By applying offense-defense theory from international relations, the research explores the nuanced relationship between offensive and defensive operations in cyberspace. Despite prevalent views favoring offense dominance, recent skepticism questions the severity of cyber threats and suggests a possible overemphasis on offensive operations. This paper systematically examines the core concepts, findings, and operational variables of offense-defense theory, providing clarity to the conceptual debates surrounding cyber conflict. Recognizing the unique characteristics of the cyber domain, it urges a careful consideration of biases that may distort judgments about offense dominance. The evolving nature of cyberspace and its potential for redesign introduces caution and underscores the need for a nuanced understanding of the offense-defense balance. The preliminary assessment concludes that the question of whether offense or defense "dominates" in cyberspace is overly simplistic. Given the intricate interactions of cyber capabilities, other coercive means available to states, and the dynamic evolution of cyber technology, this question can only be answered within specific contextual and chronological boundaries. Within such conditions, the state of the offense-defense balance is crucial to tactical and operational decision-making. At the strategic policymaking level, the more coherent question is how cyber technologies are shifting the balance of advantages between offense and defense in the overall military posture of states. In essence, this paper provides valuable insights into the ongoing discourse on cyber strategy, theoretical frameworks, and nuanced analyses to inform policy and strategic decision-making in the face of evolving cyber threats.

Keywords: Cyber Strategy, Offense-Defense Relationship, International Security, Cyber Threats, Offense-Defense Theory

1. Introduction: Offense and Defense in Cyberspace

The paper delves into the intricate realm of cyber strategy, shedding light on the delicate balance between offense and defense in cyberspace. It emphasizes the evolution from traditional information warfare to the contemporary concept of cognitive warfare, reflecting the modern focus on influencing and controlling populations on social, political, and military fronts (Buvarp, 2023). By leveraging established international relations theory, this paper provides clarity to ongoing conceptual debates, advocating for a nuanced understanding of the dynamic nature of cyber threats and the strategic importance of cognitive dimensions.

The question of whether offense or defense holds the upper hand in cyberspace is a central focus within broader discussions of military cybersecurity. However, many of these discussions rely on reasoned yet largely unsubstantiated assertions. Systematic exploration within the framework of existing offense-defense theory has been limited (Lieber, 2014). Furthermore, recent developments suggest that 'cyber' is a tool, not an end, with the ultimate targets being the minds of opponents and allies rather than their digital tools (Meriläinen,; 2023).

This paper addresses this gap by presenting an initial framework for applying the fundamental tenets of offense-defense theory to the cyber domain, while also integrating the principles of cognitive warfare (Canham, et al, 2022; Hiltunen & Huhtinen, 2022; Buvarp, 2023; Murphy, 2023). The goal is to enhance our understanding of the interplay between offensive and defensive capabilities in cyber military conflict and cognitive operations (Nye, 2010). Following a brief overview of representative claims regarding offensive advantage, the section introduces a working definition of “offense” and “defense” in cyberspace. It then applies Jervis’ (1978) two principal variables – 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).

2. The intuition of offense advantage in cyberspace

Numerous strategists and decision-makers assert that offense holds the upper hand in the cyber domain (Lynn, 2010; Harknett, Callaghan, and Kauffman, 2010; Sterner, 2010; Masters, 2011). Sheldon (2011) provides five reasons supporting the dominance of offense in cyberspace: vulnerability of network defenses, the speed of

cyber-attacks, the absence of distance as an inhibiting factor, difficulty in attributing attack sources, and the "target-rich" environment resulting from society's widespread reliance on cyberspace.

Kello (2013) and Krepinevich (2012) also argue in favor of the significant advantage of cyber offense, with a focus on costs. Kello identifies defense costs, including anticipating unpredictable and undetectable cyber-attacks, ensuring the detection of system penetrations, dealing with the "complex defense surface" in terms of hardware and software complexity, managing "defense fragmentation" caused by critical infrastructure ownership by private entities, and ensuring the reliability of supply chains. While acknowledging that cyber-attacks can be expensive, Kello emphasizes that "offensive costs [have] meaning only in reference to the expenses of the defender" (Kello, 2013, pp.27-30). Similarly, Krepinevich (2012) concludes that "the cyber competition appears to be an offense-dominant competition. That is to say, if both the attacker and defender are given equal resources, the attacker will prevail" (p. 40).

These arguments are noteworthy for their consideration of the cost aspect, aligning with one of the two principal aspects of the offense-defense balance identified by Jervis. However, they fall short in not examining the role of this balance in shaping conflict outcomes. Additionally, these formulations neglect the other key variable in determining offensive or defensive advantage: whether capabilities can be differentiated in these terms.

Aucsmith (2012) surveys new features of cyber conflict relevant to both offense and defense. The "compression" of time and space eliminates geography, granting "omnipotent mobility" that empowers the offense to choose when and where to strike. Equally crucial is offensive novelty, defined for cyber weapons as the use of tactics, techniques, or procedures unknown to the defender. The assertion that novelty is the crucial criterion for success in a cyber-attack carries significant implications for the offense-defense balance in cyberspace. If both offense and defense face equivalent costs for achieving novelty, essentially engaging in a "race" to discover vulnerabilities first, neither side gains a clear advantage by this measure.

However, when considering the full picture, even if the unit cost of discovering a relevant vulnerability is the same for both offense and defense, other factors come into play. For instance, the cost of patching vulnerable networks is likely higher than the cost of exploiting discovered vulnerabilities. This suggests that the cumulative costs of defense could still outweigh those of offense. Additionally, the failure of a significant percentage of end-users to implement patches in a timely manner adds further burdens to defense.

Contrary to the prevailing view that offense dominates in cyberspace, Gray (2013) challenges this notion. He contends, "Although it continues to be orthodox to assert that cyberspace is ... friendly to offense, rather than defense, this fashionable belief almost certainly either is wrong, or to be generous, is seriously misleading" (p. 41). Beyond the cost equivalency of offense and defense in identifying vulnerabilities, Gray notes that offense incurs unique costs. For instance, "Detailed up-to-date intelligence literally is essential for successful cyber offense" (Gray, 2013, p.51).

In contrast to traditional domains such as land, sea, air, and space, cyberspace stands out as a humanly created realm. Notably, the medium itself, not just the tools used for projecting force within it, can be modified by human intervention. This inherent quality grants defense a meta-advantage: beyond defending specific targets, those controlling the networks and systems seeking defense could potentially reshape the entire domain to enhance defensive capabilities (Nye, 2010). An illustrative example of this is the impending transition from IPv4 to IPv6, but a more profound instance could involve a comprehensive redesign of basic computer architecture. This redesign might incorporate physically distinct memory locations for data and software instructions, effectively eliminating certain types of malware attacks, such as "buffer overflows," that rely on computers storing instructions and data in the same memory locations.

Gray (2013) underscores the significance of resilience as a defensive advantage. Drawing parallels with the British experience during World War II, where strategic bombing had limited effectiveness, he notes, "Britain prepared to be able to accept damage but to fight on. This is the approach that appears most suitable to the challenge of damage from cyberspace. Cyber offense will register some success, but so what" (Gray, 2013, pp. 41). The emphasis here is on the ability to absorb damage and continue the fight, highlighting resilience as a key defensive strategy in the face of cyber threats.

While the existing analyses of the offense-defense balance in cyberspace offer valuable insights, they fall short of providing a systematic application of the frameworks and variables of offense-defense theory. However, they serve as illuminating and insightful starting points, indicating elements that require more detailed specification for a thorough systematic application. This section identifies key elements essential for such an analysis, which are discussed in the paper:

- Examining differentiation of offensive and defensive weapons in cyberspace
- Calculating costs of offense and defensive capabilities in cyberspace
- Understanding the operational aspect of the offense-defense balance
- Appreciating how the interaction of cyber and non-cyber (physical) forms of conflict shapes judgments of the utility of offensive and defensive cyber capabilities

These identified elements serve as a foundation for a more systematic examination of the offense-defense balance in cyberspace. Further specification and exploration of these components will contribute to a more nuanced understanding of the intricate dynamics within the cyber domain in the era of information warfare and persistent engagement particularly in light of the recent conflicts in Ukraine and the rising threats in Southeast Asia (Goldman & Monarez, 2021; Clarke, et al, 2023; Lehto, 2023; Van Niekerk, 2023)

3. The meanings of “offense” and “defense” in cyberspace

To comprehend the terms "offense" and "defense" in the cyber domain, it's crucial to establish a conceptual framework that aligns with broader international relations scholarship. Nye (2010) provides an insightful foundation, associating these concepts with their wider usage.

Nye begins by defining power as "the ability to affect other people to get the outcomes one wants," highlighting its relational and contextual nature. In cyberspace, power is contextual, dependent on the resources characterizing this unique domain (Nye, 2010). Cyberspace, according to Nye, represents a hybrid regime of physical and virtual properties, encompassing not just networks and software but also informational and identity dimensions. The U.S. Department of Defense similarly recognized the cyberspace domain's layers, including physical network, logical network, and cyber-persona (U.S. Joint Chiefs of Staff, 2013). In the literature this understanding has expanded into the realm of hybrid warfare—that is information warfare and the traditional physical warfare (Saressalo & Huhtinen, 2022; Sheikh, 2022; Ormrod, et al, 2023).

Within this domain, Nye identifies resources of power as infrastructure, networks, software, human skills, and more, enabling the creation, control, and communication of electronic and computer-based information. He defines cyber power as "the ability to obtain preferred outcomes through the use of electronically interconnected information resources of the cyber domain." This definition encompasses achieving outcomes within and outside cyberspace, acknowledging that relevant contexts extend beyond the cyber realm (Ackerman, et al, 2024; Briggs 2023.

By defining cyber power as the ability to obtain preferred outcomes through cyberspace capabilities, a clear distinction emerges between offensive and defensive cyber capabilities:

- *Defensive Cyber Capabilities*: Aim to preserve and protect one's own cyber resources.
- *Offensive Cyber Capabilities*: Aim to penetrate and affect another's cyber resources.

This distinction aligns with most generic notions of offense and defense in cyberspace. Libicki (2012), for instance, defines offensive cyber operations as attempts to exploit information system vulnerabilities to interfere with the ability of victims to carry out military or other tasks. This paper adopts a working definition of cyber offense as actions seeking to exploit vulnerabilities to interfere with adversaries' military or national security-related operations. Cyber defense, in turn, involves actions to thwart adversaries undertaking such offensive actions against oneself.

Understanding these definitions is crucial as they lay the groundwork for analyzing the offense-defense balance in cyberspace. The delineation between offense and defense in cyberspace also encompasses the strategies and tactics used by states and non-state actors to assert power and control within this domain. By exploring these dimensions, the paper contributes to a nuanced understanding of how cyber capabilities are deployed in both offensive and defensive contexts, shaping the broader strategic landscape of international security.

4. Offense-defense differentiation in cyberspace

The task of differentiating offensive and defensive cyber capabilities, as per the preceding definitions, initially seems straightforward. Many specific capabilities can be easily categorized as defensive, such as malware detection and robust user password requirements, while offensive capabilities involve infiltrating target systems and extracting information.

At a basic level, offensive and defensive cyber weapons are distinguishable. However, complications arise, both acknowledged in offense-defense theory and unique to the cyber domain.

4.1 Dual-Use of Offensive Capabilities.

Offensive capabilities may serve defensive functions, and vice versa. For instance, offensive software might be employed to deactivate client computers of an attacking botnet or enhance network protections by detecting threatening malware parameters (Demchak, 2012; Belk and Noyes, 2012). Even the penetration of an adversary's network for intelligence gathering could be construed as essentially defensive, akin to radar or sonar activity. Differentiation in such cases depends on usage and user intentions.

4.2 Concealment in Cyberspace.

A unique challenge in cyberspace is the ease with which offensive capabilities can be concealed. Unlike traditional offense-defense theory, where transparency and time provide early warning of aggressive intentions, offensive cyber capabilities can be developed and deployed almost invisibly. The concealment undermines the benefits of offense-defense differentiation identified by Jervis. States can acquire offensive cyber capabilities without providing early warning to others, eroding the foundational assumption of transparency.

Concealment prevents status quo states from identifying aggressive states or relying on non-acquisition of offensive capabilities as a sign of peaceful intentions. In conditions where offense dominates, even status quo states may feel compelled to acquire offensive capabilities pre-emptively due to the uncertainty caused by the concealed nature of cyber development. In conditions favoring offense, states cannot confidently rely solely on defensive capabilities unless they are certain that all potential adversaries are refraining. The concealment of offensive capabilities heightens the risk of pre-emptive acquisition among status quo states.

These complications necessitate a more nuanced approach to offense-defense differentiation in cyberspace. Traditional markers of offense and defense become blurred, requiring analysts and policymakers to consider intent, context, and the fluidity of cyber operations. Furthermore, the dual-use nature of many cyber capabilities and the inherent difficulty in discerning their true purpose exacerbate the challenge. In response, a robust framework that integrates these complexities is essential for developing effective cyber strategies and ensuring informed decision-making in both national and international security contexts.

5. Offense-defense balance of advantage in cyberspace

The second foundational variable of offense-defense theory focuses on the offense-defense balance of advantage in conflict, considering military costs and operational effectiveness. Jervis identifies these two aspects, and their application in cyberspace further elucidates the dynamics of the offense-defense relationship.

5.1 Cost Variations.

Several analysts, including Libicki, highlight cost variations to argue that offense is advantaged in cyberspace. Libicki's detailed examination of the offense-defense balance emphasizes direct military costs. In a snapshot of circumstances around 2009, he points to U.S. government expenditures on military network security as indicative of offensive advantage. Utilizing Jervis' definition, he notes that "another dollar's worth of offense requires far more than another dollar's worth of defense to restore prior levels of security" (Libicki, 2009, p.32). However, Libicki observes that these cost figures may be influenced by the historical context of relatively low levels of conflict interaction. This highlights the importance of considering the specific circumstances and dynamics prevailing in the cyber domain.

The application of the offense-defense theory to cyberspace involves a nuanced analysis of both cost variations and operational effectiveness. While cost considerations often point to offense advantage, understanding the broader operational effectiveness of offensive and defensive capabilities is essential. The balance in cyberspace is influenced by the intricate interplay between costs, historical context, and the evolving nature of conflict interactions.

5.2 Operational Effectiveness

Beyond cost considerations, operational effectiveness plays a critical role in determining the offense-defense balance. Offense in cyberspace often benefits from the element of surprise, speed, and the ability to exploit vulnerabilities before they are patched. Defensive measures, on the other hand, require constant vigilance, updates, and adaptability to new threats. The dynamic and rapidly evolving nature of cyber threats means that defense must continuously evolve, often at a significant cost.

Libicki's assessment, despite acknowledging the current cost imbalance favouring offense, ultimately concludes that "the best defense is not necessarily a good offense; it is usually a good defense." However, this conclusion is contingent on the "highly problematic" prospects for cyber-deterrence, rather than a steadfast confidence in cyber defense per se (Libicki, 2009, p.176). The rationale is 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).

Further, Turner, et al (2024) note that transitional target defense and cyber deception may lead to capabilities that places the advantage towards the defender's side. in cyberspace, the balance of advantage is not static but continuously shifting with technological advancements, new tactics, and evolving threats. Defensive strategies must adapt to not only counter immediate threats but also anticipate future vulnerabilities. Offensive strategies, meanwhile, capitalize on current weaknesses but must also innovate to stay ahead of defensive measures.

In conclusion, while cost variations and operational effectiveness often indicate an offensive advantage in cyberspace, the overall balance is fluid and context-dependent. Effective cyber strategy requires a comprehensive understanding of both offensive and defensive dynamics, continuous adaptation, and the ability to anticipate and counter emerging threats. This nuanced approach is essential for maintaining security and stability in the ever-evolving cyber domain.

6. The geography of cyberspace

Exploring the geography of cyberspace, especially in the context of offense-defense theory, reveals a complex and indeterminate realm. The traditional determinants of advantage in this theory, such as the capacity to "take" or "hold" geographic territory, face challenges in the multifaceted dimensions of cyberspace.

6.1 Metaphorical Mapping.

Cyberspace's physical attributes, including computers, networks, and people, allow for metaphorical geographical mappings. National networks could be considered home terrain, military networks as "key terrain," and malware intrusion as an equivalent to invasion. However, these applications are metaphorical and may not fully capture the virtual dimensions of cyberspace. The virtual dimensions, encompassing information, interaction networks, and identity personas, introduce further complexity. The metaphor of geography becomes both illuminating and misleading, with challenges in applying traditional concepts to the dynamic and rapidly changing nature of cyberspace.

6.2 Borderless and Border-Rich Perspectives

Cyberspace is sometimes referred to as a "borderless" realm, highlighting the ease and speed of information flow globally. The malleability of the "geography" in this context allows for infinite pathways, transcending traditional national borders. Alternatively, a "border-rich" perspective considers the thresholds between owned and unowned cyber capabilities as defining boundaries. In the physical dimension, every system's boundary with the cyber environment constitutes a border. In the virtual aspect, emerging and disintegrating boundaries occur at the speed of thought, challenging traditional concepts of distance.

6.3 Multiplicity of Conceptions

The concept of geography in cyberspace is suggestive but ultimately indeterminate. Constructed through analogy and metaphor, various conceptions of the "lay of the land" exist, each useful for illuminating specific cyber security points. While borders and key terrain may have meaningful applications within specific conflict situations, the multiplicity of potential conceptions makes it challenging to develop a single rigorous framework.

The limitations of the concept of geography in cyberspace pose challenges for the application of offense-defense theory. The essence of offense and defense, as suggested by Jervis, involves the ability to "take" or "hold" territory. However, the viability of these objectives in the diverse conceptions of cyberspace remains uncertain. The impossibility of perfect defense, a concern in cyberspace, is likened to historical battles, emphasizing that challenges in defense are not unique to the digital domain. The main point of this example for cyber conflict is simple: in cyberspace, as in many other forms of conflict, the penetrability of boundaries is not by itself an indication that offense has the advantage. Offense-defense theory points to the importance of grasping strategic consequences holistically and looking to longer-term outcomes as the primary indicators of success and failure in conflict. This holds as a reasonable standard of offensive and defensive efficacy in cyberspace.

7. Perishability and obsolescence

Cyber weapons entail two closely related traits that distinguish them from weapons in other domains. This paper terms these traits perishability and obsolescence. Perishability refers to a weapon becoming ineffective after a single use. Obsolescence refers to a weapon becoming ineffective without being used at all. These traits arise from the reliance of cyber weapons on computer system vulnerabilities, particularly zero-day exploits. These vulnerabilities can be discovered and fixed, rendering the weapon useless.

Perishability induces conservation, as cyber weapons are often saved for crucial moments, especially when exploiting specific vulnerabilities. This conservation contributes to crisis stability and increases the potential for strategic surprise. On the other hand, obsolescence can occur even without using the cyber weapon, as the targeted vulnerability may be removed through system updates or improvements. This potential obsolescence creates incentives for states to use the weapon before it becomes useless, potentially inducing crisis instability. The lack of awareness about impending vulnerability elimination adds a layer of strategic surprise.

Together, perishability and obsolescence impact the behavior of states in an escalating crisis, with the configuration of effects determining the overall stability or instability of the situation. These traits have significant implications for assessing the offense-defense relationship in cyberspace. They emphasize the importance of secrecy, complicating the distinction between offensive and defensive cyber forces. Additionally, perishability and obsolescence incentivize states to discover new vulnerabilities and stockpile a wide range of cyber weapons, leading to a "silent arms race" characterized by aggressive development in both defensive and offensive cyber capabilities. This condition aligns with the security dilemma and reflects the potential dangers of offense-defense indistinguishability and offensive advantage in the cyber domain.

Thus, cyber weapon perishability and obsolescence tend to both obscure the distinguishability of cyber forces and promote cyber capability arms-racing. This condition captures the essence of the security dilemma and approaches the “doubly dangerous” outcome Jervis identified in a world of offense-defense indistinguishability and offensive advantage.

8. Linkages of cyber and physical conflict

Up to this point, applying the basic framework of offense-defense theory to cyberspace suggests indications that trend toward offensive advantage. As discussed above, state incentives to cloak cyber capabilities and the interactivity of cyber and physical capabilities make distinguishing offensive and defensive cyber weapons difficult. Cost considerations – the first of the two aspects of the offense-defense balance—may also favor the offense, and in any event, the principal impact of offensive cost advantage—arms races—also emerges from the unique perishability and obsolescence of cyber weaponry. However, the second aspect of the offense-defense balance – operational effectiveness in shaping the outcomes of conflicts – remains.

Most formulations of offense-defense theory, including Jervis’, treat military force posture cumulatively. That is, the offense-defense balance is defined by those military capabilities that would be most likely to determine the overall results of conflict. In this sense, the concept of offense-defense balance applies to the relations of states holistically. That is, the approach directs attention not to how specific types of weapons encounter one another, but to how they change strategies of conflict overall.

The application of offense-defense theory to cyberspace underscores a tendency toward offensive advantage. This assessment takes a holistic view, considering military force posture cumulatively in terms of major state decisions, arms procurement, crisis stability, war initiation, and outcomes. Cyber weapons, while capturing strategic attention, lack the war-deciding quality seen in nuclear or certain conventional weapons. The impact of cyber capabilities in interstate conflict remains uncertain. The strategic implications of cyber weapons are intricately linked to their interaction with physical capabilities in multi-layered conflicts.

Cyber weapons alone cannot fully determine conflict outcomes, as the introduction of other weapons may be driven by circumstantial advantages. There exists the potential for an initially cyber-only conflict to escalate to the use of physical weapons, challenging the concept of an independent "cyber war." Instead, understanding the strategic implications of cyber weapons requires tracing their impacts through all potential forms of coercive interaction and conflict. The interplay of offense and defense in cyberspace is complex, with defense enabling offense and vice versa. The confidence in protecting military computer networks influences decisions related to physical military actions.

Rather than a simplistic assessment of offense or defense dominance in cyberspace, the focus shifts to understanding how cyber capabilities have shifted the broader offense-defense balance between states. Thus, the simple question of whether offense or defense dominates in cyberspace is misleading. The more strategically useful question is whether and how the advent of cyber capabilities has shifted the offense-defense balance between states more broadly. Answers to this question, in turn, depend complexly on the extent and configuration of states’ other military capabilities, and on the physical and diplomatic circumstances of their interactions with one another. This observation bounds much of the discussion of the implications of cyber weapons and cyber defenses.

9. Conclusion

Van Evera (1998; 1998/1989) taking seriously the meaningfulness of offense-defense theory to explain state behaviour and international outcomes, offers a stark conclusion. He emphasizes the historical context of offense-defense theory to caution against overestimating offense dominance, noting its rarity and inherent dangers. Exaggerated perceptions of insecurity often lead to bellicose conduct, which can exacerbate national insecurity and precipitate war. While acknowledging genuine cyber threats faced by the United States in the twenty-first century, he urges caution in assessing present and growing cyber threats, citing the potential for misjudgments and biased perceptions. The complexity, opacity, and necessary secrecy inherent in cyberspace magnify the challenges in accurately gauging the offense-defense balance.

The dynamic nature of the cyber domain underscores the need for caution, as cyberspace is a human-created domain with the potential for fundamental shifts in the exercise of power. Unlike other domains with fixed physical properties, cyberspace evolves under the influence of millions of uncoordinated individual actions. This unique dynamic terrain poses challenges in strategizing for the military uses of cyberspace. While understanding warfare patterns in other domains and historical contexts can inform our understanding of cyber warfare, it remains insufficient due to the novel and dynamic character of the cyber domain.

In a broader context, an examination of offense-defense theory and its application to cyberspace reveals significant implications for international relations and security. The historical perspective serves as a cautionary tale, urging careful consideration of the dynamics between offense and defense in the evolving realm of cyberspace. As the cyber domain continues to evolve, the imperative to learn, adapt, and exercise caution becomes increasingly paramount in ensuring the security and stability of the international order.

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).

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.

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.

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., 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.

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.

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).

Lehto, M. (2023). Cyber Warfare and War in Ukraine. Journal of Information Warfare, 22(1), 61–75.

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. (2009) *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND, 2009.

Lynn, W. J. III (2010) 'Defending a New Domain,' *Foreign Affairs,* 89:5 (September 2010), pp. 97–108.

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.

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.

Sakellariadis, J. (2022). Extending the 'Attribution Problem': Why Who-Based Attribution Is Insufficient to Deterring Cyberattacks. Journal of Information Warfare, 21(2), 64–76.

Saressalo, T., & Huhtinen, A. (2022). Information Influence Operations: Application of National Instruments of Power. *Journal of Information Warfare*, *21*(4), 41–66.

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.

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. Joint Chiefs of Staff. (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. (1998/99) 'Correspondence: Taking Offense at Offense-Defense Theory,' *International Security,* 23:3 (Winter, 1998-1999), pp. 195-200.

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

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