INTERNATIONAL JOURNAL OF CYBER THREAT INTELLIGENCE AND SECURE NETWORKING (IJCTISN)

eISSN: 3087-4297

Volume. 02, Issue. 03, pp. 06-11, March 2025

COLLATERAL EFFECTS AND UNINTENDED REPERCUSSIONS IN OFFENSIVE CYBER OPERATIONS: A SYSTEMATIC LITERATURE REVIEW

Dr. Wei-Lin Cheng
Department of Cyber Engineering, National Cheng Kung University, Tainan, Taiwan

Article received: 25/01/2025, Article Accepted: 14/02/2025, Article Published: 18/03/2025
DOI: https://doi.org/10.55640/ijctisn-v02i03-02

ABSTRACT

Offensive cyber operations (OCOs) are increasingly employed by state and non-state actors to achieve strategic objectives in cyberspace. However, these operations often produce collateral effects and unintended repercussions that extend beyond their immediate targets. This systematic literature review analyzes academic and policy research to uncover the scope, nature, and consequences of such unintended outcomes. Key themes include civilian infrastructure disruption, geopolitical escalation, legal and ethical dilemmas, and blowback on originating systems. The review also highlights gaps in risk assessment methodologies and accountability frameworks within offensive cyber strategies. By synthesizing existing findings, the study aims to inform the development of more responsible and resilient cyber doctrines that minimize harm and ensure compliance with international norms.

Keywords: Offensive Cyber Operations (OCOs), Collateral Damage, Unintended Consequences, Cyber Warfare, Cyber Ethics, Blowback Effects, Critical Infrastructure, Geopolitical Risks, International Law, Systematic Literature Review.

INTRODUCTION

The advent of the digital age has fundamentally transformed the landscape of international security, introducing cyberspace as a distinct domain of conflict [9, 15]. Alongside traditional military domains—land, sea, air, and space—cyberspace presents unique opportunities for nations to project power and achieve strategic objectives through offensive cyber operations (OCOs) [3]. These operations, ranging from espionage and sabotage to disruption and destruction, offer novel means of engagement, often characterized by their stealth, deniability, and potentially broad impact. The global cybersecurity market's substantial growth, projected to be a multi-trillion-dollar opportunity, underscores the increasing reliance on digital infrastructure and, consequently, the expanding threat surface [1]. The escalating costs of data breaches further highlight the severe repercussions of cyber incidents [2].

While OCOs offer strategic advantages, their deployment introduces a complex array of challenges, particularly concerning unintended consequences and spillover effects. Unlike kinetic warfare, where physical boundaries and the laws of armed conflict provide some degree of predictability, cyber operations often transcend geographic borders and can impact interconnected systems in unforeseen ways [8, 14]. The highly networked and interdependent nature of modern critical infrastructures, including cyber-physical systems (CPS) [10], means that an attack on one component can ripple through seemingly unrelated systems, causing widespread collateral damage [11, 13]. For instance, the Stuxnet worm, initially aimed at specific nuclear facilities, demonstrated how a highly targeted cyber weapon could escape its intended environment and spread globally, albeit with limited impact outside its primary target [4]. Such incidents underscore the inherent difficulty in precisely controlling the effects of cyber weapons once unleashed [17].

The lack of established norms, international legal frameworks specific to cyber conflict, and the technical

complexities involved make the assessment and mitigation of unintended consequences a critical yet underexplored area. Moreover, the attribution challenges inherent in cyberspace can lead to miscalculations and escalation, contributing to an unstable security environment [5, 6]. Despite the growing recognition of these risks, a systematic understanding of the types, mechanisms, and mitigation strategies for unintended consequences and spillover effects in OCOs remains nascent.

This systematic literature review aims to address this critical gap by synthesizing existing knowledge on unintended consequences and spillover effects in offensive cyber operations. It seeks to categorize the various forms these effects can take, analyze the factors contributing to their emergence, and identify current approaches to their assessment and mitigation. By providing a comprehensive overview, this review intends to inform policymakers, military strategists, and cybersecurity researchers on the profound implications of OCOs and the necessity for a more nuanced approach to their planning and execution.

METHODS

This systematic literature review was conducted to comprehensively analyze existing research and discussions on unintended consequences and spillover effects in offensive cyber operations (OCOs). The methodology involved a structured approach to identify, extract, synthesize, and categorize information from the provided references.

1. Data Source and Collection: The primary data source for this review consisted of the list of 17 references provided by the user. These references included academic papers, government reports, industry analyses, and news articles. Each reference was systematically accessed and reviewed for content relevant to OCOs, unintended consequences, spillover effects, collateral damage, and related concepts.

2. Inclusion and Exclusion Criteria: Given the predefined set of references, formal inclusion/exclusion criteria for initial literature selection were not applied. Instead, the focus was on extracting all relevant information from the provided documents. The core criterion for information extraction was its direct or indirect linkage to:

Definitions or discussions of offensive cyber operations.

Descriptions or analyses of unintended consequences, collateral damage, or spillover effects resulting from OCOs.

Discussions on the challenges of targeting, precision, and control in cyberspace.

Legal or policy frameworks attempting to govern OCOs and mitigate their impact.

3. Data Extraction and Thematic Analysis: For each relevant reference, the following information was extracted:

Definition/Conceptualization: How OCOs, unintended consequences, or collateral damage were defined or conceptualized.

Examples/Case Studies: Any specific examples of OCOs and their observed or potential unintended effects (e.g., Stuxnet [4]).

Contributing Factors: Elements identified as leading to unintended consequences (e.g., interconnectedness of systems [10, 11], lack of precise targeting [7, 12]).

Impacts: Types of impacts discussed (e.g., economic [2], reputational, operational disruption, international relations).

Mitigation Strategies/Challenges: Proposed solutions, legal frameworks, or inherent difficulties in controlling OCOs (e.g., Tallinn Manual [8], Law of War [16], assessment methodologies [17]).

Following data extraction, a thematic analysis approach was employed. Concepts and findings from across the references were grouped into overarching themes. These themes formed the basis for the "Results" section, systematically categorizing the various aspects of unintended consequences and spillover effects.

4. Synthesis and Discussion: The categorized findings were then synthesized to build a cohesive understanding of the current state of knowledge. This involved identifying overlaps, contradictions, and gaps in the literature. The "Discussion" section critically evaluates these findings, elaborates on the implications of unintended consequences, and proposes areas for future research, drawing directly from the challenges and unaddressed aspects highlighted in the reviewed literature. This methodological approach ensures that the review is directly informed by the provided sources and contributes to a structured understanding of the complex topic.

RESULTS

The systematic review of the provided literature reveals a consensus on the complex and often unpredictable nature of offensive cyber operations (OCOs), particularly regarding their unintended consequences and spillover effects. The findings can be categorized into the definitions of OCOs and their unintended effects, the mechanisms through which these effects manifest, and the challenges in their assessment and mitigation.

I. Defining Offensive Cyber Operations and Unintended Effects

Offensive cyber operations are broadly understood as actions taken in cyberspace to achieve strategic or tactical objectives, often involving the disruption, degradation, or destruction of an adversary's systems or data [3, 15]. These operations can range from espionage to sabotage and can be carried out by state actors [5] or state-sponsored entities. The intent is typically to achieve a specific effect on a target, whether military or civilian.

Unintended Consequences / Collateral Damage / Spillover Effects: The literature uses several terms interchangeably or with subtle distinctions to describe the negative outcomes of OCOs that extend beyond the primary intended target or effect.

Collateral Damage: This term, borrowed from kinetic warfare, refers to the unintentional harm or damage inflicted on non-military persons or objects during an attack on a legitimate military objective [14, 16]. In the cyber domain, it applies to damage to civilian infrastructure or data not directly targeted, resulting from a cyberattack [11, 13].

Spillover Effects: This concept describes the propagation of an OCO's effects beyond the intended target system or network, often into interconnected or interdependent systems, including those of third parties or allied nations. This is particularly relevant given the highly networked nature of modern infrastructure, including cyber-physical systems [10].

Unintended Consequences: This is a broader term encompassing any unforeseen or unsought outcomes of an OCO, which could include technical, political, economic, or legal repercussions not directly related to physical damage [11]. The IBM Security Cost of a Data Breach Report highlights the significant economic consequences of cyber incidents, even if unintended by the attacker [2].

II. Mechanisms of Unintended Consequences and Spillover

The interconnectedness and complexity of modern digital infrastructure are the primary drivers of unintended consequences and spillover effects in OCOs.

Interdependency of Systems: Modern critical infrastructures, including energy grids, financial systems, and healthcare networks, are deeply interconnected, forming a complex web of cyber-physical systems [10]. An attack on one seemingly isolated system can have cascading effects on interdependent systems, even if they are not the direct target. For instance, an attack on a specific industrial control system might disrupt power delivery to an entire region, impacting hospitals or other critical services [11].

Lack of Precise Targeting and Effects Prediction: Unlike kinetic weapons, cyber weapons often lack the same level of predictability and precision [7, 12]. Once a cyber tool is deployed, its propagation and exact effects can be difficult to control, especially in dynamic network environments. The Stuxnet worm, designed for a specific industrial control system, notably spread beyond its intended target, demonstrating the difficulty in containing sophisticated cyber tools [4]. This lack of control makes it challenging to adhere to traditional military targeting principles like distinction and proportionality [14, 16].

Vagueness of Cyber Boundaries: Cyberspace is inherently borderless. A cyber operation launched from one nation can easily impact systems in other nations due to the global nature of the internet and shared infrastructure. This blurs traditional notions of sovereignty and can lead to unintended international political or economic repercussions [8].

Unforeseen Interactions: The sheer complexity of software and network interactions can lead to unforeseen outcomes. A cyber tool designed to exploit a specific vulnerability might trigger unexpected behaviors in other parts of the system or in systems that interact with the targeted one, leading to collateral damage [13].

Attribution Challenges: The difficulty in accurately attributing cyberattacks [5] can itself be an unintended consequence. Misattribution can lead to retaliatory actions against the wrong actor, escalating tensions and creating further unintended geopolitical instability [6].

III. Assessment and Mitigation Challenges

The literature identifies significant challenges in assessing and mitigating unintended consequences of OCOs.

Difficulty in Measuring Damage: Quantifying collateral damage in cyberspace is inherently complex. Unlike physical damage, which can be visually assessed, cyber damage often manifests as data corruption, system downtime, or functional degradation, which are harder to measure consistently [11].

Operational Planning Limitations: Current military targeting doctrines, primarily developed for kinetic warfare, struggle to fully account for the unique characteristics of cyberspace. While concepts like proportionality and distinction apply [16], their practical application in cyber operations is challenging due to the unpredictable nature of effects and the interconnectedness of systems [7, 12, 17]. The U.S. Air Force Intelligence Targeting Guide highlights the complexities involved [12].

Legal and Normative Gaps: The international legal framework for OCOs is still evolving, leading to ambiguities regarding the permissibility of certain actions and accountability for unintended harm [8]. The Tallinn Manual 2.0 attempts to codify international law in cyberspace but acknowledges many unresolved areas [8].

Lack of Pre-computation Models: There is a need for robust assessment methodologies to evaluate potential collateral damage and military advantage in cyber operations before execution [17]. Developing such models requires deep understanding of system interdependencies and precise prediction of cyber weapon effects, which are currently limited.

Information Asymmetry: The attacker often has incomplete information about the target network's full topology and interdependencies, making it difficult to accurately predict collateral effects.

In summary, the review underscores that unintended consequences and spillover effects are inherent risks in offensive cyber operations, driven by the interconnected nature of cyberspace and the inherent unpredictability of cyber weapon effects. Addressing these challenges requires a concerted effort in developing more sophisticated assessment methodologies, refining international legal norms, and promoting greater transparency and restraint in OCOs.

DISCUSSION

The systematic review of the literature profoundly reinforces the notion that offensive cyber operations, while offering unique strategic advantages, inherently carry significant risks of unintended consequences and spillover effects. These effects are not mere externalities but are deeply intertwined with the fundamental characteristics of cyberspace: its pervasive interconnectedness, the borderless nature of information flow, and the inherent unpredictability of highly complex systems [10, 11]. The analysis has shown that the very strengths of cyber operations—stealth, deniability, and reach—also contribute to their potential for uncontrolled proliferation and unforeseen impacts.

The Inherent Paradox of Precision in Cyberspace

One of the most striking findings is the paradox of "precision" in offensive cyber operations. While cyber weapons can be designed to target specific vulnerabilities with high granularity (as seen with Stuxnet [4]), their effects are notoriously difficult to confine. The digital realm’s interdependencies mean that a highly precise attack on a military target could inadvertently cascade into civilian infrastructure, violating the principle of distinction in the law of armed conflict [14, 16]. This challenge is exacerbated by the attacker's frequent lack of complete situational awareness regarding the target's entire network topology and interdependencies. As Romanosky and Goldman [11, 13] highlight, understanding cyber collateral damage requires a deep appreciation of these complex linkages, a level of insight often unavailable during live operations. Traditional targeting doctrines, designed for kinetic warfare [7, 12], struggle to translate directly to the cyber domain, creating a critical gap in operational planning [15].

Broader Implications Beyond Technical Damage

The unintended consequences of OCOs extend far beyond mere technical damage. They encompass a wide spectrum of repercussions, including:

Economic Disruption: As evidenced by the rising costs of data breaches [2], even indirect impacts on civilian infrastructure can lead to significant economic losses, affecting critical services and national economies.

Geopolitical Instability: Misattribution of attacks [5] or unforeseen impacts on non-belligerent nations can escalate international tensions, leading to retaliatory measures and destabilizing global relations [6]. The "fog of cyberwar" makes de-escalation difficult.

Erosion of Trust and Norms: The frequent occurrence of unintended consequences without clear accountability erodes trust among nations and undermines efforts to establish international norms of responsible state behavior in cyberspace. The absence of robust legal frameworks and accepted conventions for OCOs, despite efforts like the Tallinn Manual [8], contributes to this normative vacuum.

Humanitarian Impact: Attacks on critical civilian infrastructure, even if unintended, can have severe humanitarian consequences by disrupting essential services like healthcare, water supply, or emergency response systems.

Future Directions and Policy Imperatives

Addressing the challenges posed by unintended consequences in OCOs requires a multi-faceted approach, integrating technical, legal, and policy solutions.

Advanced Effect Prediction and Containment: Future research and development must focus on creating more sophisticated models and tools for predicting the cascading effects of cyber operations on complex, interconnected systems [17]. This includes leveraging artificial intelligence and machine learning to analyze network topologies and anticipate spillover. Concurrently, developing better techniques for containing cyber effects, preventing their propagation beyond intended targets, is paramount.

Refinement of International Law and Norms: There is an urgent need for states to clarify and agree upon the application of international law, particularly the law of armed conflict, to cyberspace [8, 16]. This includes establishing clearer interpretations of proportionality, distinction, and necessity in the context of OCOs, and developing norms around responsible state behavior to reduce unintended escalation and harm.

Enhanced Situational Awareness and Intelligence Sharing: Improving intelligence gathering on target networks, including their interdependencies with civilian infrastructure, is critical for better operational planning. Greater international collaboration and information sharing on threat intelligence can also help prevent unintended impacts on third parties [1].

Development of "Cyber Ethics" and Responsible Conduct Frameworks: Beyond legal obligations, there is a growing need for ethical frameworks to guide the conduct of OCOs, emphasizing restraint and minimization of harm to non-combatants and civilian infrastructure.

Investment in Defensive Resilience: Recognizing the inevitability of some unintended consequences, nations must also prioritize building robust defensive capabilities and resilience in their critical infrastructures. This includes designing systems with inherent fault tolerance and rapid recovery mechanisms to absorb and mitigate external shocks, whether intended or not.

CONCLUSION

In conclusion, the systematic review underscores that while offensive cyber capabilities are a reality of modern geopolitics, their deployment demands an acute awareness of, and proactive measures against, their inherent unintended consequences and spillover effects. A failure to adequately address these risks threatens to undermine international stability, impede economic development, and cause unacceptable civilian harm. Future efforts must prioritize interdisciplinary research and international cooperation to navigate the complex ethical, legal, and technical landscape of offensive cyber operations responsibly.

REFERENCES

[1] Aiyer, B.; Caso, J.; Russell, P.; Sorel, M. Mckinsey: New Survey Reveals $2 Trillion Market Opportunity for Cybersecurity Technology and Service Providers. 2022. Available online: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers (accessed on 30 January 2024).

[2] IBM Security; the Ponemon Institute. Cost of a Data Breach Report 2022. 2022. Available online: https://www.ibm.com/downloads/cas/3R8N1DZJ (accessed on 31 January 2024).

[3] Hanson, F.; Uren, T. Australia's Offensive Cyber Capability. 2018. Available online: https://www.aspi.org.au/report/australias-offensive-cyber-capability (accessed on 31 January 2024).

[4] Farwell, J.P.; Rohozinski, R. Stuxnet and the Future of Cyber War. Survival 2011, 53, 23–40. [Google Scholar] [CrossRef]

[5] U.S. Department of Justice. Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe. 2022. Available online: https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and (accessed on 1 February 2024).

[6] Schelling, T.C. Dispersal, deterrence, and damage. Oper. Res. 1961, 9, 363–370. [Google Scholar] [CrossRef]

[7] U.S. Air Force. Air Force Doctrine Publication 3–60, Targeting. 2021. Available online: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf (accessed on 1 February 2024).

[8] Schmitt, M.N. (Ed.) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations; Cambridge University Press: Cambridge, UK, 2017. [Google Scholar]

[9] Arquilla, J.; Ronfeldt, D. Cyberwar is coming! Comp. Strategy 1993, 12, 141–165. [Google Scholar] [CrossRef]

[10] Lee, E.A.; Seshia, S.A. Introduction to Embedded Systems: A Cyber-Physical Systems Approach, 2nd ed.; MIT Press: Cambridge, MA, USA, 2017. [Google Scholar]

[11] Romanosky, S.; Goldman, Z. Cyber Collateral Damage. Procedia Comput. Sci. 2016, 95, 10–17. [Google Scholar] [CrossRef]

[12] U.S. Air Force. Intelligence Targeting Guide, Attachment 7. 1998. Available online: https://irp.fas.org/doddir/usaf/afpam14-210/part20.htm (accessed on 1 February 2024).

[13] Romanosky, S.; Goldman, Z. Understanding Cyber Collateral Damage. J. Natl. Secur. Law Policy 2017, 9, 233–257. [Google Scholar]

[14] Dinstein, Y. The Principle of Distinction and Cyber

War in International Armed Conflicts. J. Confl. Secur. Law 2012, 17, 261–277. [Google Scholar] [CrossRef]

[15] Ablon, L.; Binnendijk, A.; Hodgson, Q.E.; Lilly, B.; Romanosky, S.; Senty, D.; Thompson, J.A. Operationalizing Cyberspace as a Military Domain, Perspective, RAND Corporation 2019. Available online: https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE329/RAND_PE329.pdf (accessed on 30 January 2024).

[16] U.S. Department of Defense. Department of Defense Law of War Manual; William S. Hein & Company: Getzville, NY, USA, 2023.

[17] Maathuis, C.; Pieters, W.; Van den Berg, J. Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations. In Proceedings of the MILCOM 2018—2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 29–31 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.