Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 3 No. 10 (2025)

CYBER WARFARE AND THE APPLICATION OF INTERNATIONAL HUMANITARIAN LAW: A LEGAL VACUUM?

[1]Johar Wajahat
[2]Ms Saira Ali
[3]Dr. Rafia Naz Ali
[1]Assistant Professor, Department of Law, Shaheed Benazir Bhutto Women University Peshawar
[2]Assistant Professor, Department of Law, University of Haripur, Haripur
[3]Assistant Professor, Department of Shariah and Law Islamia College University Peshawar
[1]johar.wajahat@sbbwu.edu.pk, [2]saira.ali@uoh.edu.pk, [3]rafia@icp.edu.pk

Abstract

The integration of cyberspace into the modern battlefield has generated a paradigm shift in the character and conduct of warfare. It presents profound challenges to the established international legal order. In this context, the applicability of International Humanitarian Law (IHL) has been subject to intense debate, leading to assertions that a "legal vacuum" exists in this new and unregulated domain. This paper expostulates that such claims, while reflecting genuine operational and definitional challenges, are conceptually linear and detached from the doctrinal reality of IHL's universal applicability. IHL, with its inherent adaptive nature, is universally applicable (lex lata) to cyber operations during armed conflict, a principle firmly affirmed by the International Court of Justice (ICJ, 1996). However, the defining characteristics of cyber warfare, in particular its non kinetic nature, the pervasive anonymity it affords actors, and the deep structural entanglement of civilian and military networks, critically strain the practical application of cardinal IHL principles, such as distinction, proportionality, and the very definition of an "attack." This research, therefore, argues that the core challenge is not the absence of law, but a profound functional and interpretive gap in its implementation and enforcement. This gap, exacerbated by the strategic reluctance of major cyber powers to develop binding normative frameworks, creates a "legal labyrinth" of ambiguity rather than a true vacuum. While influential scholarly frameworks like the Tallinn Manual 2.0 (Schmitt, 2017) provide critical interpretive guidance, their non binding nature underscores the political inertia that prevents the emergence of concrete legal clarity and state practice. This study, therefore, takes a cursory examination of the security and humanitarian implications emanating from this core ambiguity, concluding that the international community's collective failure to bridge this interpretative gap poses a far larger threat to civilian protection and international security than the acknowledged difficulties of applying existing law to novel technologies.

Keywords: Cyber Warfare, International Humanitarian Law, Principle of Distinction, Legal Vacuum, Tallinn Manual, Pakistan.

Article Details:

Received on 29 Sept 2025
Accepted on 26 Oct 2025
Published on 28 Oct 2025

Corresponding Authors*:

Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 3 No. 10 (2025)

Introduction

The twenty first century battlefield has been fundamentally and irrevocably recast, extending beyond physical terrain into the nebulous and borderless domain of cyberspace. Cyber warfare, conceptualized as the use of digital tools by state and non state actors to achieve information superiority and strategic objectives during crises or declared conflict, has become a pervasive and defining feature of contemporary hostilities (Alberts, Garstka, & Stein, 2005; Qureshi, 2020). This evolution challenges the very foundations of International Humanitarian Law (IHL), the legal regime meticulously designed to mitigate the horrors of war by regulating the conduct of parties involved in an armed conflict. Codified primarily in an era anticipating kinetic warfare, IHL's transplantation into the digital realm raises a pivotal and urgent question: does the sui generis nature of cyber operations create a regulatory void, a "legal vacuum" that leaves this new domain of conflict largely ungoverned?

High profile incidents like the 2007 cyberattacks against Estonia (Herzog, 2011; Tikk, Kaska, & Vihul, 2010) and the cyber operations that coincided with the 2008 Russo Georgian War (Markoff, 2008) catapulted this question to international prominence. The subsequent and persistent lack of consensus among states on how to regulate this domain underscores its profound complexity. While the International Court of Justice (ICJ) affirmed the application of IHL principles to all forms of warfare (ICJ, 1996), the unique characteristics of cyber warfare complicate the concrete interpretation and enforcement of these established principles (Khalil & Raj, 2024; Wallace & Jacobs, 2019). This article therefore examines the applicability of IHL to cyber warfare in light of this alleged legal vacuum. It aims to demonstrate that while IHL theoretically applies as lex lata, its practical implementation faces profound "fault lines" that can be, and are being, exploited by states (Sohail, 2022), including Pakistan (Bibi, 2023), thereby creating a de facto governance gap that critically jeopardizes foundational humanitarian protections.

The Adaptability of IHL: Lex Lata Versus Political Inertia

The assertion of a complete legal vacuum is largely unfounded from a strict doctrinal standpoint. The majority opinion among international legal experts confirms that IHL applies to cyberspace (Droege, 2012; Gisel et al., 2020). The International Court of Justice (ICJ) has unequivocally affirmed that the established principles and rules of humanitarian law apply to "all forms of warfare and all kinds of weapons, including those of the future" (ICJ, 1996). This universal applicability, a product of IHL's intent to be technologically neutral, is the bedrock of its continuing relevance. Any military operation, regardless of the technology used, must be assessed against these established IHL norms (Igakuboon, 2022). Furthermore, Article 36 of Additional Protocol I (API) mandates that states evaluate new weapons, means, or methods of warfare for their compliance with international law (Jevglevskaja, 2015). Complementary to this is the enduring Martens Clause, which acts as a vital legal safety net. It ensures that in cases not explicitly covered by international agreements, civilians and combatants remain under the protection and authority of principles derived from established customary law, the principles of humanity, and the dictates of public conscience (Gisel et al., 2020; Bibi, 2023; Igakuboon, 2022).

However, the law on the books (lex lata) diverges sharply from the law in concrete practice and enforcement. Given the novelty of cyber warfare, the existing sources of authoritative international law on the subject are often restricted to the subsidiary source of academic commentary and expert interpretation (Bibi, 2023). The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Schmitt, 2017) stands as the most

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 10 (2025)

comprehensive, yet non binding, articulation of how existing IHL applies to cyber operations. Developed by an international group of experts, the Manual attempts to determine the scope and application of IHL rules, clarifying complex concepts and addressing areas of expert disagreement (Jensen, 2017; Schmitt, 2017). However, valid critiques suggest that the Manual primarily reflects the consensus of its specific expert group, rather than a universal state agreement or practice, thereby intrinsically limiting its legal authority and standing (Mathonet, 2020; Schmitt, 2017). This heavy reliance on non binding guidance, rather than on state driven customary law or new treaties, points to a critical political inertia among powerful states.

Operational and Definitional Challenges: The IHL Fault Lines

The transposition of IHL principles from the physical to the virtual domain reveals severe interpretive limitations and operational ambiguities, particularly concerning the core objective of protecting civilians from the effects of hostilities (Khalil & Raj, 2024; Schmitt, 2019).

1. The Ambiguous Threshold of "Attack"

For the specific IHL rules governing the conduct of hostilities to be triggered, an operation must first qualify as an "attack." Article 49(1) of API defines "attacks" as "acts of violence against the adversary, whether in offence or in defence." The non physical, often non destructive nature of many cyber operations critically strains this conventional definition (Biggio, 2021). The prevailing consensus among scholars and experts leans toward an effects based approach, whereby the consequences of an operation, rather than its intrinsic nature, determine its legal classification (Biggio, 2021; Mathonet, 2020). For a cyber operation to qualify as an attack governed by IHL, it must cause consequences such as physical harm to individuals, destruction of physical objects, injury or death, or excruciating pain or illness (Igakuboon, 2022; Gisel et al., 2020). The decisive factor is often whether the consequence functionally disables the object, rendering it useless for its intended purpose (Biggio, 2021). Consequently, disruptive activities that cause mere inconvenience, temporary disruption, or psychological effects, like the spread of propaganda, often fall below the necessary damage threshold to trigger the full weight of IHL's conduct of hostilities rules (Pascucci, 2017). This ambiguity creates a permissive environment for hostile cyber operations that fall just short of this contested threshold, operating in a grey zone of conflict.

2. The Challenge of Attribution and Anonymity

The pervasive anonymity inherent in the architecture of cyberspace makes reliable and timely attribution of an attack to a specific state or group extremely difficult (Sohail, 2022; Kilovaty, 2014). Malicious actors can effortlessly use proxies, compromised infrastructure, and false flags to conceal their identity and shift blame, thereby challenging the fundamental requirement of assigning responsibility that is necessary for any effective IHL enforcement and accountability (Sohail, 2022). In the context of non international armed conflict (NIAC), attribution is also linked to establishing the legal criteria of "organization" and "intensity" for a non state armed group (Cullen, 2010). While organized armed groups normally possess a discernible structure and a clear chain of command (ICTY, 1995), these traditional criteria do not easily fit loosely affiliated, remote cyber collectives that may operate transnationally without a fixed hierarchy (Sohail, 2022). This persistent attribution deficit creates a powerful shield of impunity for both state and non state actors alike, undermining the deterrent capacity of IHL.

Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 3 No. 10 (2025)

3. The Principle of Distinction and Dual Use Infrastructure

The principle of distinction, a cardinal and peremptory rule of IHL, requires parties to a conflict to distinguish at all times between protected civilian persons and objects, and lawful military objectives (Melzer, 2014). This foundational requirement is critically challenged by the inherent interconnectedness of cyberspace, where military and civilian infrastructure often share the same networks, servers, and internet service providers (Khalil & Raj, 2024; Dinstein, 2012). Targeting a military command and control system that routes through a civilian telecommunications grid may inevitably and severely disrupt crucial civilian functions, including emergency services, banking, and public health information systems (Khalil & Raj, 2024). The incidental harm caused to civilian objects is known as collateral damage, which must be considered in proportionality assessments (Pascucci, 2017).

Furthermore, the status of non physical digital data itself remains legally controversial (Mathonet, 2020). Traditional IHL rules were developed with tangible, physical objects in mind. Protecting civilians in the digital age, however, requires recognizing that the deletion, alteration, or manipulation of critical data, such as medical records or air traffic control data, could have devastating real world effects functionally equivalent to physical destruction, thereby making certain critical data sets deserving of protection as civilian objects (Mathonet, 2020).

4. The Principle of Proportionality

The principle of proportionality prohibits the launching of an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated (Pascucci, 2017; Melzer, 2014). Applying this principle to cyber operations is fraught with unprecedented difficulty, primarily due to the immense complexity of calculating indirect, second order, and cascading effects through interconnected networks (Mathonet, 2020; Pascucci, 2017). A cyber operation aimed at disabling a military power grid could trigger unpredictable chain reactions, inadvertently shutting down water purification plants, hospital generators, and traffic control systems. Furthermore, a central question for the proportionality calculus is determining whether permanently disabling a system, causing a loss of functionality, is legally equivalent to its physical destruction, a point that remains unsettled in state practice (Biggio, 20121; Sutherland, Xynos, Jones, & Blyth, 2015). The recent attacks using non traditional methods like pagers and walkie talkies have further raised complex questions about whether such actions, which can cause widespread disruption, constitute war crimes under international law (Hamzeh, 2024).

Discussion: The Legal Vacuum – Fact or Pretext?

The cumulative evidence suggests that cyberspace is emphatically not a legal vacuum in the strict doctrinal sense (lex lata). The foundational principles of IHL apply universally, as consistently recognized by the ICJ, the ICRC, and a majority of legal scholars (ICJ, 1996; Droege, 2012; Sohail, 2022).

IHL Applies, but Functional Gaps Exist

While IHL applies in principle, the absence of explicit, tailored provisions for cyber warfare and the pronounced lack of state consensus on key interpretations create substantial lacunae, or functional legal gaps (Wallace & Jacobs, 2019; Sohail, 2022). The law, developed for and through the experience of conventional kinetic warfare, is functionally strained when applied to the unique characteristics of cyber conflict, particularly its speed, scale,

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 10 (2025)

and non physical nature (Khalil & Raj, 2024; Sohail, 2022). The core inadequacy of the current framework lies in three interconnected areas: the definitional thresholds for key concepts like "attack," the erosion of the distinction principle due to ubiquitous dual use infrastructure (Dinstein, 2012; Khalil & Raj, 2024), and the enforcement deficits caused by pervasive attribution difficulties (Kilovaty, 2014).

Exploitation by Cyber Powers

A critical argument advanced by this paper is that the pervasive ambiguity surrounding these definitional thresholds is not merely an academic problem; it is often strategically exploited by powerful cyber states to evade legal responsibility and maintain operational flexibility (Geist, 2015; Sohail, 2022). This political inertia, driven by the desire to retain strategic advantage and freedom of action for their growing offensive cyber capabilities, actively prevents the emergence of clear, consistent state practice (usus) and the necessary sense of legal obligation (opinio juris) required for new customary law (Mathonet, 2020). The Stuxnet attack in 2010 on Iran's Natanz nuclear facility, which caused physical destruction of centrifuges by manipulating industrial control systems (Farwell & Rohozinski, 2011; Richmond, 2012), vividly highlighted the legal ambiguity surrounding whether such functional destruction amounts to "damage to civilian objects" under a proportionality analysis (Richmond, 2012; Mathonet, 2020; Schmitt, 2019). This seminal incident demonstrated that cyber operations can achieve kinetically destructive results, thereby blurring the once clear lines between kinetic and non kinetic warfare and exposing the inadequacy of current legal interpretations (Rid & McBurney, 2012).

The Legal Posture of Pakistan

The formidable challenge of applying IHL to cyber warfare is highly relevant and acutely felt in the South Asian region, where Pakistan is legally bound by the core IHL treaties, including the Geneva Conventions of 1949 (Bibi, 2023). However, an examination reveals that Pakistan's domestic cybersecurity and legal framework faces significant challenges in aligning with these international obligations:

- Insufficient Domestic Law: Pakistan's existing legal architecture, such as the Electronic Transactions Ordinance (ETO, 2002) and the Prevention of Electronic Crimes Act (PECA, 2016), primarily addresses cybercrimes, data protection, and commercial activities, offering only a rudimentary and fragmented framework for addressing the complex threats of cyber warfare and regulating state conduct during armed conflict in cyberspace (Bibi, 2023).
- Domestic Law as State Practice: From a international law perspective, domestic legislation like the ETO and PECA are considered constituent elements of verbal acts for discerning a state's practice and opinio juris regarding Customary International Humanitarian Law (CIHL) (Bibi, 2023). The continued reliance on a limited legislative framework focused on criminality, rather than warfare, underscores the significant gap between Pakistan's international legal obligations and its domestic doctrinal and legal readiness for cyber conflict.
- Contrasting Stance on LAWS: It is noteworthy that Pakistan has taken a notably proactive and principled stance on other emerging technologies of warfare, specifically against Lethal Autonomous Weapons Systems (LAWS). Pakistan has argued in international forums that allowing machines to make final, autonomous decisions over life and death is fundamentally against the principles of IHL and basic humanitarian considerations (Piątkowski, 2017). This indicates a capacity for engagement with the

Policy Journal of Social Science Review
Online ISSN 3006-4635
Print ISSN 3006-4627
Vol. 3 No. 10 (2025)

legal challenges of future warfare means, which contrasts sharply with the identified vulnerabilities and gaps in its defensive and legal cyber posture.

The heavy reliance on basic cybercrime legislation when facing potential threats to critical national infrastructure from state actors during times of conflict underscores the urgent and pressing need for a more comprehensive national legal and strategic doctrine in Pakistan to effectively align its cyber defense and potential offensive doctrines with established IHL principles (Qureshi, 2020).

Conclusion and Recommendations

Cyber warfare fundamentally changes the ontology of modern conflict, necessitating a clear and unequivocal application of IHL to preserve its humanitarian object and purpose. This research confirms that IHL lex lata applies to cyber operations during armed conflicts (Droege, 2012; Igakuboon, 2022), but the pronounced lack of international consensus on key definitions, such as "attack" (Biggio, 2021) and "military objective" (Melzer, 2014), coupled with the immense challenge of attribution (Kilovaty, 2014), creates a substantial, functional legal gap that critically compromises the protection of civilians and the safe functioning of civilian infrastructure (Khalil & Raj, 2024; Sohail, 2022). The international community must move beyond doctrinal debates to pragmatic, legally binding solutions. The following recommendations are advanced to address the existing legal and governance gaps:

1. Develop Binding Norms and Clarify Definitions: The international community, under the auspices of the United Nations, should prioritize the negotiation of a comprehensive, legally binding convention or a new protocol additional to the Geneva Conventions specifically governing cyber warfare and cyber operations during armed conflict (Mathonet, 2020; Qureshi, 2020; Sohail, 2022). This instrument must provide essential clarification on the threshold of a cyber "attack," moving beyond a strict requirement for physical violence to encompass functional destruction and other severe disruptive consequences that paralyse critical societal functions (Biggio, 2021).
2. Protection of Critical Civilian Datasets: Essential digital infrastructure and core data, such as health records, financial data, and humanitarian databases, must be formally recognized as "critical civilian datasets" (Mathonet, 2020), requiring protection equivalent to physical civilian objects under the principles of distinction and proportionality in IHL. Their intentional destruction or manipulation to cause harm should be unequivocally deemed a violation.
3. Enhance Accountability and Transparency: To foster the development of customary international law, states should be encouraged to publish detailed national statements and manuals regarding their interpretation and application of IHL to cyberspace, thereby contributing to opinio juris (Mathonet, 2020). Furthermore, reinforced technical and legal mechanisms for credible attribution, alongside greater transparency in legal decision making for cyber operations, are essential to ensure that IHL violations are not obscured by technological complexity and a lack of accountability (Kilovaty, 2014).
4. Strengthen National Resilience (Pakistan Focus): States like Pakistan must directly address the fragmentation and inadequacy of their current cyber legal frameworks (Bibi, 2023) by implementing a robust, modern, and comprehensive national cybersecurity strategy that specifically addresses the unique challenges of IHL application. This includes developing military doctrines for cyber operations that are fully aligned with IHL principles, particularly concerning targeting decisions in dual use networks, and

Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 3 No. 10 (2025)

investing in the technical and legal capacity to defend against and attribute attacks (Qureshi, 2020).

References

Alberts, D. S., Garstka, J., & Stein, F. P. (2005). Network Centric Warfare: Developing and Leveraging Information Superiority. CCRP Publication.

Bernard, V. (2012). Science cannot be placed above its consequences. International Review of the Red Cross, 94(886), 458.

Bibi, K. (2023). International humanitarian law on cyber warfare and Pakistan's legal regime (Master's thesis). International Islamic University Islamabad.

Biggio, G. (2021). International Humanitarian Law and the protection of the civilian population in cyberspace: Towards a human dignity-oriented interpretation of the notion of cyber attack under Article 49 of Additional Protocol I. The Military Law and the Law of War Review, 60(1), 114-140. doi:10.4337/mllwr.2021.01.06

Cullen, A. (2010). The concept of non-international armed conflict. Cambridge University Press.

Dinstein, Y. (2012). The principle of distinction and cyber war in International Armed Conflicts. Journal of Conflict and Security Law, 17(2), 261-277.

Droege, C. (2012). Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross, 94(886), 533-578.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40.

Geist, E. (2015). Deterrence stability in the cyber age. Strategic Studies Quarterly, 9(4), 44-61.

Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. International Review of the Red Cross, 102(913), 287-334.

Hamzeh, W. (2024, September 19). Pager and walkie-talkie attacks on Hezbollah look like war crimes – international legal expert. The Conversation.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security, 4(2), 49-60. doi:10.5038/1944-0472.4.2.3

Igakuboon, A. N. (2022). An appraisal of the legal framework for the protection of civilians in cyber-warfare under international humanitarian law. International Journal of Research and Scientific Innovation, 9(7), 14-26. doi:10.51244/ijrsi.2022.9702

International Court of Justice. (1996). Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion).

International Criminal Tribunal for the former Yugoslavia (ICTY). (1995). Prosecutor v. Dusko Tadic aka "Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction), IT-94-1.

Jevglevskaja, N. (2015). Legal Review of New Weapons: Origins of Article 36 of AP I. Finnish Yearbook of International Law, 109-140.

Kamiński, M. A. (2020). Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme. Security and Defense Quarterly, 20, 64.

Khalil, A., & Raj, S. A. K. (2024). Challenges to the principle of distinction in cyberspace warfare under International Humanitarian Law. Prawo i więź, 2(49).

Policy Journal of Social Science Review

Online ISSN 3006-4635

Print ISSN 3006-4627

Vol. 3 No. 10 (2025)

Kilovaty, I. (2014). Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare. American University National Security Law Brief, 5(1), 91-124.

Markoff, J. (2008, August 12). Before the gunfire, cyberattacks. The New York Times.

Mathonet, C. (2020). Protection of Civilians in the Era of Cyber Warfare: A Critical Analysis of International Humanitarian Law Towards a Treaty Restricting the Use of Cyber Weapons (Thesis). University of Amsterdam.

McDonald, J. (2016). Blind Justice? The Role of Distinction in Electronic Attacks. Ethics and Policies for Cyber Operations, 17-32.

Melzer, N. (2014). The principle of distinction between civilians and combatants. In A. Clapham & P. Gaeta (Eds.), The Oxford handbook of international law in armed conflict (pp. 296-331). Oxford University Press.

O'Donnell, B. T., & Kraska, J. C. (2006). Humanitarian law: Developing international rules for the digital battlefield. Journal of Conflict and Security Law, 8(1), 133-162.

Pascucci, C. P. (2017). Distinction and proportionality in cyber war: Virtual problems with a real solution. Minnesota Journal of International Law, 26, 419-460.

Piątkowski, M. (2017). Fully autonomous weapons systems and the prinicples of Interantional Humanitarian Law.

Qureshi, M. A. (2020). Information warfare, international law, and the changing battlefield. Fordham International Law Journal, 43(4), 901-938.

Richmond, J. (2012). Evolving battlefields: Does Stuxnet demonstrate a need for Modifications to the Law of Armed Conflict? Fordham International Law Journal, 35(3), 842-894.

Rid, T., & McBurney, P. (2012). Cyber-weapons. The RUSI Journal, 157(1), 6-13. doi:10.1080/03071847.2012.664354

Salman, H. D. (2025). The impact of contemporary war methods on the legal protection of civilians and combatants: A study in the context of International Humanitarian Law (Doctoral thesis). Al-Alamain Institute for Postgraduate Studies.

Schmitt, M. N. (2019). Wired warfare 3.0: Protecting the civilian population during cyber operations. International Review of the Red Cross, 101(910), 333-355.

Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Sharma, A. (2010). Cyber wars: A paradigm shift from means to ends. Strategic Analysis, 34(1), 62-73. doi:10.1080/09700160903354450

Sohail, H. (2022). Fault lines in the application of international humanitarian law to cyberwarfare. Journal of Digital Forensics, Security and Law, 17(1), 1-13. doi:10.15394/jdfsl.2022.1761

Sutherland, I., Xynos, K., Jones, A., & Blyth, A. (2015). The Geneva Conventions and Cyber-Warfare: A technical approach. The RUSI Journal, 160(4), 30-39. doi:10.1080/03071847.2015.1079044

Tikk, E., Kaska, K., & Vihul, L. (2010). International Cyber Incidents: Legal Considerations. Cooperative Cyber Defence Centre of Excellence.

Wallace, D. A., & Jacobs, C. W. (2019). Conflict Classification and Cyber Operations: Gaps, Ambiguities and Fault Lines. University of Pennsylvania Journal of International Law, 40(3), 643-693.