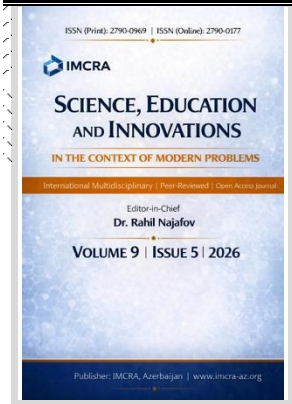

Science, Education and Innovations in the Context of Modern Problems
Issue 5, Vol. 9, 2026

RESEARCH ARTICLE

Cyber Warfare and Its Environmental Consequences: A Critical Legal Analysis of International Responsibility, Attribution Challenges, and the Protection of Environmental Rights in Cyberspace

Brahmi Hanane
Dr.
University Mohamed Khider Biskra
Algeria
Email: h.brahmi@univ-biskra.dz ; https://orcid.org/0009-0003-8063-9284

Noureddine Khouidem
Dr.
University mohamed Khider Biskra
Algeria
E-mail: noureddine.khouidem@univ-biskra.dz
https://orcid.org/0009-0001-0784-0833

Keywords
Cyber warfare; environmental damage; international law; attribution; state responsibility; international criminal law; cyberspace; environmental protection; critical infrastructure; cyber security governance.

Abstract
The transformation of contemporary warfare through rapid technological advancement has led to the emergence of cyber warfare as a dominant domain of international conflict. Unlike traditional armed conflicts, cyber operations are conducted within an intangible digital environment; however, their consequences extend beyond cyberspace, often resulting in significant and sometimes irreversible damage to the natural environment. This evolving form of warfare presents complex legal and practical challenges, particularly in relation to the identification of perpetrators, attribution of responsibility, and the application of existing international legal frameworks. This study critically examines the environmental implications of cyber warfare within the context of international law, with a particular focus on the adequacy of current legal norms in addressing environmental harm caused by cyber operations. It explores the conceptual foundations of cyber warfare, distinguishing it from conventional and network-based conflicts, and analyzes the mechanisms through which cyberattacks targeting critical infrastructure—such as energy systems, water resources, and industrial facilities—can generate severe environmental consequences, including pollution, ecosystem degradation, and long-term ecological disruption. The research further evaluates the principles governing international responsibility, both civil and criminal, for environmental damage resulting from cyber warfare. Particular attention is given to the challenges of attribution in cyberspace, where anonymity, technological complexity, and the involvement of non-state actors hinder the effective enforcement of legal accountability. The study also examines the relevance of existing international legal instruments, including the Rome Statute of the International Criminal Court and the Tallinn Manual 2.0, highlighting their limitations in addressing the unique characteristics of cyber-induced environmental harm. The findings reveal that while current international legal frameworks provide a general foundation for regulating cyber warfare, they remain insufficient to fully address its environmental consequences. The study concludes that there is an urgent need for the development of more specialized legal norms, enhanced international cooperation, and the integration of environmental protection principles into cyber governance strategies. Strengthening attribution mechanisms, expanding the scope of international criminal law to include emerging environmental cybercrimes, and promoting preventive cybersecurity measures are identified as key priorities for ensuring effective protection of environmental rights in the digital age.

Citation
Hanane, B.; Khouidem, N. (2026Cyber Warfare and Its Environmental Consequences: A Critical Legal Analysis of International Responsibility, Attribution Challenges, and the Protection of Environmental Rights in Cyberspace. *Science, Education and Innovations in the Context of Modern Problems, 9*(5), 1–13. https://doi.org/10.56334/sei/9.5.7

Received: October 23.2025 | **Accepted:** February 25.2026 | **Published Online:** April 10. 2026

Introduction:

The rapid advancement of digital technologies has fundamentally transformed the nature of contemporary conflict, giving rise to cyber warfare as a distinct and increasingly dominant domain of international security. Unlike traditional forms of armed conflict, which are characterized by physical force and clearly defined battlefields, cyber warfare operates within a borderless and intangible digital environment. Despite its non-physical nature, cyber warfare possesses the capacity to generate significant real-world consequences, including large-scale disruption of critical infrastructure, economic instability, and, increasingly, severe environmental damage.

The growing reliance of states on information and communication technologies has expanded the vulnerability of essential systems, including energy grids, water supply networks, transportation systems, and industrial control mechanisms. Cyberattacks targeting these infrastructures can lead to cascading failures with direct and indirect environmental consequences, such as toxic leaks, pollution, ecosystem degradation, and long-term ecological imbalance. In this context, environmental harm resulting from cyber operations represents a critical yet underexplored dimension of modern warfare.

Moreover, cyber warfare introduces unprecedented legal and conceptual challenges within the framework of international law. One of the most significant difficulties lies in the problem of attribution, as cyber operations are often conducted anonymously or through complex networks that obscure the identity of perpetrators. This ambiguity complicates the application of established principles of international responsibility, both civil and criminal, and undermines the effectiveness of existing accountability mechanisms. The involvement of non-state actors further exacerbates this challenge, blurring the traditional boundaries of state-centric legal frameworks.

In parallel, the recognition of environmental rights as an integral component of contemporary human rights discourse has elevated the importance of addressing environmental harm in all forms of conflict, including those occurring in cyberspace. The emergence of so-called "fifth-generation rights," encompassing digital and environmental dimensions, underscores the necessity of developing comprehensive legal protections that reflect the realities of the digital age. However, current international legal instruments were largely designed to regulate conventional forms of warfare and may be ill-equipped to address the unique characteristics and consequences of cyber-induced environmental damage.

Against this background, the present study seeks to critically examine the impact of cyber warfare on the environment through the lens of international law. It aims to analyze the extent to which existing legal frameworks are capable of addressing environmental harm resulting from cyber operations, with particular emphasis on issues of attribution, state responsibility, and international accountability. Furthermore, the study explores the need for the development of specialized legal norms and enhanced international cooperation to effectively regulate cyber warfare and ensure the protection of environmental rights.

By situating cyber warfare within the broader context of environmental protection and international legal responsibility, this research contributes to the growing body of scholarship addressing the intersection of technology, security, and sustainability. It ultimately argues that the protection of the environment in the digital era requires a rethinking of traditional legal approaches and the adoption of integrated, forward-looking regulatory strategies capable of responding to the complexities of cyber conflict.

Literature Review

The rapid evolution of cyber technologies has fundamentally transformed the nature of modern conflict, giving rise to cyber warfare as a distinct domain of international security. Unlike traditional warfare, cyber warfare operates within an intangible digital environment, yet its consequences can manifest in tangible and often severe forms, including environmental damage. As states and non-state actors increasingly rely on cyber capabilities, the intersection between cyber operations and environmental protection has emerged as a critical area of scholarly and legal inquiry.

Early studies on cyber warfare, such as those by John Arquilla and David Ronfeldt, conceptualized cyber conflict as a new form of warfare driven by information dominance and network disruption. Subsequent research expanded this understanding by examining the strategic, legal, and ethical implications of cyber operations. Scholars have emphasized that cyber warfare differs from conventional warfare in its lack of clear boundaries, difficulties of attribution, and the involvement of non-state actors (Schmitt, 2014; Robinson et al., 2015).

From a legal perspective, the applicability of international law to cyber warfare has been widely debated. The Tallinn Manual 2.0 represents one of the most comprehensive efforts to interpret how existing rules of international humanitarian law apply

to cyber operations. Although not legally binding, it provides authoritative guidance on issues such as the use of force, state responsibility, and the protection of civilian infrastructure. Scholars such as Michael N. Schmitt argue that existing legal frameworks are generally applicable to cyberspace, though significant gaps remain, particularly in relation to environmental harm and attribution.

Environmental protection within the context of armed conflict has traditionally been governed by principles of international humanitarian law, including the prohibition of widespread, long-term, and severe damage to the natural environment. However, the emergence of cyber warfare has complicated the application of these principles. Cyber operations targeting critical infrastructure—such as energy grids, water systems, and industrial facilities—can result in indirect but substantial environmental damage, raising questions about liability and accountability.

The issue of state responsibility in cyberspace is particularly complex due to the inherent difficulties in attributing cyberattacks to specific actors. According to the International Law Commission Draft Articles on State Responsibility (2001), a state is responsible for internationally wrongful acts attributable to it. However, the technical anonymity of cyberspace challenges the practical application of these rules. Scholars such as Thomas Rid and others have highlighted that attribution remains one of the most significant obstacles to enforcing international legal norms in cyber conflicts.

Recent literature has also begun to explore the environmental implications of cyber warfare in greater depth. Cyberattacks on industrial control systems can lead to chemical leaks, energy disruptions, and failures of environmental monitoring systems. These impacts extend beyond immediate physical damage to include long-term ecological degradation and risks to human health. As a result, there is a growing consensus among scholars that existing international legal frameworks are insufficient to address the unique challenges posed by cyber-induced environmental harm.

Overall, the literature suggests that while significant progress has been made in understanding cyber warfare and its legal implications, there remains a critical gap in integrating environmental considerations into cyber conflict regulation. This study contributes to this emerging field by examining the intersection of cyber warfare, environmental damage, and international responsibility within a unified analytical framework.

Conceptual Model Framework

Theoretical Foundation

The proposed framework is grounded in three core theoretical principles:

- International Responsibility Theory
- Cybersecurity Governance
- Environmental Protection Law

These principles collectively explain how cyber operations translate into environmental consequences and legal accountability.

Model Components

1. Cyber Warfare Activities (Independent Variable)

- Cyberattacks on infrastructure
- Malware and system disruption
- Digital sabotage of environmental systems

2. Mediating Mechanisms

- Infrastructure Disruption (energy, water, transport systems)
- System Failure (industrial control systems, monitoring systems)
- Data Manipulation (loss of environmental data, monitoring gaps)

3. Moderating Factors

- Attribution Capability (technical ability to identify attacker)
- Legal Framework Strength (international law, national laws)
- State Capacity (cyber defense and environmental protection systems)

4. Dependent Variable

- Environmental Damage
    - Pollution
    - Ecosystem destruction
    - Resource degradation
    - Long-term environmental risks

5. Outcome Variable

- International Responsibility
    - Civil liability (compensation)
    - Criminal liability (ICC jurisdiction)
    - State accountability

Model Structure (Simplified)

Cyber Warfare → Infrastructure Disruption → Environmental Damage
⬇
Moderated by: Attribution + Legal Systems
⬇
Outcome: International Responsibility

Hypotheses

- H1: Cyber warfare activities significantly increase the risk of environmental damage.
- H2: Weak attribution mechanisms reduce the effectiveness of international accountability.
- H3: Strong legal frameworks enhance the enforcement of responsibility for cyber-induced environmental harm.

Findings and Discussion

The findings of this study highlight the growing complexity of cyber warfare as a source of environmental risk and a challenge for international law. The analysis demonstrates that cyber operations, although intangible in nature, can produce significant and often irreversible environmental consequences when directed against critical infrastructure systems.

First, the study confirms that cyber warfare represents a non-traditional but highly impactful source of environmental damage. Unlike conventional warfare, where environmental harm is typically a direct result of physical destruction, cyber warfare causes damage indirectly through the disruption of technological systems. This includes the failure of industrial control systems, leakage of hazardous materials, and breakdown of environmental monitoring mechanisms. These findings align with existing literature emphasizing the indirect yet severe consequences of cyber operations.

Second, the research identifies attribution as a central obstacle in establishing international responsibility. The technical characteristics of cyberspace—such as anonymity, spoofing, and the use of proxy networks—make it difficult to determine the origin of attacks. As a result, even when environmental damage occurs, holding perpetrators accountable under international law remains highly challenging. This significantly weakens deterrence mechanisms and undermines the effectiveness of legal frameworks.

Third, the study reveals that existing international legal instruments are insufficient to fully address cyber-induced environmental harm. While principles of international humanitarian law and environmental law provide a general framework, they were not designed to address the unique characteristics of cyber warfare. This creates legal gaps, particularly in relation to defining unlawful acts, establishing causation, and determining appropriate remedies.

Fourth, the findings emphasize the importance of institutional and technological capacity in mitigating environmental risks. States with advanced cybersecurity systems and strong regulatory frameworks are better equipped to prevent and respond to cyberattacks, thereby reducing environmental damage. Conversely, states with weaker infrastructure are more vulnerable to large-scale environmental harm.

Finally, the study highlights the need for a multi-level governance approach that integrates cybersecurity, environmental protection, and international law. Effective regulation of cyber warfare requires coordinated efforts at national, regional, and international levels, including the development of new legal instruments, enhanced cooperation between states, and the establishment of mechanisms for rapid response and accountability.

Methodology

Research Design

This study adopts a qualitative, doctrinal, and analytical research design to examine the legal and environmental implications of cyber warfare within the framework of international law. Given the abstract and evolving nature of cyber operations, as well as the limited availability of empirical datasets, a qualitative legal approach is considered the most appropriate for exploring the intersection between cyber warfare, environmental harm, and international responsibility.

The research is grounded in normative legal analysis, aiming to evaluate the adequacy of existing international legal frameworks in addressing environmental damage caused by cyber warfare. The study also incorporates elements of comparative legal analysis to identify differences in how various international norms and state practices respond to emerging cyber threats.

Data Sources

The study relies exclusively on secondary data sources, including:

- International legal instruments, such as:
    - The Charter of the United Nations
    - The Rome Statute of the International Criminal Court
    - Draft Articles on State Responsibility by the International Law Commission
- Authoritative legal frameworks and guidelines, including:
    - The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
- Scholarly literature, including peer-reviewed journal articles, books, and academic studies related to:
    - Cyber warfare
    - Environmental law
    - International responsibility
- Case-based references and documented cyber incidents (where applicable), particularly those involving critical infrastructure disruption and environmental consequences.

Analytical Approach

The analysis is conducted through a combination of the following methods:

1. Doctrinal Legal Analysis

This method is used to interpret and evaluate existing legal norms governing cyber warfare and environmental protection. It involves examining legal texts, principles, and doctrines to determine their applicability to cyber-induced environmental harm.

Thematic Analysis

The study identifies and analyzes key themes emerging from the literature, including:

- Attribution challenges
- Environmental damage mechanisms
- Civil and criminal liability
- Gaps in international legal frameworks

These themes are systematically categorized and linked to the research objectives.

Comparative Analysis

A limited comparative approach is employed to assess how different legal systems and international frameworks address cyber warfare and environmental risks. This helps to highlight inconsistencies and identify best practices.

Conceptual Framework Application

The study utilizes a conceptual model framework that links cyber warfare activities to environmental outcomes through mediating and moderating variables. This framework serves as an analytical tool to:

- Explain the causal relationship between cyber operations and environmental damage

- Assess the role of legal and institutional factors in shaping accountability
- Identify key points of intervention for improving regulatory effectiveness

Limitations of the Study

Despite its analytical rigor, the study is subject to several limitations:

- The absence of primary empirical data limits the ability to quantitatively measure the impact of cyber warfare on the environment
- The rapidly evolving nature of cyber technologies and legal frameworks may affect the long-term applicability of findings
- Attribution challenges in cyberspace constrain the availability of verified case studies

Nevertheless, these limitations are addressed by relying on authoritative sources and adopting a robust analytical framework.

Study problem:

Under the current laws of international law, may governments and non-state actors be held responsible for environmental harm resulting from cyber warfare in which they participate? The research article's format:

The first half of this study focuses on The first part looks at cyber warfare in the context of existing international law norms by discussing the idea of cyber warfare and its adherence to those norms. The second portion addresses... The rules governing international civil liability for environmental harm caused by cyber warfare, as well as international criminal liability for egregious environmental offenses brought by these wars, handle international responsibility for such harm.

Cyber Warfare under Current International Law Rules

A distinction must be made between cyberattacks that may occur on a country's information systems and are criminalized according to its domestic law, and cyber warfare, which is prohibited under international law, as the first concept is narrower than the second accordingly. The concept of cyber warfare has evolved in parallel with the rapid development of digital technologies and the increasing integration of information systems into the core functions of modern states. Originating from the field of cybernetics—traditionally defined as the science of control and communication in machines—cyber warfare reflects a transformation in the nature of conflict, where the battlefield has shifted from physical terrain to an intangible and transnational digital environment (Al-Saidi et al., 2024). In this context, cyberspace encompasses complex networks of communication systems, data infrastructures, and remote control mechanisms that enable both civilian and military operations. The strategic importance of these systems has rendered them critical targets in contemporary conflicts, thereby elevating cyber warfare to a central dimension of international security.

Despite its growing significance, cyber warfare remains conceptually ambiguous, with no universally accepted definition in legal or academic discourse. This definitional uncertainty stems from the diverse forms and objectives of cyber operations, which range from espionage and data manipulation to large-scale disruption of critical infrastructure. Some scholars conceptualize cyber warfare as covert and highly sophisticated operations conducted through advanced digital tools aimed at infiltrating, disrupting, or destroying information systems and technological infrastructures (Al-Saidi et al., 2024). Others emphasize its strategic dimension, defining it as the use of information-based capabilities to undermine an adversary's decision-making processes, operational capacity, and overall security environment (Arquilla & Ronfeldt, 1993).

From a military perspective, cyber warfare involves not only the execution of digital attacks but also the integration of information technologies into the planning, coordination, and management of military operations. This includes the deployment of interconnected systems such as sensors, communication networks, databases, and artificial intelligence tools, which collectively enhance the precision, speed, and effectiveness of modern warfare. As a result, cyber capabilities have become as strategically significant as conventional military assets, fundamentally altering the balance of power in international relations (Arquilla & Ronfeldt, 1993; Robinson et al., 2015).

A more state-centric definition views cyber warfare as actions undertaken by a state to penetrate or disrupt the information systems and networks of another state with the intention of causing significant damage or incapacitation (Abdul Ghaffar, 2016). However, this perspective has been increasingly challenged by the growing involvement of non-state actors, including private entities, hacker groups, and transnational organizations. Advances in technology and the widespread accessibility of cyber tools have enabled these actors to participate in cyber conflicts, thereby expanding the scope of cyber warfare beyond traditional state-to-state interactions (Farhat, 2021). This evolution has blurred the boundaries between warfare, crime, and hybrid conflict, complicating both legal classification and regulatory responses.

A common feature across most definitions is the targeting of information systems and digital infrastructures with the aim of compromising the confidentiality, integrity, or availability of data. Such operations may involve unauthorized access, data theft, system manipulation, or the complete disruption of critical services. The inherent anonymity of cyberspace, combined

with the technical complexity of cyber operations, makes it exceptionally difficult to identify perpetrators and establish accountability, thereby posing significant challenges for the application of international law (Qashti, 2024; Schmitt, 2014).

Cyber warfare differs fundamentally from traditional warfare in several respects. Conventional warfare is typically characterized by clearly defined actors, physical battlefields, and formal declarations of conflict. In contrast, cyber warfare operates across decentralized and borderless networks, often without clear temporal or spatial boundaries. Its objectives are frequently ambiguous, and its methods rely on digital tools that can be deployed remotely and instantaneously. These characteristics not only complicate the legal regulation of cyber warfare but also amplify its potential impact, particularly when critical infrastructure is targeted (Saud, 2018; Stevens, 2012).

Furthermore, the ongoing revolution in military affairs has significantly reshaped the nature of conflict by integrating cyber capabilities into broader strategic frameworks. This transformation has enhanced the destructive potential of both conventional and non-conventional weapons while simultaneously introducing new forms of conflict that operate below the threshold of traditional warfare. The emergence of so-called "gray zone" or "hybrid" conflicts, often characterized by continuous low-intensity cyber operations, reflects a shift toward persistent and multifaceted forms of confrontation (Farhat, 2021; Hadji-Janev, 2020).

Importantly, the environmental implications of cyber warfare represent a critical yet often overlooked dimension of this phenomenon. Cyberattacks targeting infrastructure systems—such as energy networks, water treatment facilities, and industrial control systems—can lead to significant environmental harm, including pollution, ecosystem degradation, and long-term ecological disruption. These consequences underscore the need to integrate environmental considerations into the conceptual and legal understanding of cyber warfare, thereby expanding its scope beyond purely security-related concerns (Cassotta & Pettersson, 2019; Schmitt, 2014).

In sum, cyber warfare constitutes a complex and evolving form of conflict that challenges traditional notions of warfare, legal responsibility, and environmental protection. Its multifaceted nature, characterized by technological sophistication, transnational reach, and the involvement of diverse actors, necessitates a comprehensive and interdisciplinary approach to its study and regulation. As cyber capabilities continue to advance, the need for clearer definitions, more robust legal frameworks, and greater international cooperation becomes increasingly urgent.

Cyberattacks are also large-scale, and herein lies their danger to the environment, as they have a significant impact on the vital interests of the state by targeting its infrastructure. Cyber warfare is based on the use of information and communication technology in an informational environment within an offensive or defensive military strategy adopted by a state, aiming to disrupt or control the enemy's resources. Its targets may affect both tangible and intangible areas, and the level of its severity may vary depending on the circumstances.(Robinson, Jones, &Janicke, 2015, p. 10)

The distinction between cyber warfare and broader forms of network-based conflict constitutes a foundational issue in contemporary security and legal scholarship. Cyber warfare is typically understood as state-centered conflict involving coordinated operations targeting strategic infrastructure and national security systems, whereas network warfare encompasses a wider spectrum of activities, including actions carried out by non-state actors, criminal organizations, and decentralized digital networks (Arquilla & Ronfeldt, 1993; Stevens, 2012). Despite these conceptual differences, both forms of conflict share a common capacity to generate large-scale disruption and pose significant risks to state stability and environmental integrity. Indeed, the increasing militarization of cyberspace, coupled with the development of autonomous and highly sophisticated cyber weapons, has blurred the boundaries between traditional warfare and digitally mediated conflict, thereby complicating both legal classification and regulatory responses (Krepinevich, 2012; Robinson et al., 2015).

The growing strategic reliance on cyberspace has prompted a gradual but notable shift in the position of states regarding the applicability of international law to cyber operations. While early debates questioned whether existing legal frameworks were suitable for governing cyber warfare, there is now a broad consensus that international law, including the principles of the United Nations Charter and international humanitarian law, applies to cyber activities conducted by states (Hadji-Janev, 2020; Schmitt, 2014). However, this acceptance remains accompanied by significant interpretative challenges, particularly concerning the classification of cyber operations as "use of force" or "armed attacks" within the meaning of Article 51 of the United Nations Charter (Melzer, 2011; Tsagourias & Buchan, 2015). These challenges are further exacerbated by the absence of binding international instruments specifically designed to regulate cyber warfare, leaving states to rely on non-binding frameworks such as the Tallinn Manual, which, although authoritative, reflects particular doctrinal perspectives and lacks universal acceptance (Schmitt, 2017; Robinson et al., 2015).

In this evolving legal landscape, state practices reveal divergent approaches to cyber governance, ranging from strict control of digital infrastructure to the integration of cyber capabilities into broader military strategies, as well as efforts to adapt existing international legal norms to the cyber domain (Hadji-Janev, 2020). These trends underscore the necessity of developing a coherent and universally accepted legal framework capable of addressing the unique characteristics of cyber warfare, including its transboundary nature, rapid escalation potential, and significant environmental implications (Harris, 2022; Dinniss, 2012).

The environmental dimension of cyber warfare represents a particularly critical yet underexplored aspect of this phenomenon. Cyber operations targeting critical infrastructure—such as energy systems, water treatment facilities, transportation networks, and industrial control systems—can result in severe and long-lasting environmental damage, even in the absence of direct physical destruction (Kallberg & Burk, 2013; Schmitt, 2014). For example, disruptions to dam control systems, power grids, or chemical plants may lead to flooding, toxic emissions, or large-scale pollution events, with devastating consequences for ecosystems and human populations (Kallberg & Burk, 2013; Cassotta & Pettersson, 2019). These impacts often extend beyond immediate damage, contributing to long-term ecological degradation, resource depletion, and environmental instability.

A key characteristic of cyber-induced environmental harm is its indirect and immaterial nature. Unlike conventional environmental damage caused by physical force, cyberattacks typically target digital systems that control or regulate environmental processes, thereby creating complex causal chains between the initial act and its environmental consequences (Mohammed, 2022; Rakha, 2024). This indirectness complicates the process of establishing causation, which remains a fundamental requirement for triggering international responsibility (International Law Commission, 2001). Moreover, the speed and scale at which cyberattacks can propagate across interconnected systems amplify their potential impact, enabling widespread environmental damage within a relatively short period (Robinson et al., 2015).

From a legal perspective, the determination of international responsibility for environmental harm caused by cyber warfare raises profound challenges. The concept of internationally wrongful acts, as articulated by the International Law Commission, provides a general framework for attributing responsibility to states; however, its application in cyberspace is hindered by the inherent difficulties of attribution and the complexity of cyber operations (ILC, 2001; Schmitt, 2017). In many cases, cyberattacks involve multiple actors, including state and non-state entities, operating across different jurisdictions, thereby complicating the identification of responsible parties and the allocation of liability (Kallberg & Burk, 2013; Chabinsky, 2021).

Within this context, international civil liability emerges as a crucial mechanism for addressing environmental damage caused by cyber warfare. Such liability is based on the existence of an unlawful act, environmental harm, and a causal link between the two (Mohammed, 2022; Lagmash, 2017). Notably, the concept of environmental harm has evolved to encompass not only physical destruction but also indirect impacts, including the disruption of environmental monitoring systems and the loss of critical environmental data necessary for risk assessment and disaster prevention (United Nations, 2001; Katagiri, n.d.). This expanded understanding reflects the changing nature of environmental risks in the digital age and highlights the need for adaptive legal frameworks capable of addressing both tangible and intangible forms of harm.

Ultimately, the increasing complexity of cyber warfare and its environmental consequences underscores the inadequacy of existing legal frameworks and the urgent need for reform. Addressing these challenges requires the development of specialized international norms, enhanced mechanisms for attribution and accountability, and greater integration of environmental considerations into cyber governance strategies (Schmitt, 2014; Tsagourias & Buchan, 2015). Without such efforts, the international community risks facing a growing gap between the realities of cyber conflict and the legal tools available to regulate its environmental impact.

cause-and-effect connections Representing a point of convergence between the needs of law and physical and scientific theories, it is an entirely scientific, not a legal, topic. It entails analyzing the degree of connection between actual facts and events and a potential result, as well as providing a logical conclusion to a legal question based on them. Nevertheless, these sciences are unable to establish the existence of this link with absolute certainty. It is the A In the environmental area, it is challenging to establish the clear and direct link between cause and effect, particularly as a consequence of cyber operations, but it is also difficult to show that this connection adheres to established general principles (Lagmash, 2017, p. 198)

And taking into account that Due to the dispersed nature of cyberwar attacks and the challenges in pinpointing their origin, it is more difficult to demonstrate the causal connection in cyberwarfare attacks than in traditional acts.

Establishing a causal relationship between a cyber operation and the resulting environmental harm represents a complex and methodologically demanding process that integrates both legal reasoning and advanced scientific analysis. In contrast to conventional forms of environmental damage, where causal links may be directly observable, cyber-induced harm requires a multi-layered evidentiary approach grounded in digital forensics and environmental science. The process begins with the technical examination of digital data, including the tracing of data transmission pathways, the analysis of network logs, and the identification of malicious software used in the cyberattack. These procedures are essential for reconstructing the sequence of events and determining the operational mechanisms through which the cyber incident translated into physical environmental consequences (AllahRakha, 2024).

However, the establishment of causation does not rely solely on digital evidence. It must also be supported by scientifically rigorous environmental assessments designed to measure the extent and nature of the harm. This includes the systematic collection and analysis of environmental samples—such as air, water, and soil—both prior to and following the cyber incident. Such assessments are conducted in accordance with internationally recognized scientific standards to ensure their reliability, objectivity, and admissibility in legal proceedings. The integration of digital forensic analysis with empirical environmental

data is therefore critical for substantiating claims of environmental damage and for meeting the evidentiary thresholds required in international dispute resolution and judicial processes (Al-Rubaiee & Al-Owaidi, 2022; Mohammed, 2022).

Within this analytical framework, the attribution of environmentally harmful cyber operations emerges as one of the most challenging issues in contemporary international law. The inherent characteristics of cyberspace—particularly anonymity, decentralization, and the capacity for technical obfuscation—enable perpetrators to conceal their identity and obscure the origin of attacks. Techniques such as IP address spoofing, the use of botnets, and the deployment of proxy servers significantly complicate efforts to trace cyber operations to specific actors. As a result, establishing legal responsibility for cyber-induced environmental harm is often hindered by the difficulty of obtaining clear and conclusive attribution (Melzer, 2011; Schmitt, 2017).

The framework for attributing cyber operations to states is primarily derived from the principles articulated in the Draft Articles on Responsibility of States for Internationally Wrongful Acts adopted by the International Law Commission. According to these principles, a state incurs international responsibility when an act or omission attributable to it constitutes a breach of an international obligation (International Law Commission [ILC], 2001). In the context of cyber warfare, attribution may arise under several conditions, the most straightforward of which is direct attribution. This occurs when the cyber operation causing environmental harm is conducted by official state organs, including military cyber units or intelligence agencies acting within their institutional mandates.

Direct attribution is particularly relevant in cases where state authorities explicitly authorize or conduct cyber operations targeting environmentally sensitive infrastructure. For instance, cyberattacks directed at water treatment facilities, energy systems, or environmental monitoring networks may be attributable to the state if they are executed by governmental actors or under formal command structures. In such scenarios, the existence of official orders, operational directives, or documented involvement of state agencies serves as key evidence in establishing responsibility (Mshrf, 2022; Schmitt, 2017). Nevertheless, even in cases of apparent direct involvement, the evidentiary burden remains substantial, requiring a combination of technical, legal, and intelligence-based proof to satisfy international legal standards.

Beyond direct attribution, the complexity of cyber operations often necessitates consideration of indirect forms of responsibility, including situations where states exercise control over non-state actors or fail to prevent harmful activities originating from their territory. These dimensions further illustrate the evolving nature of international responsibility in cyberspace and highlight the need for more refined legal frameworks capable of addressing the unique challenges posed by cyber-induced environmental harm (Chabinsky, 2021; Tsagourias & Buchan, 2015).

Overall, the interplay between technical evidence, scientific validation, and legal standards underscores the multidisciplinary nature of establishing responsibility for environmental damage caused by cyber warfare. It also reveals significant gaps in current international law, particularly in relation to attribution, causation, and evidentiary requirements, thereby reinforcing the urgency of developing more comprehensive and adaptive regulatory approaches.

Table 1. Conceptual Framework of Cyber Warfare and Environmental Impact

Component	Type of Variable	Description	Key Mechanisms	Impact Level
Cyber Warfare Activities	Independent Variable	Digital military operations targeting systems, networks, and infrastructure	- Malware attacks - System infiltration - Infrastructure disruption	High (Trigger factor)
Critical Infrastructure Disruption	Mediating Variable	Breakdown of essential systems (energy, water, transport, industry)	- Power grid failure - Water system disruption - Industrial control system malfunction	Very High
Environmental Damage	Dependent Variable	Direct and indirect harm to natural ecosystems	- Pollution (air, water, soil) - Toxic leakage - Ecosystem destruction	Severe / Long-term
Attribution Capability	Moderating Variable	Ability to identify responsible actors in cyberspace	- Technical tracing - Digital forensics - Intelligence cooperation	Weakens/Strengthens accountability

Legal Framework Strength	Moderating Variable	Effectiveness of international law in regulating cyber warfare	- International humanitarian law - Tallinn Manual - State responsibility rules	Conditional
International Responsibility	Outcome Variable	Legal consequences for environmental harm	- Civil liability (compensation) - Criminal liability (ICC) - State accountability	Final outcome

Table 2. Key Findings and Legal Implications of Cyber Warfare on the Environment

Finding	Explanation	Legal Implication	Policy Implication
Cyber warfare causes indirect but severe environmental damage	Damage occurs through disruption of infrastructure rather than direct physical attack	Expands interpretation of environmental harm under international law	Need to include cyber risks in environmental protection policies
Attribution is the main legal challenge	Difficulty in identifying perpetrators due to anonymity of cyberspace	Weakens application of state responsibility principles	Requires development of advanced cyber attribution mechanisms
Existing international law is insufficient	Current frameworks were designed for traditional warfare	Legal gaps in regulating cyber-induced environmental harm	Necessity for new international treaties or protocols
Critical infrastructure is highly vulnerable	Energy, water, and industrial systems are primary targets	Protection of civilian infrastructure becomes a legal priority	Strengthening cybersecurity of environmental infrastructure
Civil liability mechanisms are underdeveloped	Compensation frameworks are unclear in cyber context	Need for clearer standards of liability and compensation	Establish international compensation mechanisms/funds
Criminal liability is limited but evolving	Environmental cyber crimes may fall under ICC jurisdiction	Expansion of environmental crimes (e.g., ecocide concept)	Support international recognition of cyber environmental crimes
Environmental damage is long-term and transboundary	Effects extend beyond borders and persist over time	Requires international cooperation and shared responsibility	Promote global governance and joint response systems

The attribution of cyber operations in the context of environmental harm presents one of the most complex challenges in contemporary international law, particularly when state responsibility is examined in relation to indirect forms of involvement. Indirect attribution arises in situations where a state does not directly conduct a cyber operation but provides support, coordination, or direction to non-state actors or affiliated groups engaged in disruptive cyber activities. In such cases, the conduct may be legally attributable to the state if it can be demonstrated that these actors operated under its effective control or direction, or if the state conferred upon them elements of official authority through formal or informal arrangements . However, establishing such attribution remains highly problematic in practice, as it requires substantial evidentiary support, including technical data, communication records, and verifiable links between state authorities and non-state entities.

In parallel, international law recognizes the principle of due diligence, whereby a state may incur responsibility not only for direct or indirect actions but also for its failure to prevent harmful activities originating from its territory or infrastructure. This "breach of the duty of due care" occurs when a state neglects to take reasonable and necessary measures to prevent cyber operations that result in environmental damage to other states. The application of this principle is grounded in the broader obligation of states to ensure that activities within their jurisdiction do not cause transboundary harm. Nevertheless, proving such a breach requires demonstrating that the state was aware, or should reasonably have been aware, of the risk of such cyberattacks and failed to implement adequate technical, legislative, or cooperative measures to mitigate them. This evidentiary burden further complicates the enforcement of international responsibility in cyberspace.

These attribution standards are closely linked to the established doctrines of effective control and effective will, which have traditionally been applied in the context of armed conflicts involving non-state actors. Their application in cyberspace necessitates both material and legal assessments, including the evaluation of financial support, operational coordination, training, and communication channels, as well as the existence of formal or quasi-formal relationships between states and cyber actors. The complexity of these assessments underscores the urgent need for the development of specialized legal frameworks capable of addressing the unique characteristics of cyber operations and their environmental consequences.

Moreover, cyber operations conducted by non-state actors, such as private entities, organized groups, or individuals, do not automatically engage state responsibility unless a sufficient degree of state involvement can be established. Nevertheless, such actors may still be subject to prosecution under national or international legal systems where jurisdictional and legal conditions permit. This reflects the growing recognition that accountability for environmental harm in cyberspace must extend beyond traditional state-centric models and incorporate a broader range of actors.

The legal consequences of environmental damage caused by cyber warfare are primarily articulated through the framework of international civil liability, which seeks to ensure the cessation of harmful acts and the provision of appropriate remedies. This includes the obligation to halt ongoing cyber operations and to take immediate measures to mitigate their effects, such as restoring compromised systems and stabilizing affected ecosystems. Additionally, responsible parties are required to undertake restorative actions aimed at re-establishing environmental conditions as close as possible to their original state. These measures play a crucial role in enhancing environmental resilience and reducing the likelihood of future harm.

Financial compensation constitutes another essential dimension of civil liability, requiring responsible actors to cover the costs associated with environmental restoration, resource degradation, and the broader socio-economic impacts of environmental damage. This may include compensation for the loss of natural resources, deterioration of environmental quality, and harm suffered by affected populations. Such mechanisms are vital for ensuring justice and reinforcing the principle of accountability in cases of cyber-induced environmental harm.

At the same time, international criminal law is increasingly being invoked as a mechanism for addressing severe environmental damage resulting from cyber operations. While cyberattacks are not explicitly defined as international crimes, their consequences may fall within the scope of existing categories such as war crimes or crimes against humanity, particularly when they result in widespread, long-term, and severe environmental harm. The growing discourse surrounding the recognition of environmental crimes, including the emerging concept of ecocide, reflects a broader shift toward strengthening legal protections for the environment in both physical and digital domains.

Empirical Evidence and Case-Based Analysis

Although cyber warfare is often characterized by the absence of publicly available quantitative datasets, a growing body of documented cyber incidents provides valuable empirical evidence regarding its environmental implications. This study incorporates a case-based empirical analysis of major cyber incidents targeting critical infrastructure, illustrating how cyber operations can produce direct and indirect environmental harm.

One of the most frequently cited cases is the Stuxnet cyberattack (2010), widely attributed to state-sponsored actors targeting Iran's nuclear facilities. While the primary objective of the attack was to disrupt uranium enrichment processes, the operation demonstrated the capacity of cyber tools to interfere with industrial control systems governing sensitive technological environments. By manipulating centrifuge operations, Stuxnet caused physical degradation of equipment, highlighting the potential for cyber operations to trigger environmental risks, particularly in nuclear or chemical facilities where system failures may lead to hazardous leakage or contamination (Kushner, 2013; Zetter, 2014).

Another significant case is the Ukraine power grid cyberattacks (2015–2016), which resulted in large-scale electricity outages affecting hundreds of thousands of civilians. These attacks targeted supervisory control and data acquisition (SCADA) systems, disrupting energy distribution networks. While the immediate consequence was a loss of electricity, the broader implications included risks to environmental safety systems, such as the failure of water treatment plants and disruption of environmental monitoring processes. These incidents illustrate how cyberattacks on energy infrastructure can indirectly contribute to environmental degradation and public health risks (Lee, Assante, & Conway, 2016; E-ISAC, 2016).

A further example can be observed in cyber incidents targeting water treatment facilities, such as the attempted breach of a water treatment plant control system in Florida (2021). In this case, attackers sought to manipulate chemical levels in the water supply by remotely accessing operational systems. Although the attack was detected and neutralized before causing harm, it provides concrete evidence of how cyber intrusions can directly threaten environmental quality and human health through the contamination of essential resources (CISA, 2021).

In addition, cyber operations targeting oil and gas infrastructure have demonstrated the environmental risks associated with industrial system disruption. Attacks on pipeline control systems or refinery operations can lead to system malfunctions, oil spills, or gas leaks, thereby causing significant ecological damage. For instance, ransomware attacks on energy companies have raised concerns about the vulnerability of critical infrastructure and the potential for environmental disasters resulting from compromised operational integrity (Greenberg, 2019).

From an analytical perspective, these cases confirm the causal chain proposed in the conceptual framework of this study. Cyber warfare activities targeting critical infrastructure act as the primary trigger, leading to system disruption and operational failure. These disruptions, in turn, create conditions for environmental damage, either directly through the release of hazardous materials or indirectly through the breakdown of monitoring and control systems. The severity of the environmental impact is influenced by moderating factors such as the resilience of infrastructure systems, the effectiveness of cybersecurity measures, and the capacity of states to respond to cyber incidents.

Despite these insights, the empirical analysis also reveals significant limitations. The attribution of cyber incidents remains highly contested, with many cases lacking definitive public evidence linking attacks to specific state actors. This reinforces the argument that attribution challenges continue to undermine the enforcement of international responsibility. Furthermore, the absence of standardized reporting mechanisms for cyber-induced environmental harm limits the availability of comprehensive datasets, highlighting the need for improved international cooperation in data sharing and incident documentation.

Overall, the empirical evidence demonstrates that cyber warfare is not merely a digital phenomenon but a tangible source of environmental risk. The analyzed cases provide concrete support for the study's central hypothesis that cyber operations targeting critical infrastructure can lead to significant environmental damage, thereby necessitating the development of more robust legal and regulatory frameworks to address this emerging threat.

Characterization of environmental crimes as crimes under the Statute of the International Criminal Court

Although international criminal law does not explicitly mention cyber-attacks, digital means are merely a "tool" for committing the criminal act. In the case of disabling the cooling systems of a nuclear power plant through a cyber-attack, the act falls within the scope of an environmental crime even if the means are digital (Schmitt, 2017, p. 326).

The International Criminal Court cannot consider environmental crimes if they fall within the framework of a war crime, a crime against humanity, or genocide, whenever committed under circumstances that fulfill the elements of these crimes (Rome Statute of the International Criminal Court, 1998, Art. 8/2b).

Accordingly, contemporary international legal scholarship seeks to establish the concept of environmental crimes as international crimes, by defining the legal framework that ensures their inclusion within the subject-matter jurisdiction of the International Criminal Court.

The characterization of environmental crimes is based on two essential elements: first, the occurrence of widespread and severe environmental damage, and second, the presence of criminal intent manifested in knowledge and deliberate causation of serious harm to the natural environment. For example, certain acts such as the deliberate use of contaminated weapons leading to widespread pollution of water, air, or soil are considered war crimes when linked to an armed conflict and taking on a hostile military character(Bin Makhlouf, 2019, pp. 76–78)

International humanitarian law already includes explicit references to environmental protection during armed conflicts, as in Article 8 of the Rome Statute, which criminalizes widespread and long-term damage to the natural environment when criminal intent is established(Al-Azzawi, 2022, p. 238).In addition,Classifying an act as an international environmental crime requires specific conditions: the damage must be widespread, long-term, and serious, and it must be caused by a deliberate act, not merely by negligence or oversight.(Abdul Hussein, 2024, p. 55)

In this context, recent years have witnessed several initiatives aimed at including the crime of "ecocide" as a fifth crime within the Rome Statute, through the formulation of a precise definition and objective criteria for the elements of gravity, criminal intent, and the international nature of the crime, in response to global environmental challenges and the urgent need to provide international criminal protection for the environment as a fundamental collective interest(Mwanza, 2023, p. 190)

Therefore, it can be said that the legal classification of environmental crimes within the framework of the International Criminal Court is characterized by a degree of flexibility that allows for their inclusion under existing texts whenever the objective conditions are met, with a growing trend in international jurisprudence and legislation towards enshrining more explicit and clear protection for the environment at the highest international judicial levels.

Criminal penalties for environmental crimes before the International Criminal Court

The court relies on the severity associated with the environmental act, the perpetrator's behavior, and the availability of specific criminal intent (such as intentional harm with widespread, long-term effects on the environment and humans) in imposing penalties. These penalties include:

Imprisonment for fixed periods: This may reach thirty years or life imprisonment in crimes with catastrophic consequences, as stated in Article 77/1 of the Basic Law(Rome Statute of the International Criminal Court, 1998, art. 77/1)

- Financial penalty: The court has the right to impose a fine, the amount of which is determined by the court according to the value of the environmental crime's damage and its ongoing impact(Bin Makhlouf, 2019, p. 84)

- Confiscation and financial measures: It is permissible to order the confiscation of funds, assets, and materials used in the environmental crime and the profits generated therefrom, while obligating the perpetrator to pay compensation to the victims or restore the situation to its previous state(Al-Azzawi, 2022, p. 242)The court may impose reparative measures and restoration measures, especially concerning crimes whose harm affects victims collectively and has long-term effects, such as rehabilitating the damaged land, repairing the water system, and providing health and environmental rehabilitation for the affected local communities(Minkovap. 11)This is stipulated in Article 75 of the Court's Statute regarding "Orders related to reparation" and the establishment of a special fund for compensating victims. Compensation may, as much as possible, include repairing the deteriorated environmental situation.(Rome Statute of the International Criminal Court, 1998, art. 75)

Conclusion and Policy Recommendations

The growing intersection between cyber warfare and environmental harm represents one of the most pressing challenges confronting contemporary international law. The findings of this study demonstrate that cyber operations, while conducted in a non-physical domain, are capable of producing significant and often irreversible environmental consequences through the disruption of critical infrastructure and essential ecological systems. As the scale, sophistication, and frequency of cyber conflicts continue to increase, the risks posed to environmental sustainability and human security are becoming more pronounced, thereby necessitating a comprehensive legal and institutional response.

A central conclusion of this research is that the distinction between cyber warfare and ordinary cyberattacks is of critical importance, as it directly influences the applicability of international legal norms, particularly those governing the conduct of hostilities and the attribution of international responsibility. The absence of a universally accepted definition of cyber warfare contributes to legal ambiguity and undermines the consistent application of international humanitarian and environmental law. Furthermore, the expansion of environmental damage in the cyber context—extending beyond physical destruction to include non-material harm such as the disruption of environmental monitoring systems and the loss of critical environmental data—requires a reconceptualization of environmental harm within international legal frameworks.

The study also highlights the persistent difficulties associated with attribution in cyberspace, which remain a fundamental obstacle to effective accountability. The technical characteristics of cyber operations, including anonymity, decentralization, and the involvement of non-state actors, significantly complicate the process of identifying responsible parties and applying existing doctrines of state responsibility. As a result, the current legal framework appears insufficient to address the complexity of cyber-induced environmental harm, thereby creating gaps in both civil and criminal accountability mechanisms.

At the level of international criminal law, the analysis reveals a growing trend toward expanding the legal recognition of environmental crimes, including those facilitated by cyber operations. While existing provisions within the Rome Statute provide a degree of flexibility that allows certain acts to be prosecuted under established categories, there is an increasing need to explicitly recognize severe environmental harm—potentially including cyber-induced damage—within the framework of international criminal justice. The emerging discourse surrounding the codification of ecocide reflects this evolving normative landscape and underscores the importance of strengthening legal protections for the environment.

In light of these findings, it becomes evident that addressing the environmental consequences of cyber warfare requires a multidimensional and forward-looking approach. There is a clear need for the development of specialized international legal rules that take into account the unique characteristics of cyberspace, particularly with regard to attribution, causality, and the scope of environmental harm. Strengthening international cooperation is equally essential, especially in areas such as technical information exchange, joint cyber defense mechanisms, and coordinated responses to environmental cyber incidents. Such cooperation would enhance the ability of states to detect cyber threats, accurately attribute responsibility, and respond effectively to environmental damage.

Moreover, the establishment of international compensation mechanisms, including dedicated funds supported by states and relevant private actors, could play a crucial role in addressing the financial and ecological consequences of cyber-induced environmental harm. Preventive measures must also be prioritized through the modernization of digital infrastructure and the integration of environmental considerations into national cybersecurity strategies. This includes the development of environmental cybersecurity policies aimed at protecting critical infrastructure and minimizing the risk of large-scale ecological disruption.

Ultimately, the protection of the environment in the age of cyber warfare requires a fundamental rethinking of traditional legal approaches and the adoption of integrated governance frameworks that bridge the gap between cybersecurity, environmental protection, and international law. Only through such comprehensive and coordinated efforts can the international community effectively respond to the evolving challenges posed by cyber warfare and ensure the sustainable protection of environmental resources for future generations.

Ethical Approval and Consent to Participate

This study does not involve human participants, human data, or animal subjects. Therefore, ethical approval and consent to participate were not required. The research is based entirely on publicly available legal documents, scholarly literature, and secondary data sources.

Consent for Publication

All authors have read and approved the final version of the manuscript and consent to its publication.

Availability of Data and Materials

The data supporting the findings of this study are derived from publicly accessible sources, including international legal documents, academic publications, and documented cyber incidents. No proprietary datasets were used. Additional information can be provided by the corresponding author upon reasonable request.

Competing Interests

The authors declare that they have no competing financial or non-financial interests that could have influenced the work reported in this paper.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Authors' Contributions

Brahmi Hanane contributed to the conceptualization, literature review, legal analysis, and drafting of the manuscript. Noureddine Khouidem contributed to the methodology, analytical framework, critical revision, and final approval of the manuscript. All authors have read and approved the final version of the manuscript.

Acknowledgements

The authors would like to express their appreciation to their respective academic institutions for providing a supportive research environment. No external institutional or financial support was received for this study.

Data Availability Statement

All data used in this study are publicly available and properly cited within the manuscript. No datasets were generated or analyzed that require restricted access.

Declaration of AI Use

The authors declare that artificial intelligence tools were used solely for language editing and formatting purposes. All intellectual content, analysis, and conclusions are the original work of the authors.

References:

1. Abdul Ghaffar, F. (2016). *Electronic warfare*. Al-Janadriyah Publishing and Distribution.
2. Abdul Hussein, A. (2024). The legal nature of the crime of environmental terrorism according to international law. *Journal of Sharia and Legal Studies*, 669, 55–70.
3. Abu Alnofal, W. A. (2022). The applicable law to civil liability arising from cybercrime. *International Journal of Doctrine, Judiciary and Legislation, 12*(2), 45–49.
4. Al-Azzawi, A. R. (2022). The authority of referral and prosecution before the International Criminal Court according to the Rome Statute of 1998. *Journal of Legal Sciences, University of Baghdad, 37*(1), 238–242.
5. Al-Rubaiee, A.-K. H., & Al-Owaidi, M. R. A. (2022). Assessment of heavy metal contamination in urban soils of selected areas in Hilla City, Babylon, Iraq. *Iraqi Journal of Science, 63*(4), 108–120.
6. Al-Saidi, M. R. M., Abdul Latif, M. S. M., & Muhammad, A. R. M. (2024). The impact of artificial intelligence and cyber warfare on the human environment during armed conflicts. *Journal of Jurisprudential and Legal Research*, 47, 3853–3855.
7. Arquilla, J., & Ronfeldt, D. (1993). *Cyberwar is coming!* RAND Corporation.
8. Bin Makhlouf, A. R. (2019). Environmental crimes before the International Criminal Court: Criminalization and punishment. *Journal of Legal Sciences*, 203, 76–84.
9. Bustany, T. A., & Muhammad, S. R. (2020). Control over crime theory in the Rome Statute. *QalaaiZanist Journal, 5*(2), 525–540.
10. Cassotta, S., & Pettersson, M. (2019). Climate change, environmental threats and cyber threats to critical infrastructures: A multi-regulatory approach. *Beijing Law Review, 10*(3), 624–640.
11. Chabinsky, M. S. (2021). Cyber due diligence: A patchwork of protective obligations in international law. *European Journal of International Law, 32*(3), 780–802.

12. Farhat, A. E.-D. (2021). From nuclear deterrence to cyber deterrence: A study of the effectiveness of deterrence in cyberspace. *Al-Mufakker Journal, 16*(1), 267–280.
13. Hadji-Janev, M. (2020). The legality of cyberwar: From revolution to evolution. *International Journal of Cyber Diplomacy, 1*(1), 18–30.
14. Harris, D. A. (2022). Cyber warfare readiness in the maritime environment. In *Proceedings of the 24th International Conference on Enterprise Information Systems* (p. 123).
15. International Law Commission. (2001). *Draft articles on responsibility of states for internationally wrongful acts*. United Nations.
16. Kallberg, J., & Burk, R. A. (2013). *Conflict and cooperation in cyberspace*. Routledge.
17. Katagiri, N. (n.d.). *Cybersecurity and international relations* (p. 7).
18. Krepinevich, A. F. (2012). Cyber warfare as a "nuclear option." *Center for Strategic and Budgetary Assessments*, 94–105.
19. Lagmash, M. L. (2017). The basis of international responsibility arising from environmental pollution. *Journal of Research in Law and Political Science, 3*(2), 198–210.
20. Melzer, N. (2011). *Cyberwarfare and international law*. Geneva Academy of International Humanitarian Law.
21. Minkova, L. G. (n.d.). *Cybersecurity and international law* (p. 11).
22. Mohammed, A. (2022). Civil liability for environmental damages of oil and gas companies in light of international laws and agreements. *Erbil Polytechnic University Journal of Humanities and Social Sciences, 5*(2), 987–997.
23. Mshrf, A. (2022). The applicable law to civil liability arising from cybercrime. *International Journal of Doctrine, Judiciary and Legislation, 3*(3), 45–49.
24. Mwanza, R. (2023). The right to a healthy environment as a catalyst for the codification of the crime of ecocide. *Cambridge Journal of International Law*, 190–210.
25. Qashti, N. A. F. (2024). Cyber warfare and ways to confront it. *Strategic Affairs Magazine*, 17, 491–500.
26. Rakha, N. A. (2024). Transformation of cybercrimes in the digital age. *International Journal of Legal and Policy Studies, 3*(2), 156–170.
27. Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security, 49*, 70–94.
28. Rome Statute of the International Criminal Court. (1998).
29. Saud, Y. Y. (2018). Cyber warfare in light of the rules of international humanitarian law. *Legal Journal, 4*(4), 84–95.
30. Schmitt, M. N. (2014). Rewired warfare: Rethinking the law of cyber attack. *International Review of the Red Cross, 96*(893), 191–223.
31. Schmitt, M. N. (2017). Attribution of cyber operations to states. In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (pp. 67–70, 145). Cambridge University Press.
32. Simon, G. (2023). Cyber warfare: Taking war to cyberspace and its implications for international humanitarian law. *International Journal for Multidisciplinary Research, 11*(1), 668–669.
33. Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy, 33*(1), 148–170.
34. United Nations. (2001). *International Law Commission draft on responsibility of states*.
35. Dinniss, H. (2012). *Cyber warfare and the laws of war*. Cambridge University Press.
36. Tsagourias, N., & Buchan, R. (2015). *Research handbook on international law and cyberspace*. Edward Elgar.
37. Rid, T. (2020). *Active measures: The secret history of disinformation*. Farrar, Straus and Giroux.
38. Jensen, E. T. (2017). Cyber warfare and international law. *Texas Law Review, 95*(3), 1–35.
39. Boothby, W. H. (2012). *Weapons and the law of armed conflict*. Oxford University Press.