SRIWIJAYA CRIMEN AND LEGAL STUDIES
FACULTY OF LAW UNIVERSITAS SRIWIJAYA
Jalan Srijaya Negara, Palembang, 30139, Indonesia
Email: scls@fh.unsri.ac.id
http://journal.fh.unsri.ac.id/index.php/SCLS/index
E-ISSN: 2987-7350 P-ISSN: 2986-6367

FROM ATTRIBUTION TO COMPENSATION: DEFINING INTERNATIONAL CIVIL RESPONSIBILITY FOR CYBER ATTACKS

Shaker Al akayleh

Faculty of Law, University of Debrecen, Hungary. E-mail: shaker_akayleh@yahoo.com

Article

Keywords:

Civil; Cyber Attack; Responsibility; International; Compensation.

DOI: 10.28946/scls.v3i2.5144

Abstract

Humanity today, and those who will come after us, are aware of the consequences of cyberattacks, and the absence of international civil liability in the face of these attacks has become clear and evident. All countries must come together at one table to discuss the issue of this era: regulating cyberattacks and establishing the necessary legislation. The research problem in this paper is summarized in the absence of civil liability for cyberattacks, both theoretically and practically. Therefore, the aim of this paper is to bring the concept of civil liability for cyberattacks, its components, the provisions of international civil liability related to cyberattacks, the effects of its application, and how to assign civil liability to the perpetrators of cyberattacks from absence to actual reality and to put it into the framework of practical application to stop cyberattacks. This is a first step for any researcher in this field.

This is an Open Acces Research distributed under the term of the Creative Commons Attribution Licencee (https://Creativecommons.org/licences/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original works is properly cited.

A. INTRODUCTION

Cyberattacks have become a prominent global challenge, targeting critical infrastructure, public institutions, the private sector, and individuals. They exploit digital vulnerabilities to inflict significant economic, social, military, and political damage. These attacks may be perpetrated by governmental or non-governmental actors, or by anonymous individuals. . They are characterized by their transnational nature, the difficulty in tracing them, and their diverse forms, such as ransomware. There is an urgent need to quickly establish civil liability in response to these incidents, as the situation is not only evolving but rapidly escalating. Despite this, international law lacks a clear and coherent legal framework governing civil liability for damages resulting from cyberattacks. Most studies have focused on the criminal aspects of cyberattacks targeting individuals, institutions, and sensitive entities, creating a significant gap in the civil sphere, particularly regarding compensation, its forms, and the obligations of states. Therefore, the research problem addressed in this paper is the gap that has emerged regarding "civil liability for cyberattacks," both theoretically and practically.

This paper aims to clarify the concept of civil liability, explore the possibility of applying legal principles and rules to such incidents, understand the legal implications of establishing a civil liability system, and address international civil liability in the event of a cyberattack. It is essential to identify legal gaps and develop analytical legal frameworks that contribute to establishing a solid foundation for civil liability. This can be achieved through comprehensive strategies encompassing national legislation and international agreements, as well as setting standards and controls that define state responsibility, ensuring justice and compensation for victims of cyberattacks.

This paper also contributes to fostering international understanding through cooperation and information exchange among countries to effectively combat cyber threats. This collaborative effort is essential to address the escalating cyberattacks and ensure civil liability, justice, compensation, and accountability in the face of increasing cyber threats and their perpetrators. This research is limited to civil liability and does not extend to criminal prosecution or the technical aspects of the cyber operation.

B. RESEARCH METHODS

This study adopted an inductive research approach, beginning with the analysis of specific international legal texts, scholarly opinions, and state practices, and culminating in conclusions regarding the applicability of civil liability to cyberattacks. The research is primarily based on jurisprudential legal analysis, examining the rules, principles, and interpretations contained in international conventions, United Nations documents, and recognized non-binding legal instruments such as the Tallinn Manual.

To ensure a rigorous methodology, the researcher selected sources based on clear criteria. Primary sources included international resolutions, treaties, and intergovernmental declarations concerning civil liability and cyber operations. Secondary sources, such as academic books, graduate theses, and peer-reviewed articles, were used based on their scholarly rigor and contribution to international cyber law. Through legal analyses and internationally agreed-upon interpretations, the researcher identified widely accepted legal opinions and commentaries.

C. ANALYSIS AND DISCUSSION

1. The Concept of International Responsibility

The concept of international responsibility has evolved from the stage where only states were considered the sole entities bearing international responsibility. Later, international organizations were added to this framework after being recognized as legal personalities. Perhaps the legal arena may witness the addition of individuals as entities subject to civil accountability. However, what remains constant is that international responsibility has become one of the stable and firmly established principles in international law. To define the concept of international responsibility, it is essential to delve into its definition, followed by an explanation of its legal basis according to legal jurisprudential theories.

a. Definition of International Responsibility:

There are two trends: the traditional narrow understanding of international responsibility and a broader perspective based on the legitimacy or illegitimacy of the act causing harm to the victim states. These are:

1) Traditional Trend: This perspective views international responsibility as arising from the violation of a rule of international law. According to this trend, international responsibility is defined as "a legal bond that arises when there is a breach of an international commitment

by the person violating the commitment, and the person who suffers as a result of this breach has the right to demand compensation. The person responsible must also take measures to remedy the consequences of their actions"[1] or "a legal situation binding states attributed to committing an unlawful act under international law to compensate the state that faces this act".

2) The Second Trend : The modern and broad trend considers any action causing harm to other states as a reason for the state's responsibility from which the harmful act originated.[2] According to this perspective, international responsibility is defined as "a set of legal rules governing any act or incident attributed to any legal person under international law, resulting in harm to another person under international law and the consequent obligation of the first person to compensate"[3] It is also defined as "the legal penalty for a violation by any legal person under international law of one of its international obligations or for the harm caused by their act resulting.

From a hazardous activity stipulated for punishment by an international agreement.[4] International jurisprudence and judicial precedents have played a significant role in shaping the concept of international responsibility. This includes holding a state responsible for the failure of its entities to fulfil international obligations, causing harm to foreigners. Responsibility, in this context, implies compensation as a penalty for the failure to comply with international obligations. Additionally, a state may be held accountable when obligated to compensate other affected states.[5] The study argues that the modern trend, which broadens the concept of international responsibility and expands its scope to include all legal persons under international law, deserves approval and praise. This approach is closer to achieving justice and the goal of establishing rules of international responsibility primarily based on compensating for damages, without considering the legitimacy or illegitimacy of the committed act that caused harm under international.

b. The foundation of international responsibility:

Is closely tied to establishing the legal bases upon which it relies. The most significant theories that constitute the basis of international responsibility can be summarized as follows:

1) Fault Theory:

This theory is one of the oldest in international responsibility, with international jurisprudence playing a key role in transferring it from domestic legal systems to the international legal framework.[6] The theory posits that a state must commit a wrongful act, whether intentional or negligent, against another state. Negligence occurs when a state fails to exercise due diligence to prevent harm to other states or if the ruling authority does not impose

[1] Mukhlid Irhkais Al-Tarawneh, *The Mediator in Public International Law*, 2nd ed. (Jordan: Dar Wael for Publishing and Distribution, 2015), 589.
[2] Al-Attiyah Essam, *Public International Law* (Baghdad: Al-Nahda Library Publications, 2008), 517.
[3] Salah El-Din Amer, *Introduction to the Study of Public International Law*, 1st ed. (Cairo: Dar Al-Nahda Al-Arabiya Publications, 2003), 779–87.
[4] Amjad Heikal, *International Individual Criminal Responsibility before International Criminal Justice: A Study within the Framework of International Humanitarian Law*, 1st ed. (Cairo: Dar Al-Nahda Al-Arabiya Publications, 2009), 131–32.
[5] Permanent Court of International Justice, Factory at Chorzow (Jurisdiction) (1927).
[6] Wael Abdel Salam, *The Status of the Individual in the System of International Liability*, 1st ed. (Egypt: Dar Al-Nahda Al-Arabiya, 2001), 12.

appropriate penalties on the perpetrator of the harmful act.[7] Writings have been written about this diverse theory in international jurisprudence, including the jurists (Anzlotti and Cafferi), in that it was applied when the personality of the king or ruler was a person with the state. However, after the invention of the concept of the state and its sovereignty, it became difficult to detect the error of the legal person who has no soul or Conscience, because the basic principle is that the mistake is committed by a natural person, not a legal person, , and therefore the responsibility of a legal person is a responsibility for the actions of others. the international judiciary has taken final action in the Corfu Strait case.[8] Furthermore, due to the difficulty of proving fault and the inadequacy of this theory to address all damages, resulting in a lack of appropriate compensation, it has been criticized, leading to a shift towards the theory of an unlawful act.

2) Unlawful Act Theory:

This theory is based on the objective criterion of committing an unlawful act, which constitutes a violation of provisions of international law. International responsibility is thus established on the state that committed the act, expressing objective responsibility. This theory relies on the presence of a causal relationship between the state's activity, i.e., the act contrary to international law, and the resulting harm. It reflects objective responsibility based on the availability of a causal relationship between the state's activity, the act contrary to international law, and the actual damage incurred.[9] theories that preceded it, and it was applied by the International Court of Justice to determine France's responsibility for radioactive damage in 1973. This theory has found widespread acceptance in international jurisprudence and within international legislation and decisions from international courts.[10] Nevertheless, criticism has been directed at the theory of the unlawful act, considering it no longer suitable to cover all damages, especially those resulting from actions not prohibited by international law but still causing significant harm. Therefore, there was a necessity to explore a more advanced basis for international responsibility in light of evolving risks and damages arising from scientific and technological developments. A new trend emerged to adopt the theory of risk or the theory of assumption of risk, relying on the existence of harm as the basis for international responsibility, regardless of the presence of committed fault or an internationally unlawful act.

3) Risk Theory:

This theory establishes international liability based on the damage achieved, and thus we encounter the difficulty of proving error and the illegality of the act. The origin of this theory is derived from domestic law, which establishes responsibility for the damage achieved. This theory was adopted and the idea of international liability was adopted in cases of nuclear tests and spaceships, and it is the theory closest to applying it to damages resulting from cyber-attacks. This theory is also considered a modern concept compared to the traditional understanding of previous traditional theories based on error or illegal action.[11] This theory is considered complementary to the theories that preceded it, and it was applied by the International Court of Justice to determine France's responsibility for radioactive damage in 1973. The researcher believes that the approach of international jurisprudence that supports the idea of risk theory is the closest to supporting and also endorsing the validity of its supports,

[7] Ali Sadiq Abu Haif, *Public International Law*, 6th ed. (Alexandria: Alam Al-Ma'arif Press, 1962), 259.
[8] Al-Tarawneh, *The Mediator in Public International Law*, 597.
[9] Muhammad Hisham Al-Ebriqji, *Counter-espionage via Satellites in International Law*, 1st ed. (Cairo: New University Office Publications, 2020), 243.
[10] Article 2 International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts" (2001); Amer, *Introduction to the Study of Public International Law*, 784–85.
[11] Al-Ebriqji, *Counter-espionage via Satellites in International Law*, 251.

which achieve the establishment of responsibility for errors caused by cyber operations without adhering to the necessity of the act being internationally wrongful.

a) International judicial applications of risk theory:
International judiciary began to apply the risk theory in many international events, including the decision of the ICJ in the case of French nuclear tests in the Pacific Ocean in 1974, which indicates the adoption of the risk theory.[12]
b) International legal codification and risk theory:
Despite the jurisprudential differences regarding this theory, some international treaties adopted it, including the Japanese Society of International Law in 1977, the Convention on International Liability in the Field of Nuclear Energy in 1960, and the International Convention on Civil Liability for Damage Resulting from Oil Pollution in 1969.[13]

Therefore, not ratifying international agreements becomes a reason for evading responsibility, especially agreements that result in harm to others.

c. Elements of International Responsibility:

Individuals under international law bear international obligations and, in return, have rights under the legal framework of international responsibility. If states commit acts that cause significant harm to other states, they will bear the consequences. Whether these acts are carried out directly or indirectly, responsibility requires the presence of necessary elements and conditions, which we will clarify as follows:[14]

1) The Incident Establishing International Responsibility:

This incident can either be an unlawful act, as it contravenes the provisions of international law, or a lawful act within the framework of conventional international law. However, it causes harm to others according to the basis of responsibility built on the theory of risk.

a) The international wrongful act:

This is the prevailing concept in determining international responsibility. It involves committing a wrongful act, that is, violating an international obligation that a state is bound to uphold. This usually takes the form of a breach of the provisions of an international treaty or customary law. International courts typically apply this standard to determine a state's responsibility for harm caused to other states and the extent of its obligation to provide compensation. The act that violates international law may be an action, an omission, or both.[15] For example, in the Russian-Ukrainian War, the Russian Federation bears civil responsibility for violating international law and committing unlawful acts that resulted in serious harm to the Ukrainian side, and the link between the act and the result is very clear.[16] In the context of cyberspace, carrying out cyberattacks that violate the rules of international law or the principles of international humanitarian law, causing injuries, deaths, or damage to civilian property, is considered a wrongful act. Such actions may give rise to international responsibility when the necessary conditions are met.[17] Of international responsibility for the risky activity of the

[12] Namaryan Green, *International Law*, 1st ed. (pitman publishing, 1987), 242.
[13] Abdul Hadi Muhammad Al-Ashry, *Environment and Regional Security in the Arab Gulf States*, 1st ed. (Cairo: Dar Al-Nahda Al-Arabiya Publications, 1977), 84.
[14] Heikal, *International Individual Criminal Responsibility before International Criminal Justice: A Study within the Framework of International Humanitarian Law*, 77.
[15] ICJ Reports, Corfu Channel, U.K. v. Albania, Judgment (1949).
[16] Olena Nihreieva, "State Responsibility for Cyberattacks as a Use of Force in the context of the 2022 Russian Invasion of Ukraine," *IDP Revista de Internet Derecho y Política*, no. 42 (2025), https://doi.org/10.7238/idp.v0i42.430724.
[17] Mahmoud Hussein Al-Sharqawi, *Cyber Attacks in Light of the Provisions of International Humanitarian Law*, 1st ed. (Cairo: Dar Al-Nahda Al-Arabiya, 2021), 173.

incident, even if the incident is lawful. This implies the establishment of civil international responsibility based on the concept of responsibility without fault or without an unlawful act.[18]

b) The Incident Establishing Objective International Responsibility Devoid of Wrongfulness:

The basis for international responsibility in this case is presumed or objective, meaning there is no wrongdoing or unlawful act according to the perspective of international law. This situation applies the theory of strict liability or the theory of risk, focusing on the existence of harm triggering international responsibility, regardless of whether the act or incident is lawful. This situation is applied when a state engages in or commits technically hazardous activities. In other words, the state bears the consequences.

2) Attributing the international incident to a person of international law:

Attributing the act to the state: It is not enough to say that a state is responsible if the act is harmful or illegal; it must be related to the concerned state. The act can be attributed to a state, if this state is fully sovereign, independent state. It means that its sovereignty lies in its three authorities (legislative, executive, and judicial).[19]

a) The issuance of the act by the legislative authority:

Any act, omission, or negligence by the legislative authority that constitutes a violation of the provisions of international law and represents a breach of international obligations towards states or organizations establishes the responsibility of the state. This includes:

a. Enacting a law by the legislative authority that conflicts with previous international commitments made by the state.
b. Refraining from legislating a law that establishes a specific international commitment subject to implementation.
c. Failing to repeal a law that hinders or conflicts with international obligations.

In these cases, responsibility falls on the state, and this is stipulated in the Vienna Convention on the Law of Treaties of 1969.[20]

b) The issuance of the act by the executive authority:

This passage describes the image representing the state in its narrow sense. However, this interpretation is not limited to the government; it also includes the administrative branches and entities that are not part of the state apparatus. State law allows these entities to exercise governmental powers, whether within their specified authorities or if they exceed them. It encompasses actions by entities placed under the control of another state, as well as entities that exercise their powers in cases where they are not fulfilling their responsibilities.

c) The issuance of the act by the judicial authority:

The act is attributed to the judicial authority and entails international responsibility in the event of an error by the judge in applying a legal rule consistent with international obligations. This also applies if the judge applies an internal rule that conflicts with international commitments. Moreover, it includes situations of denial of justice, which involve shortcomings in internal regulations or the exercise of judicial functions, constituting a breach of the state's international duty to provide judicial protection for the lives and property of foreigners. This

[18] Nizar Al-Anbaki, *International Humanitarian Law* (Jordan: Dar Wael for Publishing and Distribution, 2010), 463.
[19] Faisal Saleh Alabbadi, Emad Mohammad Al Amaren, and Sultan Ibrahim Aletein, "International Responsibility Arising from Cyberattacks in The Light of the Contemporary International Law," *International Journal of Cyber Criminology* 16, no. 1 (2022): 156–69, https://doi.org/10.5281/zenodo.4766562.
[20] "Vienna Convention on the Law of Treaties" (1969), Article 46 and 73.

extends to situations where courts refuse to hear a dispute involving a foreigner despite having jurisdiction or fail to punish aggressors against foreigners or delay in doing so, among other scenarios.

d) Special circumstances of state responsibility for internationally wrongful acts include:

a. International responsibility for the actions and actions of private persons:

The general rule is that a state is not responsible for the actions of ordinary individuals residing on its territory. However, a state is obligated to exercise due diligence because it is required to provide security. If it fails in this duty, it may be subject to international responsibility. An illustrative example of this responsibility is the judgment of the International Court of Justice in the case of the U.S. hostages in Iran in 1980. The court affirmed Iran's responsibility as a state, not because the actions were directly attributed to the state, but because Iran "failed in its duty to prevent individuals from attacking the U.S. embassy and holding the diplomatic hostages, despite having the means to address the situation".[21] However, there are two exceptions to this rule:

1. The first one is when individuals act according to instructions issued by the state, under its direction or under its control when engaging in actions that violate the law, this is explicitly stated in Article 8 of the Draft Articles on State Responsibility.[22]
2. The second one is the failure to exercise due diligence to prevent actions that cause harm to others, which explains the implicit consent of the state to unlawful or harmful actions by individuals.

b. International responsibility in the event of civil wars and for the actions of revolutionaries: Regarding cases of rebellion and armed rebellion, which typically lead to civil wars or internal armed conflicts, whether they involve confrontations between armed groups or between these groups and the state, international jurisprudence has generally established that the state is not responsible for acts of war based on the principle of "force majeure" when foreign nationals are harmed, unless these acts violate the rules of international humanitarian law.[23] As for the international responsibility for the actions of rebels in disturbances, revolutions, and internal conflicts, we will consider two hypotheses: The first hypothesis: The occurrence of rebellion and revolution without the rebels gaining control of the government. Here, in general, insurgent movements and their actions are not attributed to the state. This is a well-established principle in international law because these movements have an independent structure from the state. Therefore, their actions are considered not attributable to the state, and they are not held accountable based on the principle of non-attribution unless the state has exercised due diligence to prevent these actions. Otherwise, the state may be held accountable internationally.[24] The second hypothesis: The situation of a successful revolution with the rebels coming to power. Here, the state is held accountable for the actions of the rebels and the damages caused to foreign nationals, whether the rebels formed a government in part of the state or in the entire state. Consequently, the new state cannot disclaim international responsibility for the actions of the rebels. This is a well-established principle in international law that states "the responsibility of the revolution for its actions committed before coming to power." It has been recognized by the International

[21] Al-Anbaki, *International Humanitarian Law*, 475; Salam, *The Status of the Individual in the System of International Liability*, 25.
[22] Article 8 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts; ICJ Reports, Military and paramilitary activities in and against Nicaragua (Nicaragua vs. united state of America) (1986).
[23] Al-Anbaki, *International Humanitarian Law*, 473–76.
[24] Heikal, *International Individual Criminal Responsibility before International Criminal Justice: A Study within the Framework of International Humanitarian Law*, 89.

Law Commission in the Draft Articles on State Responsibility.[25] In the cyber context, attributing acts to states under international law presents significant challenges, particularly in the case of cyberattacks. This is due to the ease with which the perpetrator's identity can be concealed and the difficulty of identifying the source and origin of cyberattacks two inherent characteristics of the cyber domain and cyberattacks themselves. These attacks may be carried out by governmental organizations, whether global or regional, or by individuals with international communications privileges, or those connected to terrorist groups, insurgents, or liberation movements.[26] Furthermore, gathering forensic evidence in the cyber domain is a complex process, as it can be completed in mere seconds, leading to the erasure of evidence or the prevention of tracking, and the use of different or non-existent IP addresses. This may involve using networks not belonging to the attacker, making attribution difficult and potentially inaccurate.[27] Therefore, attributing an act to the state does not require the actual control if domestic law assigns specific governmental functions to an entity. An example of such a case is the Cyber Unit affiliated with the Estonian Defence League State responsibility remains applicable for the actions of entities granted governmental powers under domestic law, even if they exceed or violate those powers.[28] This is addressed by Article 7 of the Draft Articles on State Responsibility.[29]

3) The wrongful conduct or act results in harm to a person of international law:

Damage is considered one of the essential conditions for the establishment of responsibility. International jurisprudence defines damage as "an encroachment upon the right or legitimate interest of an individual under international law" or "the material and moral loss incurred by a state".[30]

a. The necessity of damage:

The prevailing international trend does not require the existence of damage for international responsibility to arise. Most international commitments in agreements do not necessitate the presence of damage, as the violation of obligations in treaties and international customs is sufficient for international responsibility, even if damage is potential or a possible result of the unlawful act.[31] However, some legal perspectives argue for the necessity of actual damage resulting from an unlawful act to establish international responsibility. Damage, whether material or moral, is defined as the loss incurred by a state or an encroachment upon the right or legitimate interest of an individual under international law. Proving the existence of damage can be challenging, and damage may not manifest immediately, especially in cyber-attacks.[32] The application of the risk theory might make damage a crucial element, but it is a narrow

[25] Al-Anbaki, *International Humanitarian Law*, 479.
[26] Rashid Muhammad Al-Marri, *Cybercrimes in Light of Contemporary Criminal Thought: A Comparative Study*, 1st ed. (Egypt: Dar Al-Nahda Al-Arabiya, 2018), 122.
[27] Alabbadi, Amaren, and Aletein, "International Responsibility Arising from Cyberattacks in The Light of the Contemporary International Law."
[28] Tom Gjelten, "Volunteer Cyber Army Emerges In Estonia," *NPR News*, 2011.
[29] Artricle 7 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts.
[30] Al-Tarawneh, *The Mediator in Public International Law*, 615; Rashad Al-Sayyid, *Principles of Public International Law*, 3rd ed. (Amman: Dar Wael for Publishing and Distribution, 2000), 186.
[31] Article 1 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts.
[32] Heikal, *International Individual Criminal Responsibility before International Criminal Justice: A Study within the Framework of International Humanitarian Law*, 97.

approach as international responsibility typically hinges on the existence of an unlawful act, as emphasized by Articles 1 and 2 of the Draft Articles on State Responsibility.[33]

b. Damage characteristics:

To establish harm, a prerequisite for triggering international responsibility, certain conditions must be met, and the harm must possess specific characteristics. The characteristics of harm include:

1. The harm must be direct and actual, meaning there is a causal relationship between the incident and the harm, and the harm is not merely potential.
2. The harm must result from an attack on a legally protected right. This implies that there is a legal interest worthy of protection under international law, as confirmed by international jurisprudence in the "Barcelona Traction" case.[34]
3. The harm must be related to the individual right of the injured party in the international responsibility claim (individualization of harm). International courts have emphasized the requirement of a state's self-interest in claims for compensation,[35] and this interest should not be related to a general international interest in the world community, as the international legal and judicial reality has not yet reached the level of establishing public claims.
4. The harm can be either material or moral. Material harm is compensable and can take the form of either restitution, restoring the situation to what it was before the harm occurred, or compensatory damages, which involve the payment of a sum of money. Since material harm generally lends itself to monetary compensation, this form of compensation is more common. In contrast, moral or moral harm, such as the violation of a state's dignity, flag, or leader, does not naturally lend itself to valuation in monetary terms.[36]

The best way to remedy moral harm is through satisfaction, taking the form of a formal diplomatic apology or the punishment of individuals responsible for internationally wrongful acts, triggering the state's international responsibility for that harm.[37]

4) International responsibility under Tallinn manual, ICJ perspectives:

a. Contributions of the Tallinn Manual:

The Tallinn Manual functions as an official non-binding document which explains how international law applies to cyber operations. The document maintains sovereignty principles and due diligence standards and non-interference rules while applying them to digital operations. The document establishes that harmful cyber operations qualify as internationally wrongful acts even when they do not amount to armed force. States become responsible for cyber activities that start from their territory when they know about the activities or should have known about them.[38] The interpretation matches existing international law principles while strengthening the possibility of civil liability .The Tallinn Manual provides detailed information about the effects of illegal cyber operations which include both stopping the activity and providing compensation for damages. The established legal framework now applies to complex

[33] Article 2 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts.
[34] ICJ Reports, Barcelona Traction (1970).
[35] Al-Anbaki, *International Humanitarian Law*, 491.
[36] Talal Yaseen Aleisaa and Odai Mohammad Innab, "International Responsibility for Cyber-Attacks in Light of the Contemporary International Law," *Zarqa Journal for Research and Studies in Humanities* 19, no. 1 (2019): 88, https://doi.org/10.12816/0054788.
[37] Al-Anbaki, *International Humanitarian Law*, 493.
[38] Liis Vihul, "The Tallinn Manual on the International Law Applicable to Cyber Operations," *Georgetown Journal of International Affairs* 18, no. 3 (2017): 40–49.

technological damages through these specific definitions which enhance the development of civil liability systems in cyberspace.[39]

5) ICJ Jurisprudence and Its Application to Cyber Contexts:

The International Court of Justice has not made any decisions about cyber-specific cases but its existing decisions provide essential guidance. The Corfu Channel case established that states must prevent their territory from being used for actions which harm other nations.[40] The duty of due diligence has become a key foundation for cyber responsibility because states must demonstrate they took proper measures to stop malicious operations that started from their territory. States that allow cyberattacks to start from their territory through intentional or careless actions will need to compensate for the resulting damage .The ICJ has established two important principles through its Bosnian Genocide case and other decisions which help determine when states can be held responsible for cyber operations conducted by their hacker groups or proxy forces. The court established two essential criteria to link cyber operations to states and to determine if states maintained sufficient preventive and supervisory control.[41] The court's decisions establish practical standards for cyber attribution while upholding theoretical principles.

6) Provisions of international liability for cyber-attacks:

For the purpose of elucidating the provisions of international responsibility for cyber-attacks, it is essential to delve into the conventional and customary legal rules governing international responsibility in its general context.[42] This exploration is necessary to clarify the legal framework for international responsibility concerning cyber-attacks and to review key decisions issued by international courts. This is particularly relevant as we navigate the realm of cyber-attacks within a legal landscape that could be described as an international legal vacuum or the absence of an international agreement regulating cyber operations and imposing international responsibility for them.

a. Cyber Attacks and Principles of International Responsibility:

The use of cyber-attacks in the realm of security and military affairs has become a prominent aspect of international relations, whether in times of peace or during international and non-international armed conflicts. Each case has its own rules and legal principles that may apply. To determine international responsibility for cyber-attacks, international efforts must grapple with the issue of attributing these attacks to a state as a subject of international law, which is accountable for international responsibility.

b. International responsibility for cyber-attacks and attribution rules:

The significance of cyber power has permeated various aspects of life, with a substantial impact on military and security domains. Cyber capabilities are now integral to international conflicts, prompting many nations to establish dedicated cyber units, These units, whether military or civilian, are tasked with ensuring cyber security. Additionally, some countries have

[39] Michael N Schmitt, "Fault Lines in the Law of Cyber Operations," *AJIL Unbound* 111 (2017): 61–66.
[40] Tom Dannenbaum, "Due Diligence in Cyberspace," *AJIL Unbound* 111 (2017): 24–29.
[41] Marko Milanovic, "State Responsibility for Cyber Operations," *International Law Studies* 96 (2020): 1–50.
[42] Rizqa Ismail, "Cyberspace and Transformation in Concepts of Power and Conflict," *Journal of Legal and Political Sciences* 10, no. 1 (2018): 1018.

entrusted this responsibility to private cybersecurity companies, leveraging the challenge of attributing cyber-attacks to specific entities.[43]

This situation complicates the process of attributing cyber actions to states, allowing them to evade international responsibility. In this context, we will examine the legal provisions governing state responsibility for cyber-attacks and violations of the duty to prevent and ensure compliance with international law. The following key aspects will be addressed:

1. Determining a state's international responsibility for cyberattacks requires attribution. It serves as the foundation of the legal system that assigns responsibility and fights cyberthreats. The distinction between direct and indirect international liability helps clarify the legal implications of attributing cyber operations to countries.
    a. Direct international responsibility for cyberattacks issued by state agencies or some of the entities that implement them based on their authorization or authorization:
    It is established in law and jurisprudence that any unlawful act committed by state authorities, entities, or institutions is considered an act attributable to the state under international law. Article 4 of the Draft Law on International Responsibility explicitly states this principle, and it is reinforced by Rule 6 of the Tallinn Manual.[44] This principle is a well-established principle of customary international law. Cyber-attacks launched by non-state actors, which are not officially part of state authorities or institutions, but which exercise legal powers delegated to them by the state through legal or official authorization, are considered acts expressing the will of the state. Although these attacks are carried out by non-state actors, they are attributed to and endorsed by the state. Consequently, some states use cyber tools to launch their attacks with impunity, knowing (or at least strongly suspecting) that their digital attacks will not provoke a response or will only elicit a response limited to "slander" in diplomatic and media circles Thus, the state bears direct responsibility for such actions.[45] A prime example of this is the state's contracting with cybersecurity firms.[46]
    b. Indirect international liability for cyber-attacks:
    When cyber-attacks are perpetrated as unlawful acts and violations of international law by groups, entities, or individuals not affiliated with state apparatuses, lacking official authorization or legal delegation, it does not absolve the state from international responsibility. This is explicitly affirmed by Article 8 of the Draft International Responsibility Law of 2001, which establishes an internationally recognized legal norm. The article places emphasis on terms such as, guidance, and control.[47] In international jurisprudence, two fundamental criteria have been applied to establish the connection of non-state groups or entities with a state, enabling the attribution of unlawful acts, such as cyber-attacks, to the state. Consequently, legal responsibility rests on that state. These criteria are the standards of effective control and complete or total control. The first criterion, effective or actual control:
    The International Court of Justice, in the case of military or quasi-military activities in Nicaragua against the United States, adopted the criterion of effective control as

[43] Badran Abbas, *Cyber War: Clash in the World of Information* (Lebanon: Kufa Studies Center, 2010), 111; Abdul Karim Alwan, *The Mediator in Public International Law*, 1st ed. (Amman: Dar Al-Thaqafa for Publishing and Distribution, 2010), 163.
[44] Rule 6 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).
[45] William Banks, "Cyber Attribution and State Responsibility," *International Law Studies* 97 (2021).
[46] Kazem Muhammad Al-Ali, *Direct Participation in Cyber Attacks*, 1st ed. (Beirut: Modern Book Foundation, 2019), 227.
[47] Article 8 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts.

suitable for application regarding quasi-military forces at least.[48] This criterion necessitates a strong and direct connection of the state to prove a relationship of subordination between the state and these groups. It involves the state issuing specific instructions, directives, and orders to these groups regarding the intended or required cyber operation. Strict proof of subordination is required, making it imperative for the state to exert tight and effective control over specific cyber operations to attribute them to the state.[49] In adherence to this criterion, which focuses on actions carried out by groups inherently independent of the state, proving the connection between these groups and the state in executing specific cyber-attacks requires clear evidence of state-directed support, funding, skills, expertise, and resources for these attacks. The application of this criterion involves strict and effective control over cyber, operations and attacks specific enough to be attributed to the state. However, this requirement contradicts the nature of cyber-attacks characterized by speed, difficulty in proving the identity of actors, and identifying the source of cyber-attacks, leading to a significant drawback in attributing responsibility to the state.[50] Given the difficulties in applying this criterion due to its ambiguity and its lack of applicability to many operations, including cyber-attacks, international jurisprudence has sought a less stringent and more flexible standard – that of complete or total control. Consequently, the legal community has explored an alternative standard that is less strict and more adaptable, given the challenges posed by cyber warfare .

The second criterion: Total or complete control:

Considered more flexible and expansive, the criterion of total control offers a broader framework for attributing military conduct executed by armed groups to a state. It suffices for the state to have a role in organizing, coordinating, or planning military or quasi-military actions by armed entities, whether there are specific instructions for the execution of a cyber operation or attack or not. This means that this criterion does not demand effective control over the action but total control over the actor and the executor of the cyber-attack itself. It represents a less stringent standard than the criterion of effective control, and the International Criminal Tribunal for the former Yugoslavia adopted the total control standard in the Tadic case (57), Similarly, Article 8 of the Draft Articles on State Responsibility for 2001 endorsed the total control criterion.[51] In the cyber context, a state that provides organized groups with cyber weapons, plans cyber-attacks with them, and selects targets becomes and selects targets becomes internationally responsible for those cyber-attacks and for every operation executed by those groups, even if it exceeds the limits of those instructions or directives, contrary to the effective control criterion that attributes state responsibility only to specific cyber-attacks.[52] The researcher emphasizes the importance of applying the total control criterion to cyber-attacks to determine international responsibility, as it is more suitable and closer to attributing cyber-attacks to the state. Applying the

[48] ICJ Reports, Military and paramilitary activities in and against Nicaragua (Nicaragua vs. united state of America); ICJ Reports, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (2007).

[49] Marco Milanovic, "State Responsibility for the Actions of Non-State Actors," *Journal of International Law*, 2009, 315.

[50] Ahmed Oubais Al-Fatlawi, "Cyber Attacks: Its Concept and Arising International Responsibility In the Light of Contemporary International Organization," *AL- Mouhaqiq Al-Hilly Journal for Legal and Political Science* 8, no. 4 (2016): 638–39.

[51] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Article 8.

[52] Kubo Mačák, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors," *Journal of Conflict & Security Law* 21, no. 3 (2016): 422, https://doi.org/10.1093/jcsl/krw014.

effective control criterion narrows the scope of international responsibility, as explained earlier, and encourages violations of international law. If cyber-attacks are executed, the victim state may struggle to prove the aggressor state's responsibility for its conducted cyber operations. Therefore, the significance lies in focusing on the state's funding, provisioning, training, and establishing the total control criterion as sufficient evidence to establish international responsibility for cyber-attacks, which is deemed more effective.

2. The Tallinn Manual tends to favor it, also supported by the paperdue to its legal soundness in the framework of distinguishing between two scenarios:
   a. Execution of cyber-attacks by organized groups. In this case, the actions and unauthorized cyber operations are attributed to the state based on the total control criterion.
   b. In the case of cyber-attacks executed by non-organized groups or individuals, determining state responsibility requires applying the criterion of effective control. The state's exercise of control and direction over these groups must go beyond mere oversight and guidance to reach the level of direct participation in the cyber-attack.[53]

In the context of state responsibility for cyber-attacks perpetrated by non-organized groups or individuals, it is imperative to provide evidence establishing the affiliation of these groups with the state and the issuance of instructions to them by the state.[54] It is worth noting that there are specific cases related to international responsibility for cyber operations and attacks, including:

1. In cases where responsibility for cyber-attacks, which has not been substantiated, is later acknowledged, such acts are considered emanating from the aggressor state under the provisions of international law, as indicated by Article (11) of the Draft International Law on Responsibility of States for 2001.[55]
2. In the case of cyber-attacks carried out through the cyber infrastructure of a second state to assault a third state without the consent or intervention of the second state, the actions of the cyber actors cannot be attributed to the second state. Consequently, international responsibility cannot be invoked against it due to the criminal nature of these cyber actors, who may be launching cyber-attacks against their own state for certain political reasons in some cases.[56]
3. It is essential to emphasize that both the effective control and total control standards, while providing a fertile ground for establishing international responsibility for violations of international law within its general framework, necessitate the conclusion of a clear and detailed international agreement on the regulation of cyber-attacks. This is crucial to overcome the difficulty of identifying the identity of the cyber attacker and consequently attributing the action to the state, leading to international responsibility, whether within the civil framework or in the context of individual international criminal responsibility in the event of victims, injuries, or fatalities.[57] Cyber-attacks exhibit a non-materialistic nature that contradicts conventional means of proof and attribution.

7) International Responsibility for Violating the Duty of Prevention and Ensuring Respect

[53] Comment 11 Rule 6 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.
[54] Mačák, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors," 415.
[55] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Article 11.
[56] Al-Sharqawi, *Cyber Attacks in Light of the Provisions of International Humanitarian Law*, 190.
[57] Adel Abdullah Al-Masadi, *The War Against Terrorism and Legal Defense within the Framework of Interna-Tional Law*, 1st ed. (Egypt: Dar Al-Nahda Al-Arabiya, 2006), 127; Al-Sharqawi, *Cyber Attacks in Light of the Provisions of International Humanitarian Law*, 191.

In this context, we discuss a scenario where cyber-attacks constitute unlawful acts but cannot be attributed to a specific state. Legal logic necessitates the exploration of new standards to subject international perpetrators to international responsibility for the necessities of respecting the rules of international law, maintaining international peace and security, and respecting the sovereignty of states while refraining from interfering in their internal affairs. The most notable manifestation in this context is the international responsibility for violating the duty of prevention, which involves a two-fold international commitment: one aspect involves preventing the execution of cyber-attacks before harm occurs, while the other involves the duty of suppression, i.e., punishing perpetrators of cyber-attack,[58] Another aspect is the establishment of international responsibility for violating the duty to enforce respect for international humanitarian law. In this context, state responsibility does not revolve around the execution of cyber-attacks but rather pertains to the failure to prevent the unlawful behavior manifested in cyber-attacks. Therefore, responsibility in this context does not necessitate the occurrence of physical damage to civilian property or casualties, injuries, and deaths among civilians. It suffices that the negative impact resulting from cyber-attacks, such as the breach of the duty of prevention, is present. The existence or occurrence of harm, however, serves as a ground for intensifying responsibility and demanding compensation.[59]

2. The consequences of establishing international responsibility for cyber-attacks:

After addressing the principles of state responsibility for cyber-attacks, it becomes evident that, both jurisprudentially and in international practice, state responsibility for unlawful acts is a form of civil international responsibility. This holds true unless the act in question, taking the form of cyber-attacks, falls under one of the exclusionary circumstances such as consent, compulsion, necessity, the occurrence of a legitimate self-defence situation, collective security measures, or if the cyber-attacks constitute part of countermeasures. Therefore, it is crucial to elucidate the consequences and effects resulting from the assertion of international responsibility.

a. Effects of international liability arising from cyber-attacks:

Proving international responsibility for an individual under international law entails legal consequences that are divided into two main categories:

1) Consequences related to restoring the affected international relationship to its normal state: When a specific state violates the provisions of international law by committing unlawful acts or actions that cause harm to other states, it becomes crucial to restore the legal relationship between the states and ensure the continuation of good relations. If the unlawful cyber-attacks, representing a breach of the United Nations Charter during peacetime, rise to the level of the use of force, leading to a violation of the principles of sovereignty and non-intervention in internal affairs, or constitute a breach of international obligations under the laws of international humanitarian law and rules of targeting, there may be actions, attacks, or cyber operations that may not be expressly prohibited by international law. Still, the executing state must adhere to the provisions of international law in a manner that does not cause harm to others, according to the theory of due diligence.[60]
    a) Commitment to notification and consultation: It emphasized this commitment as one aspect of jurisprudence and includes the commitment of states carrying out hazardous

[58] Essam, *Public International Law*, 278.
[59] Comment 5 Rule 5 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.
[60] Al-Ali, *Direct Participation in Cyber Attacks*, 186.

cross-border activities to notify the potentially affected states of the possible harm resulting from these activities.[61]

b) Commitment to stop illegal actions: Ceasing the unlawful conduct, incident, or actions is considered a form of the effects of responsibility aimed at restoring the situation to its state before the unlawful act occurred internationally. This form of the effects of international responsibility is invoked when the unlawful conduct or incident is ongoing. The International Court of Justice affirmed the principle of ceasing unlawful activities in its decision on the Military and Paramilitary Activities in and against Nicaragua in 1986.[62] In the cyber context, this image can be applied by analogy to international judicial decisions and texts of international law, including what is stated in the draft law of international responsibility, requiring the state to stop illegal cyber operations and attacks, whether they violate the provisions of general international law or the provisions of international humanitarian law.

2) Effects related to reparations: The responsible state is obligated to make full reparation for the damage and loss it causes to another state as a result of its illegal actions, including compensation for material and moral damage. This is what was stipulated in the International Liability Project of 2001, which provided three images of these effects:
   a) In-kind compensation: Restoring the situation to its pre-unlawful state means undoing all the legal and material effects resulting from the unlawful act, including the return of any seized funds, properties, legal statuses, or situations to the victim state. The principle of reprisals, where the aggressor cannot benefit from their aggression, is a well-established principle in international law. Restitution in kind is considered the primary form of compensation, and resorting to monetary compensation or settlement is only considered when restoring the situation to its pre-unlawful state becomes impossible.[63]
   b) financial compensation: This form of the effects of international responsibility is verified in the event that it is not possible to restore the situation to what it was, that is, the inability to redress the damage through in-kind restitution. The way is to resort to material reparation or financial compensation, which means compensation for the harmful and unlawful act.[64]
   c) Satisfaction: Compensation is an exceptional form of redress, not considered a compensation for loss, as it is a compensatory measure with a literary and moral character. It is resorted to when it is impossible to remedy the harm through restitution in kind or monetary compensation. It may take the form of acknowledging the unlawful act, expressing regret,[65] or issuing an official apology, ppossibly accompanied by a specific amount of money. However, in all cases, it is a formal expression of the aggressor state's dissatisfaction with the unlawful act committed by one of its authorities or officials. It can be said that compensation is the legal consequence of international responsibility for wrongful acts that affect the honor, dignity, and prestige of the state.

In-kind compensation in the cyber context, and when illegal cyber combines and causes harm to other countries, analogy to the state of international precedents, rules of international

[61] Robert Quentin-Baxter, "Third Report on International Responsibility for Harmful Consequences Arising from Acts Not Prohibited by International Law," 1982, 87.
[62] ICJ Reports, Military and paramilitary activities in and against Nicaragua (Nicaragua vs. united state of America).
[63] Article 34 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts.
[64] Heikal, *International Individual Criminal Responsibility before International Criminal Justice: A Study within the Framework of International Humanitarian Law*, 103.
[65] Ibid., 104.

law, and judicial precedents can confirm the normal countries' wonderful cyber, which may be through cyber-electronic treatments for the effects of cyber takeover that you mention, and disabling electronic viruses, in addition to returning files and data that you need electronically and financial compensation in the cyber context, this image can be easily applied to the case of claims for damages arising from the completion of illegal cyber-attacks through the assistance of experts specialized in the cyber context, so that the compensation is fair, appropriate, and affected by the specificity of the arising arising from the combination Cyber.

b. Justifications for concluding an international agreement to regulate cyber-attacks:

1) Acknowledging that most international agreements, whether conventional or customary, related to regulating international relations during times of peace and international and non-international armed conflicts, as well as regulating the means and methods of warfare, were concluded at a time when cyber-attacks were not prevalent. It is natural, therefore, not to find a clear legal framework explicitly regulating cyber-attacks and cyberspace.
2) Within the framework of international criminal law, it is no longer acceptable to expand criminalization without clear legal texts, and it has become unacceptable to rely on a broad interpretation of penal texts and rules, which requires the existence of an international agreement that regulates cyber-attacks within the framework of international individual civil and criminal responsibilities.
3) Addressing the effects of cyberattacks at the international level must start from the same point from which the international effort to criminalize cybercrimes at the national level began, as well as the relevant international customary rules.[66]

c. Obstacles to concluding an international agreement to regulate cyber-attacks:

1) Electronic superiority that characterizes some countries in the cyber context has brought the issue of cyber-attacks within the circle of traditional conflict and the arms race, and has restored the concept of hegemony for the sake of influence and the unwillingness of countries to curb their ambition in cyber armament and reveal their cyber capabilities.
2) The difference of views between two international parties, one of which is the United States of America and NATO, while the second party is led by Russia, China, and the countries that fall under the Shanghai Information Security Organization, and includes in addition to the countries of the former socialist bloc and Iran.
3) There is a serious challenge represented in the use of cyber-attacks, not only by states, but also by groups and entities that do not belong to states and are not linked to a legal relationship with them. They represent a great danger due to the difficulty of subjecting them to the provisions of international law and international responsibility, which has encouraged states to seek the help of these groups in order to evade international responsibility.

d. The international position on concluding an international agreement regulating cyber-attacks and operations:

The Council of Europe's Convention on Cybercrime, known as the Budapest Convention (2001), has played a significant role in the development of international perspectives on the need for an international agreement to regulate cyber-attacks. This was preceded by the United Nations General Assembly's resolution in 2001, which called for the examination of threats associated with the use of electronic systems for military purposes. It emphasized the importance of exploring the possibility of adopting international standards to mitigate their

[66] Adnan Al-Naqeeb, *Electronic Warfare in Light of the Seventy-Seven Protocols Annexed to the 1949 Geneva Conventions (Cyber Attacks)*, 1st ed. (Egypt: Arab Center for Publishing and Distribution, 2022), 367.

risks at the international level.[67] As for the United States of America, it supported the application of the contents of the Budapest Agreement in the international framework on cyber-attacks, and sees the importance of the agreement on disarmament of cyber weapons. As for Russia, it has gone further than the United States of America, and Russia says it is important to limit cyber-attacks.[68] The researcher believes that the international community needs an international initiative that brings out the internal intentions of interested countries regarding concluding an agreement restricting cyber-attacks and brings them into existence. It begins with a negotiating path that ends with the conclusion of international agreements that regulate cyber-attacks, just as they regulate the issue of nuclear and chemical weapons and others, and that there be education about the danger of cyber-attacks, and so that the realistic picture is clear to the leaders and commanders that they are not facing just a virtual electronic game, especially when it entails It has devastating effects on property, injuries and victims on the ground that do not differentiate between civilian or military.

D. CONCLUSION

This study addressed the problem of the absence of civil liability for cyberattacks and concluded that international law lacks any accountability mechanisms. After analyzing the concept of civil liability, its legal basis, and its components within the cyber context, it became clear that attribution, compensation, and the obligation of due diligence exist only as customary principles in international law. However, their application to cyberattacks is inconsistently effective and incomplete. The researcher arrived at three analytical conclusions:

1. There is significant difficulty in the attribution process immediately upon initiating civil liability proceedings.
2. The absence of binding legal texts and legislation. While the Tallinn Manual provides important guidance, it lacks the force to bind parties to any dispute or other states.
3. The number of victims of cyberattacks will continue to rise unless we establish and coordinate international standards for obtaining compensation and legal redress for the victims; otherwise, achieving these will be extremely difficult.

Clarifying how civil liability rules align with the damages resulting from cyberattacks will help bridge the gap between traditional civil liability and cyber realities. This is the focus of this paper at the theoretical level. At the practical level, we undoubtedly need national legislation adopted by governments and an agreement on an international cooperative mechanism as a preventative measure to help avoid cyberattacks in the first place, and to facilitate information exchange and dispute resolution.

As for the recommendations, we recommend a comprehensive international dialogue for all and working to define civil liability for cyberattacks. However, the desired outcome must include procedural mechanisms, legal obligations, and compensation with its standards and forms. All future efforts should be directed towards this issue in general, through intensifying studies and creating feasible and accountable cyber models, with the aim of development and reaching advanced stages that will make anyone who thinks about committing such attacks think twice before committing them.

REFERENCES

Abbas, Badran. *Cyber War: Clash in the World of Information*. Lebanon: Kufa Studies Center, 2010.

Al-Ali, Kazem Muhammad. *Direct Participation in Cyber Attacks*. 1st ed. Beirut: Modern Book Foundation, 2019.

Al-Anbaki, Nizar. *International Humanitarian Law*. Jordan: Dar Wael for Publishing and Distribution, 2010.

[67] United Nations General Assembly, "Responsibility of States for Internationally Wrongful Acts" (2001).
[68] Abbas, *Cyber War: Clash in the World of Information*, 656.

Al-Ashry, Abdul Hadi Muhammad. *Environment and Regional Security in the Arab Gulf States*. 1st ed. Cairo: Dar Al-Nahda Al-Arabiya Publications, 1977.

Al-Ebriqji, Muhammad Hisham. *Counter-espionage via Satellites in International Law*. 1st ed. Cairo: New University Office Publications, 2020.

Al-Fatlawi, Ahmed Oubais. "Cyber Attacks: Its Concept and Arising International Responsibility In the Light of Contemporary International Organization." *AL- Mouhaqiq Al-Hilly Journal for Legal and Political Science* 8, no. 4 (2016).

Al-Marri, Rashid Muhammad. *Cybercrimes in Light of Contemporary Criminal Thought: A Comparative Study*. 1st ed. Egypt: Dar Al-Nahda Al-Arabiya, 2018.

Al-Masadi, Adel Abdullah. *The War Against Terrorism and Legal Defense within the Framework of Interna-Tional Law*. 1st ed. Egypt: Dar Al-Nahda Al-Arabiya, 2006.

Al-Naqeeb, Adnan. *Electronic Warfare in Light of the Seventy-Seven Protocols Annexed to the 1949 Geneva Conventions (Cyber Attacks)*. 1st ed. Egypt: Arab Center for Publishing and Distribution, 2022.

Al-Sayyid, Rashad. *Principles of Public International Law*. 3rd ed. Amman: Dar Wael for Publishing and Distribution, 2000.

Al-Sharqawi, Mahmoud Hussein. *Cyber Attacks in Light of the Provisions of International Humanitarian Law*. 1st ed. Cairo: Dar Al-Nahda Al-Arabiya, 2021.

Al-Tarawneh, Mukhlid Irhkais. *The Mediator in Public International Law*. 2nd ed. Jordan: Dar Wael for Publishing and Distribution, 2015.

Alabbadi, Faisal Saleh, Emad Mohammad Al Amaren, and Sultan Ibrahim Aletein. "International Responsibility Arising from Cyberattacks in The Light of the Contemporary International Law." *International Journal of Cyber Criminology* 16, no. 1 (2022): 156–69. https://doi.org/10.5281/zenodo.4766562.

Aleisaa, Talal Yaseen, and Odai Mohammad Innab. "International Responsibility for Cyber-Attacks in Light of the Contemporary International Law." *Zarqa Journal for Research and Studies in Humanities* 19, no. 1 (2019): 81–95. https://doi.org/10.12816/0054788.

Alwan, Abdul Karim. *The Mediator in Public International Law*. 1st ed. Amman: Dar Al-Thaqafa for Publishing and Distribution, 2010.

Amer, Salah El-Din. *Introduction to the Study of Public International Law*. 1st ed. Cairo: Dar Al-Nahda Al-Arabiya Publications, 2003.

Banks, William. "Cyber Attribution and State Responsibility." *International Law Studies* 97 (2021).

Dannenbaum, Tom. "Due Diligence in Cyberspace." *AJIL Unbound* 111 (2017).

Essam, Al-Attiyah. *Public International Law*. Baghdad: Al-Nahda Library Publications, 2008.

Gjelten, Tom. "Volunteer Cyber Army Emerges In Estonia." *NPR News*, 2011.

Green, Namaryan. *International Law*. 1st ed. pitman publishing, 1987.

Haif, Ali Sadiq Abu. *Public International Law*. 6th ed. Alexandria: Alam Al-Ma'arif Press, 1962.

Heikal, Amjad. *International Individual Criminal Responsibility before International Criminal Justice: A Study within the Framework of International Humanitarian Law*. 1st ed. Cairo: Dar Al-Nahda Al-Arabiya Publications, 2009.

ICJ Reports. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (2007).

———. Barcelona Traction (1970).

———. Corfu Channel, U.K. v. Albania, Judgment (1949).

———. Military and paramilitary activities in and against Nicaragua (Nicaragua vs. united state of America) (1986).

International Law Commission. Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001).

Ismail, Rizqa. "Cyberspace and Transformation in Concepts of Power and Conflict." *Journal of*

Legal and Political Sciences 10, no. 1 (2018): 1018.

Mačák, Kubo. "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors." *Journal of Conflict & Security Law* 21, no. 3 (2016): 405–28. https://doi.org/10.1093/jcsl/krw014.

Milanovic, Marco. "State Responsibility for the Actions of Non-State Actors." *Journal of International Law*, 2009.

Milanovic, Marko. "State Responsibility for Cyber Operations." *International Law Studies* 96 (2020).

Nihreieva, Olena. "State Responsibility for Cyberattacks as a Use of Force in the context of the 2022 Russian Invasion of Ukraine." *IDP Revista de Internet Derecho y Política*, no. 42 (2025). https://doi.org/10.7238/idp.v0i42.430724.

Permanent Court of International Justice. Factory at Chorzow (Jurisdiction) (1927).

Quentin-Baxter, Robert. "Third Report on International Responsibility for Harmful Consequences Arising from Acts Not Prohibited by International Law," 1982.

Salam, Wael Abdel. *The Status of the Individual in the System of International Liability*. 1st ed. Egypt: Dar Al-Nahda Al-Arabiya, 2001.

Schmitt, Michael N. "Fault Lines in the Law of Cyber Operations." *AJIL Unbound* 111 (2017).

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017.

United Nations General Assembly. Responsibility of States for Internationally Wrongful Acts (2001).

Vienna Convention on the Law of Treaties (1969).

Vihul, Liis. "The Tallinn Manual on the International Law Applicable to Cyber Operations." *Georgetown Journal of International Affairs* 18, no. 3 (2017).