

International Law and Cyber Challenges: Protecting International Security in the Age of Technology

القانون الدولي والتحديات السيبرانية: حماية الأمن الدولي في عصر التكنولوجيا

Abdelaziz Selma Achba

Laboratory of human security: reality;
challenges; Perspectives

University of M'sila, University Pole, Road
Bourdj Bou Arreiridj, M'sila 28000 Algeria
selma-achba.abdelaziz@univ-msila.dz

Mansouri Mohamed

Laboratory of Studies and Research in Law
Family and Administrative Development

University of M'sila, University Pole, Road
Bourdj Bou Arreiridj, M'sila 28000 ;Algeria.
mansouri.mohamed@univ-msila.dz

Date of submission:03/04/2025 Date of final acceptance:24/07/2025 Date of publication :September

Abstract:

This study aims to explore cyber challenges and their impact on international security in light of rapid technological advancements. It begins by analyzing the nature of cyberattacks, demonstrating how these attacks have emerged as a new and transnational threat, affecting the stability of states and international relations. The study also examines the relationship between technology and international law, highlighting the challenges that technological development poses to current legal frameworks. Additionally, it focuses on the legal protection of international security, discussing the need for an updated international legal framework that keeps pace with the growing cyber threats. The study emphasizes the importance of developing international legislation capable of addressing attacks targeting critical infrastructure, such as energy, communications, and financial sectors. The primary goal of the study is to underscore the need for enhanced international cooperation to develop legal systems capable of protecting global security in the technological age, while stressing the importance of safeguarding critical infrastructure to ensure secure and sustainable economic and social stability.

Keywords: Cybersecurity; Cyberattacks; International Law; Critical Infrastructure; Cooperation.

ملخص:

سعى هذه الدراسة إلى استكشاف التحديات السيبرانية وتأثيرها على الأمن الدولي في ظل التطور التكنولوجي المتسارع. تبدأ بتحليل طبيعة الهجمات السيبرانية، موضحةً كيف أصبحت هذه الهجمات تشكل تهديداً جديداً وعابراً للحدود التقليدية، مما يؤثر على استقرار الدول والعلاقات الدولية. كما تدرس الدراسة العلاقة بين التكنولوجيا والقانون الدولي، مسلطة الضوء على التحديات التي يفرضها التطور التقني على الأطر القانونية الحالية. تركز الدراسة أيضاً على الحماية القانونية للأمن الدولي، حيث تناقش ضرورة وجود إطار قانوني دولي محدث يواكب التهديدات السيبرانية المتزايدة. وتشير إلى أهمية تطوير تشريعات دولية قادرة على التصدي للهجمات التي تستهدف البنية التحتية الحيوية مثل الطاقة، والاتصالات، والقطاعات المالية.

***Auteur correspondant :Abdelaziz Selma Achba.**

Introduction:

The modern world is witnessing rapid technological advancements, accompanied by growing cyber challenges that increasingly threaten international security. The expanding interaction between technology and international law raises questions about how to address cyberattacks and their repercussions on the international order.

Cyber challenges are escalating, and their impact on international security is intensifying through the illicit use of information technology to access confidential information or manipulate critical infrastructure. This results in significant economic losses and severe political and security damage on a global scale.

The importance of this study lies in the necessity of establishing effective mechanisms for global collaboration in cybersecurity, enhancing the ability for a swift and coordinated response to transnational cyberattacks. Furthermore, it highlights the need to develop international laws that align with new technological challenges and provide a comprehensive legal framework for protecting international security in the technological era.

To comprehend the detrimental impacts of cyberattacks on global security and the obstacles they provide to the international legal foundation, it is essential to comprehend the impact of advanced technology in exacerbating international tensions and its negative influence on international relations and their stability. This underscores the urgent need for an effective international legal framework capable of protecting critical infrastructure and comprehensively addressing the ramifications of cyberattacks.

From this perspective, the following question arises:

Study Problem:

The central issue addressed in this study is: **How can international law adapt to technological developments to protect cybersecurity and critical infrastructure?**

In light of this research problem, the study seeks to address the following sub-questions:

- What is the definition and classification of cyber attacks, and how do they impact international security?
- How do cyber challenges influence the stability of international relations and global security?
- To what extent can existing international law address cyber threats, and what are the obstacles to its effective application?
- How can international legal frameworks be developed or updated to provide comprehensive protection for critical infrastructure in the technological era?
- What role does international cooperation play in enhancing cyber security and responding to transnational cyber attacks?

To address the primary concern of this research, which revolves around the legal and political challenges posed by cyberattacks to international security, and how to frame these challenges within an international legal framework capable of protecting critical infrastructure and responding to the threats of advanced technology, we adopted a methodology combining description and analysis. This includes describing the nature and concept of cyberattacks through various rules of international law, as well as reviewing previous research, articles, and studies. Additionally, we analyze the available international legal frameworks for protecting critical infrastructure and cybersecurity, assessing their effectiveness and suitability.

We have divided our study into two main sections: the first explores cyber challenges and international security, while the second addresses the legal protection of international security in the technological era.

Section I: Cyber Challenges and International Security

In the contemporary era, cyber challenges are among the most significant hazards to international security. These challenges encompass various aspects that affect nations, companies, and individuals alike. Addressing them requires integrated efforts at all levels, in addition to

developing a strong cybersecurity infrastructure capable of countering attacks and safeguarding international security. In this section, we will endeavor to establish the definition of cyberattacks and investigate the correlation between international law and technology.

A) Conceptual Approach to Cyberattacks and Their Impact on International Security:

The digital and information revolution has resulted in a technological leap that created cyberspace, built on a global infrastructure of information and communication technology. This has triggered a new arms race, focusing on the development of technical programs used in cyberspace to achieve various goals on military, political, economic, and social levels, forming what is now known as cyberattacks.

1- Definition of Cyberattacks and Their Types:

- International Committee of the Red Cross Definition: "The intentional use of actions to modify, disrupt, mislead, undermine, or incapacitate an opponent's information, including computer systems or networks and software included inside these systems, which may also impact associated companies."¹
- Michael N. Schmitt Definition: "A series of measures implemented by a state to assault adversarial information systems with the objective of impairing and harming them, while concurrently safeguarding the information systems of the attacking state."²
- Abdelkader Mohamed Fahmy Definition: "The use of a state's network system and computer devices, or individuals or groups not affiliated with state entities, to disrupt or reduce the efficiency of other actors' control systems or to destroy them, which could endanger national security."
- Tallinn Manual Definition: "Cyber operations, whether offensive or defensive, aimed at causing harm, damage, or destruction to targets."³

Defining the concept of a cyber attack is central to academic, legal, and policy-oriented discussions. While the definitions provided by various sources offer valuable insights, they also suffer from a number of conceptual and practical limitations, as outlined below:

- Limitations in Conceptual Scope; The International Committee of the Red Cross (ICRC) focuses predominantly on the informational dimension of cyber attacks, including software and networks. However, it overlooks the physical consequences of such attacks, such as disruptions to power grids, healthcare systems, or infrastructure, which have become increasingly common in real-world scenarios.

The Tallinn Manual definition, while comprehensive in military-legal terms, fails to distinguish between different types of cyber operations (e.g., espionage, cybercrime, or disinformation campaigns), thereby limiting its applicability outside the context of armed conflict.

- Lack of Actor-Specific Clarity: Michael Schmitt's definition centers on the state as the primary actor, implying a traditional, state-centric view of cyber operations. This perspective neglects the growing role of non-state actors—such as hacktivist groups, cybercriminal organizations, and even individuals—who often operate independently or as proxies.

In contrast, Abdelkader Mohamed Fahmy does mention both state and non-state actors, yet the definition lacks a clear analytical framework to categorize or assess these actors, especially in cases of attribution or hybrid operations where the line between state and non-state involvement is blurred.

- Ambiguity Regarding Intent and Objectives: Most definitions emphasize the intent to harm or disrupt, yet they fail to account for non-destructive or covert objectives, such as data theft, surveillance, psychological manipulation, or influence operations, which are increasingly prevalent in cyber conflicts.

- Inattention to the Evolving Nature of Cyberspace: None of the definitions adequately reflect the dynamic and rapidly evolving nature of cyber operations, particularly with the integration of emerging technologies like artificial intelligence, quantum computing, and the Internet of Things (IoT). This raises concerns about their long-term relevance.

Based on these definitions, cyberattacks can be defined as a deliberate and hostile cyber operation, conducted by state or non-state actors through digital vectors—such as networks, software, or connected systems—with the intent to disrupt, degrade, manipulate, or destroy digital, physical, or cognitive assets. These actions may target critical infrastructure, information systems, or societal functions, and often involve tactics like malware deployment, data exfiltration, or influence operations. Characterized by their asymmetry, anonymity, and transnational nature, cyber attacks pose multidimensional threats to national security and global stability.

The key characteristics of cyberattacks are:

- Highly advanced, technology-based attacks that rely on digital and electronic tools.
- Speed, flexibility, and global reach, eliminating temporal, spatial, and geographical barriers.
- Unlimited targets and outcomes.
- Relatively low cost compared to traditional military attacks.
- Difficulty in attribution due to the use of easily concealable methods.
- Considerable impact of non-state entities, such as multinational corporations like Google,

Microsoft, and Apple, alongside criminal organizations that target nations through data theft, hacking, and resource exploitation. Additionally, terrorist organizations have developed substantial cyber capabilities.⁴

1- Types of Cyberattacks:

Based on the perspective presented by Andrew Rathmel regarding cyberattacks, which states: "Technological and socio-political developments indicate that future threats faced by nations will take on an electronic form centered around information in the world, through various and diverse informational attacks, which can be well-prepared to attack a large number of carefully selected targets,"⁵ it becomes clear that there are multiple forms of potential security threats and anticipated cyberattacks, which can be categorized as follows:

- Cyber Piracy: This involves unauthorized copying, reproduction, and distribution of software, as well as accessing confidential or personal information through digital technology by hacking websites, social media pages, email accounts, or databases, followed by modifying or taking control of them.⁶
- Cyber Espionage: This refers to attempts to access concealed information from a targeted party and unlawfully seize it. It is a continuous process carried out over a specific period to obtain confidential information. Cyber espionage takes various forms, including eavesdropping, spreading misinformation, and remote hacking.⁷
- Cyber Terrorism: According to Dorthy E. Deming, this term refers to "the convergence of traditional terrorism with cyberspace, indicating illegal attacks targeting computers, networks, and stored information to intimidate the government and terrorize its people for political, social, cultural, or ideological objectives." To be considered terrorism, such actions must lead to damage or destruction, often using various methods, including social media networks and websites.⁸
- Cybercrime: This includes all crimes committed in a digital environment, ranging from exploiting electronic system vulnerabilities for theft and sabotage to money laundering for economic crimes such as fraud, extortion, manipulation, and destruction, often using fake identities to avoid prosecution.⁹
- Cyber Warfare: The most dangerous type of cyber challenge, this encompasses all the previously mentioned forms and results in greater losses and effects, often comparable to the impact of traditional armed warfare or conflicts occurring in the context of military disputes.

2- The Impact of Cyberattacks on International Security:

The use of cyberspace has revealed significant conflicts between the needs, values, and interests of many actors, whether state or non-state, thus shaping new methods of international conflict with

a technical nature. This has had a direct and rapidly escalating impact on international security, which can be summarized as follows:

- Increasing Cyber Risks: Particularly with the vulnerability of critical national infrastructures to attacks, affecting their operations. This makes control over the execution of such attacks a strategic tool for dominance.¹⁰
- Expanding the Scope of Conflict and Actors Involved: Cyberspace has reshaped the capabilities of influential parties, leading to a diffusion of power among multiple actors competing to protect themselves, enhance their offensive capabilities, and gain dominance. This competition is centered around control, innovation, and the manipulation of information to increase both domestic and international influence.¹¹
- Militarization of Cyberspace: The study of practical examples of cyberattacks worldwide reveals that they often reflect real conflicts among various international actors. Consequently, nations have been developing their cyber capabilities, leading to an unprecedented evolution in defense and cybersecurity policies. This includes the intensification of the cyber arms race, increased investment in developing warfare tools within modern armies, and the enhancement of information infrastructure.¹²
- Incorporating Cybersecurity into the International Security Agenda: This is evident in the heightened efforts of states, organizations, researchers, and legal experts to develop legal frameworks addressing these emerging security threats. Additionally, there is a push to strengthen international cooperation to ensure global cybersecurity and to establish an international strategy to confront the rise of cyber threats, fostering a global culture of cybersecurity.

B) The Interaction between Technology and International Law:

The significance of international law is increasing as the pace of global events intensifies, driven by the ongoing interactions state and non-state entities, especially in light of technological advancements and their consequences. This evolution makes it necessary to focus on the substance and principles of international law, developing and updating its rules to better align with the demands of the technological revolution. The need for this adaptation becomes more critical with the rising risks and threats stemming from the use of electronic and cyber weapons to achieve goals of control and influence. Consequently, legal scholars have begun to explore how cyberattacks can be addressed within the framework of rules applicable to traditional armed attacks under international law.

1- Legality of cyberattacks: between security and sovereignty

In the past five years, researchers have intensified their efforts to analyze and provide legal solutions for cyberattacks, aiming to establish a legal framework to regulate these incidents or, at the very least, adapt them to the tenets and norms of international law. This initiative arises in response to evident signs that cyberattacks threaten global peace and security on a level comparable to the most serious internationally recognized threats. However, there are dissenting voices arguing that it is impossible to apply international legal rules to cyberattacks, citing several key points, including:

- The essential tenets of international law were defined prior to the advent of electronic technology and their use for military reasons.¹³ They refer to the period when key treaties were concluded, such as the Additional Protocols of 1977, the four Geneva Conventions of 1949, and The Hague Conventions of 1899-1907, during which cyberattacks were not yet a known phenomenon.¹⁴
- The difficulty of proving material evidence resulting from cyberattacks, unlike traditional security attacks that leave tangible, direct, or indirect material traces.¹⁵
- The absence of a globally recognized definition for cyberattacks, as well as a consensus on the tools and methods used for attack and defense in such contexts.¹⁶

Thus, international law has not explicitly regulated cyberattacks. This is due to the relatively recent use of the internet and cyber networks, while the tenets of international law regulating international relations predate the existence of cyberspace. As a result, these rules may be insufficiently aligned with new technologies of warfare.¹⁷ Nevertheless, the widespread use of cyberspace as a new battleground for states has led to increased threats to international peace and security.¹⁸ Given the lack of specific legal provisions addressing these attacks in general international law, we will attempt to examine the possibility of adapting them in accordance with the foundational tenets of public international law, specifically the concept of sovereignty and the principle that prohibits the use of force or its threat.

1.1- Cyberattacks and the Principle of Sovereignty:

Cyberattacks have become one of the most modern and widely used methods to resolve conflicts between nations due to their speed, ease of use, and low cost. A state can disable the military and/or civilian infrastructure of another state with the push of a few buttons, effectively subjugating it without resorting to traditional means of warfare.¹⁹ This allows a state to exercise its jurisdiction both domestically and internationally.

The concept of sovereignty has evolved beyond its traditional political and legal interpretations, adapting to technological advancements and the emergence of cyberspace as a fifth realm in addition to land, sea, air, and outer space. Thus, the concept of cyber sovereignty has emerged, referring to a state's authority and jurisdiction over the digital space, specifically the internet. This sovereignty is crucial for protecting national security against new threats that transcend geographical boundaries.²⁰

It becomes clear that cyber sovereignty differs from cybersecurity. While cybersecurity aims to protect cyber sovereignty pertains to the information and material disseminated over the internet, seeing it as a natural extension of state sovereignty inside cyberspace, distinct from the infrastructure and activities associated with the internet.²¹ Military power is no longer the sole threat to nations and the international community; the possession of electronic power by states has become the greatest threat to the sovereignty of targeted states, whether in military, economic, cultural, or political spheres.²² This is particularly significant with the rise of e-governments, as cyberattacks increasingly target the informational systems of states with the aim of controlling or destroying data and associated infrastructure quickly and at minimal cost, with fewer legal and accountability burdens.²³

It is evident that cyberattacks carried out by one state against the virtual space of another state constitute a violation of the latter's cybersecurity and sovereignty over its installations and systems within that space, which are under its control. This makes such attacks internationally unlawful. Therefore, protecting various activities, whether commercial, civil, or otherwise, is a fundamental element in ensuring national security in the future.

1.2- Cyberattacks and the Principle of Prohibition of the Use of Force and Threat of Its Use:

The application of force or its threat against the territorial integrity or political sovereignty of any state is considered unlawful under international law, except in two circumstances:²⁴ As stipulated in Article 42 of the UN Charter, the United Nations Security Council is responsible for maintaining international peace and security through self-defense and intervention.²⁵

Technological advancements in the electronic domain have given rise to new concepts, including "cyber power," where superiority in the cyber domain has become an essential element in executing effective operations on land, at sea, in the air, and in outer space. Combat capabilities in cyberspace rely on technological control and command systems. However, it is important to distinguish between cyberattacks aimed at military purposes, such as targeting military infrastructure and military information security, and other cyberattacks without military objectives, such as information warfare, rumor dissemination, and illegal financial transactions. Only military-purpose cyberattacks, which produce effects similar to the use of conventional military force—such as large-scale killings, destruction of the infrastructure of a state, theft and manipulation of military

information, and authority over military systems is encompassed by Article 2(4) of the United Nations Charter.²⁶

The criterion for classifying cyberattacks under Article 2(4) is based on their effects and damages, not the means used. The International Court of Justice confirmed this in its advisory judgment on the legality of the threat or use of nuclear weapons.²⁷ Article 2(4) prohibits any use of force, regardless of the weapons employed. According to this viewpoint, several countries argue that exceeding the threshold for the use of force depends not on the digital techniques used, but rather on the consequences of the cyber operation. Thus, a cyber operation conducted by one state against another violates the prohibition on the use of force if its effects are similar to (or exceed) those caused by conventional weapons. In these cases, the stipulations of international humanitarian law for the protection of persons and property during armed conflicts would apply.²⁸

The definition of force under Article 2(4) of the UN Charter include extensive cyberattacks targeting civilian populations during or outside of armed conflicts. Examples include disabling computers that control water stations or dams, causing flooding in populated areas, deliberate and deadly engineering incidents, such as feeding false information to computers controlling airplanes, and nuclear power plant failures resulting in the release of radioactive materials in densely populated areas. The consequences of such attacks on civilian populations may surpass the severity of conventional warfare.²⁹ All of this does not exempt states from their responsibility to intervene under Article 2(4) of the UN Charter if cyberattacks result in tangible material effects on civilian or military objects.

This was also confirmed by the Tallinn Manual, prepared by the NATO-affiliated International Committee composed of legal and military experts in 2013. The manual asserts that real military force can be used in response to a cyberattack on a state if that attack causes loss of human life.³⁰

2- Challenges in Applying International Law to Cyberattacks:

In an era marked by significant digital interconnectivity among states and individuals in cyberspace, cyberattacks have emerged as a severe threat to international security and public safety. Given these escalating risks, it has become essential to address them effectively by applying international law and global standards. However, this task faces numerous challenges that hinder the achievement of justice in this complex virtual domain, where control or destruction of data and infrastructure can be carried out quickly, with minimal cost and accountability. These challenges raise several issues regarding the limitations and constraints of applying certain international law rules to cyberattacks, particularly during armed conflicts. Additionally, they bring into question the issue of international responsibility resulting from such attacks.

2.1- Limitations and Constraints on the Application of Certain International Law Rules to Cyberattacks:

In the face of these growing risks, it is crucial to address them through the effective implementation of international law and global standards. However, this mission faces significant challenges, particularly the limitations and constraints posed by applying certain rules of international law to cyberattacks. Some of these challenges include:

2.1.1- The Rule of Distinction and the Prohibition of Indiscriminate Attacks:

In the domain of cyberattacks, distinguishing between combatants and non-combatants, as well as between civilian and military infrastructures, poses a significant challenge, as mandated by international humanitarian law.³¹ This is due to the nature of these attacks, which can disrupt systems and infrastructure without the need for traditional military force, obscuring the distinction between military and civilian objectives. Moreover, military computer systems often overlap with commercial and civilian systems, complicating the capacity to differentiate between military and civilian uses in cyberspace. These challenges make it difficult to launch cyberattacks that solely target military infrastructure and limit their effects to specific military objectives.³²

2.1.2- The Rule of Precautionary Measures:

The 1949 Geneva Conventions' Additional Protocol, Article 75, stipulates that nations use all practicable measures to prevent or mitigate incidental damage to civilian infrastructure and civilian casualties during military operations. The challenge here lies in the difficulty of executing such attacks due to the intertwining of communication and information networks, which makes it hard to differentiate between civilian and military systems.³³

2.2- International Responsibility Arising from Cyberattacks:

Cyberattacks necessitate careful judgment of facts and the accurate determination of responsibility, particularly in light of the complexities of distinguishing systems and the technical challenges associated with cyberspace. The diverse uses of cyberattacks, including hacking, espionage, and service disruption, present significant challenges for the international community in identifying and punishing those responsible for these unlawful acts. Notably, Rule 6 of the Tallinn Manual places legal responsibility on states for their cyber activities that violate any international obligations. In this context, several legal challenges arise, including:

2.2.1- Addressing Attribution and Responsibility:

The issue of attributing responsibility for cyberattacks is a prominent legal challenge, particularly for states experiencing cyberattacks amidst heightened international tensions and conflicts. In such cases, identifying the source of an attack and confirming responsibility becomes difficult, especially if the attacks occur as reactions or responses to escalating tensions. This increases the complexity of distinguishing between involved parties and may render the attacks illegal due to crossing international borders and harming neutral parties. Investigations into cyberattacks require a combination of intelligence operations as essential material means and electronic dimensions that transcend international borders. However, accessing other countries for international intelligence investigations may be limited, as it could conflict with those countries' sovereignty and national laws.³⁴

Additionally, a significant challenge lies in determining the identity of the attacker in cyberspace, where anonymity often prevails over visibility. This makes it difficult to assign responsibility for an attack to a specific entity or individual. International law typically allocates responsibility based on identifying the parties involved in the conflict or attack, but in cases of cyberattacks where the identity of the attacker is unclear, significant challenges arise. As a result, establishing the link between cyberattacks and armed conflicts remains difficult, as does determining whether international responsibility can be attributed without clear evidence of the attacker's identity.³⁵

These challenges underscore the need for effective international mechanisms to determine responsibility in cyberattack cases, while simultaneously respecting state sovereignty and ensuring fair compensation for victims according to international law.

2.2.2- State Responsibility for Individual Actions:

Assigning a specific act to a state under international law requires substantial evidence that proves the state's effective control over individuals operating under its jurisdiction. According to the principles of indirect responsibility in international law, a state is accountable for the conduct of its citizens if full and effective control over them is established.

The specific characteristics of this effective control have been a topic of contention among international law specialists. However, the International Court of Justice (ICJ) has adjudicated that breaches of the rules of armed conflict by individuals cannot be attributed to the state unless it is proven that the state either ordered such actions or had actual control over all aspects of the cyberattack. This is not an easy task and remains a subject of ongoing research and debate, especially given the challenges of applying state responsibility rules to the use of individuals in cyber warfare operations.³⁶

Section II: Legal Protection of International Security in the Age of Technology

The widespread applications of technology have introduced numerous new challenges that are now a source of concern for all nations. Among these, cyberattacks stand out as the most

significant and pressing issue today. Consequently, the international system, in its diverse formation, has intensified its efforts to establish regulatory legal frameworks to address the transnational risks of cyber threats and their impact on the global level. These efforts aim to provide the necessary guarantees to ensure the protection of state actors, thereby achieving cybersecurity. This will be explored further in this section.

A) The International Legal Framework for Cybersecurity Protection:

With the increase in cyberattacks and the growing dangers they pose, states and international organizations have recognized the importance of international cooperation in countering these cyber threats. This section will clarify the efforts undertaken by international organizations and the contributions of legal scholarship in this regard.

1- The Role of International Organizations in Combating Cyberattacks:

This is seen via the efforts of several international organizations, including:

1.1- The United Nations (UN):

The UN has sought to ensure the safe use of technology and information networks by organizing numerous conferences and issuing several resolutions and activities via its organs (General Assembly, Security Council, Economic and Social Council). These efforts can be summarized as follows:

- Resolutions 63/55³⁷ and 121/56³⁸: Issued on December 4, 2000, and December 19, 2001, respectively, these resolutions provide a legal framework to combat the misuse of information technology for criminal purposes. The first resolution recommended that states ensure, through their laws, the confidentiality and integrity of computer systems against any attacks.
- Resolution 239/57: Issued on January 31, 2003, on the creation of a worldwide cybersecurity culture, this resolution emphasized the need to incorporate security into the planning of information systems and networks and adopt a comprehensive approach to managing them.
- Resolution 2341³⁹: Issued on February 13, 2017, this resolution urged member states to collaborate to prevent terrorists from obtaining weapons through information and communication technologies, while upholding human rights, basic freedoms, and adherence to international legal responsibilities.
- Resolution adopted on January 20, 2020: This resolution pertains to countering the exploitation of information and communication technologies and formed an intergovernmental committee of experts to formulate a comprehensive international convention aimed at combatting the illegal utilization of information technology.

1.2- The Council of Europe:

The European Council has made significant strides in regulating parts of cybersecurity. Key initiatives include:

- Recommendation No. 13/95: Issued on September 11, 1995, this recommendation addresses the challenges of criminal procedures related to information technology and encourages member states to review their procedural laws.⁴⁰
- The Budapest Convention: Signed on December 23, 2001, this was the first legal attempt to address the growing problem of cyberattacks (to be discussed in detail later).

1.3- The North Atlantic Treaty Organization (NATO):

In response to the cyberattacks that targeted Estonia's infrastructure in 2007, NATO adopted a range of measures intended to improve cybersecurity capabilities, including:

- Issuing the "Tallinn Manual" in its 2013 and 2017 editions, which serves as a non-binding legal reference for regulating cyberspace and addressing cyberattacks.
- Strengthening international security partnerships through cooperation outside treaties and with international organizations to share information and expertise on cybersecurity.

Notably, NATO established a partnership with the UN to counteract the utilization of the internet to achieve terrorist objectives.⁴¹

- Developing the necessary technical and operational skills to counter electronic security threats worldwide through various missions and operations, such as Cyber Defender, which organizes joint training exercises to respond to cyber emergencies⁴².

1.4 The International Telecommunication Union (ITU):

As a United Nations organization focused on information and communication technology, the ITU plays a key role in building trust and security in these technologies. Its efforts in drafting legal and regulatory frameworks to combat cyberattacks are particularly evident through its Global Cybersecurity Agenda launched in 2007. This initiative is a serious attempt to develop a strict protocol to coordinate and combat cybercrimes, based on five fundamental principles:⁴³

- Ensuring all countries provide their citizens with access to communications.
- Ensuring all countries protect their citizens in cyberspace.
- Ensuring that no country harbors criminals or terrorists within its borders.
- Ensuring no country launches cyberattacks against others.
- Promoting international cooperation to guarantee peace in cyberspace.

1.5- The World Intellectual Property Organization (WIPO):

This UN agency, specializing in the electronic domain, focuses on providing legal protection for computer programs and databases. After determining that patent laws could not offer sufficient protection, WIPO reached a consensus to safeguard them through global agreements, particularly TRIPS⁴⁴ and Berne⁴⁵, which urged member states to enhance their legislation, particularly in matters of copyright. These agreements also emphasized the importance of imposing penalties for trademark counterfeiting and intentional piracy in a commercial context.⁴⁶

2- The Role of Legal Doctrinal Frameworks in Combating Cyberattacks:

2.1- Budapest Convention:

The Budapest Convention represented a collective review by member nations of the Council of Europe aimed at establishing a standard criminal procedure for addressing cybercrimes. The convention consists of 48 articles, which emphasize the need for legal measures to fight computer-related crimes. The key measures taken under this convention include:

- Defining technical terms for crimes committed in cyberspace and classifying them into four main categories: (offenses against the confidentiality, integrity, and accessibility of systems and data, such as illegal access; fraud and forgery; content-related crimes, such as the production and distribution of child pornography; and crimes involving intellectual property and related rights).⁴⁷
- Outlining the methods to be adopted for investigating internet-related crimes, as specified in Articles (2-13).
- Establishing procedures for international cooperation and information exchange between states to pursue and prosecute offenders, while considering the needs of developing countries.
- Enhancing national legislation to combat cybercrime and providing necessary support to legal authorities in dealing with such crimes.
- Training legal and technical personnel to increase the capacity to effectively combat cybercrime.

2.2- Tallinn Manual:

Interpreting international law, the Tallinn Manual is the most thorough attempt to date (*jus ad bellum* and *jus in bello*) in the context of cyber warfare. In the absence of a formal stance from the United Nations, many legal academics have sought to tackle the subject of cyberattacks. One of the most prominent international responses was the publication of the Tallinn Manual on International Law Applicable to Cyber Warfare. This guidebook was created by prominent worldwide legal authorities, with the first edition published in 2013, containing 95 legal guidelines to regulate state

behavior in the realm of cyber warfare. In 2017, the second edition was released, expanding to 154 rules, providing a more comprehensive treatment of cyber operations, and addressing contentious issues raised in the first edition.⁴⁸

In the initial incarnation of the Tallinn Manual (Tallinn Manual 1.0), the "Scale and Effects Test" detailed in Article 11 was employed by experts to ascertain the threshold that a cyberattack must meet in order to be classified as an armed attack or the use of force. As per this examination, a cyberattack can be considered an armed attack if it causes significant harm or attains a certain level of severity, resulting in substantial material damage.⁴⁹

The specialists formulated this criteria based on the International Court of Justice's verdict in the Nicaragua case, viewing it as the most appropriate standard for distinguishing between actions that constitute the use of force or armed attacks. Drawing on the Nicaragua ruling, the Tallinn experts concluded that some acts, even those that may not result in significant material damage, could still meet the threshold for the use of force.⁵⁰

3- Legal Protection of Critical Infrastructure from Cyberattacks:

There is no doubt that critical infrastructure represents one of the most important strategic targets for any state, requiring protection and security from all forms of traditional and modern threats due to the material and human losses and damages that can result. The situation becomes even more severe when the infrastructure in question is critical and internet-dependent, encompassing vital sectors such as energy, electricity, water, healthcare, and nuclear reactors. Attacks on such infrastructure can have far-reaching consequences. This has necessitated the exploration of the legal dimensions that constrain the use of cyberattacks against critical infrastructure.

Marco Roscini argues that cyberattacks on critical infrastructure constitute a clear violation of paragraph 4 of Article 2⁵¹ of the United Nations Charter when such attacks reach a certain level of severity. The attacked state has the authority to employ force under Article 51⁵² of the same Charter, which allows the right to self-defense.⁵³

The United Nations, as the entity empowered to evaluate and ascertain threats to tranquility or actions of hostility, has seen its members of the Security Council classify cyber attacks aimed at key infrastructure as a danger to international peace and security. They have also advocated for the closure of the global digital gap⁵⁴. According to UN General Assembly Resolution 70/237 of 2015, which pertains to advancements in science and telecommunications within the framework of international security. This resolution confirmed the relevance of international law, specifically the UN Charter, to the utilization of information and communication technologies (ICT) by states, highlighting its necessity for preserving peace and stability, but also safeguarding human rights and basic freedoms in the utilization of ICT.⁵⁵

The Tallinn Manual clearly addresses this problem in Article 10, which prohibits the application of force against the cyber infrastructure of another state. The guideline asserts that a cyberattack on key infrastructure qualifies as an act of force, and that nations must not intentionally let their digital infrastructure to be used by external entities for actions that adversely affect other states.

Conclusion:

Cyberspace has become a new and complex environment that presents numerous challenges to international security. Its significance lies in its ability to transform the nature of conflicts between states, as cyberattacks can be carried out with secrecy, speed, and low cost compared to traditional attacks.

This research paper has addressed the legal and doctrinal frameworks for protecting cybersecurity in the age of technology. The study has shown that cyber threats have become one of the most prominent challenges to international security, given their diverse forms and cross-border effects. It reviewed international efforts and organizational frameworks aimed at providing effective protection for critical infrastructure and data against cyberattacks.

The research emphasized the significance of international entities, including the United Nations, as well as regional groups such as the European Union and NATO, in fostering international cooperation and establishing laws and procedures to combat cybercrime. Additionally, it examined the importance of legal frameworks like the Budapest Convention and the Tallinn Manual delineates the legal regulations pertinent to cyber warfare and electronic assaults.

Based on the above, we reached several conclusions:

- Lack of a Unified Legal Definition of Cyber attacks; despite various definitions provided by institutions like the ICRC, the Tallinn Manual, and legal scholars, the absence of a universally recognized and binding definition of cyber attacks hinders the formulation of a coherent and enforceable international legal framework.
- Inadequacy of Traditional International Law in Addressing Cyber Threats: existing principles such as sovereignty and the prohibition of force under the UN Charter are insufficient to cope with the nature of cyber threats, particularly given the difficulty of attribution and the non-physical nature of digital attacks.
- Cyber attacks Pose a Serious Threat to Critical National Infrastructure: attacks increasingly target vital infrastructure sectors—such as energy, finance, and communications—resulting in potentially catastrophic consequences. These attacks rival traditional military threats and require a reevaluation of legal protection measures.
- Fragmentation and Non-Binding Nature of Current International Efforts: existing international efforts (e.g., the Budapest Convention, Tallinn Manual, and various UN resolutions) remain non-binding and are inconsistently applied across jurisdictions. This legal fragmentation undermines the global capacity to deter or respond to cyber threats.
- Attribution and State Responsibility Remain Major Legal Obstacles: the principle of “effective control” as a basis for attributing individual actions to states is difficult to establish in cyberspace. This challenge weakens legal accountability and complicates the enforcement of international obligations.
- The Strategic Necessity of Strengthening International Cooperation: the study highlights the urgent need for robust and institutionalized international cooperation mechanisms to facilitate real-time information sharing, technical assistance, and legal harmonization, particularly for developing states.
- Legal Gaps Represent a Direct Threat to International Peace and Security: the inability of current international legal norms to adapt to the technological realities of cyberspace creates a vacuum that may lead to escalating global instability, cyber conflicts, and unchecked transnational threats.

1- Ihab Khalifa, *Electronic Power and the Dimensions of Transformation in the Characteristics of Power*, Future Studies Unit, Alexandria, 2014, pp. 40-43.

2- Schmitt, M. N., *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, Columbia Journal of Transnational Law, vol. 37, 1999, p. 890.

3- Mohammed El-Saghir Kaouja, *Cyber Attacks: Reality and Methods of Confrontation*, Al-Risala Journal for Media Studies, vol. 6, no. 3, 2022, p. 111.

4- Ihab Khalifa, *Electronic Power and the Dimensions of Transformation in the Characteristics of Power*, Future Studies Unit, Bibliotheca Alexandrina, 2014, pp. 40-43.

5- Alaa El-Din Farhat, *Cyber Warfare and the Future of Global Security*, Al-Naqid Journal for Political Studies, vol. 6, no. 2, 2022, p. 680.

6- Amira Abdel Azim Mohammed Abdel-Gawad, *Cyber Risks and Ways to Address Them in Public International Law*, Journal of Law and Sharia, Egypt, no. 35, 2020, p. 410.

7- Hanan Drissi, *Cyber Warfare: A Transformation in Combat Methods and Stability in Fields and Objectives*, Journal of Legal and Political Thought, vol. 6, no. 1, p. 915.

- 8- Belasel Bint Nabi Suleiman, Amrouche El-Hussein, *Electronic Threats and Cybersecurity in the Arab World*, Noumeros Academic Journal, vol. 2, no. 2, p. 166.
- 9- Hanan Drissi, *op. cit.*, p. 914.
- 10- Lamia Ben Talla, *Cyber Threats and Crimes: Their Impact on National Security and Strategies for Combatting Them*, Maalem Journal of Legal and Political Studies, vol. 9, no. 2, 2020, p. 59.
- 11- Alaa El-Din Farhat, *op. cit.*, p. 689.
- 12- Lamia Ben Talla, *op. cit.*, pp. 59-60.
- 13- Davis Brown, *Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, Harvard International Law Review, vol. 47, 2006, p. 179.
- 14- Scott J. Shackelford, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, in C. Czossek and K. Podins (eds.), CCD COE Publications, Tallinn, Estonia, 2010, p. 202.
- 15- Michael Schmitt, *Bellum Americanum: The Law of Armed Conflict into the Next Millennium*, Newport, Naval War College, 1998, p. 408.
- 16- Clémentine B., *Understanding Cyber Warfare in International Law: Some Reflections and Clarifications*, *La Revue des Droits de l'Homme*, Revue du Centre de Recherche et d'Études sur les Droits Fondamentaux, 2014, pp. 4-24.
- 17- Omar Mohammed Aomar, *Electronic Warfare in International Humanitarian Law*, *Darat Journal for Sharia and Law Studies*, vol. 46, no. 3, p. 136.
- 18- Walter Peretti, *La Souveraineté à l'Épreuve des Cyberattaques «Supply Chain»*, Conférence des Grandes Écoles, 28 September 2021, online: <https://www.cge.asso.fr/liste-actualites/la-souverainete-a-lepreuve-des-cyberattaques-supply-chain/>.
- 19- It is noted here that the concept of sovereignty has been associated with the earliest beginnings of the modern state and the organization of the international community. The Treaty of Westphalia of 1648 is considered the first international instrument to establish the foundations of this concept, which has undergone several developments to adapt to new situations arising from the evolution of the international community in various fields. Traditionally, sovereignty has a political meaning, referring to "the supreme authority of the state internally and its independence from others externally." From a legal perspective, sovereignty is "the international term that indicates the legal capacity of the state, distinguishing it from other subjects of international law." For more on this subject, see: Mohammed Talaat Al-Ghoneimi, *Al-Ghoneimi, The Intermediate in the Law of Peace*, Mansha'at Al-Maaref, Alexandria, 1993, p. 319. Also see: Dakhlef Sofiane, *The Legal Qualification of Cyber Attacks in Light of International Law Provisions*, *The Academic Journal of Legal Research*, vol. 13, no. 2, 2022, p. 307.
- 20- The concept of cyber sovereignty is closely linked to the concept of cybersecurity, which encompasses the technical and administrative measures used to prevent unauthorized use, misuse, and recovery of electronic information and the communication and information systems it contains. This is aimed at ensuring the availability and continuity of information systems, protecting the confidentiality of personal data, and taking all necessary measures to safeguard citizens and consumers from risks in cyberspace. Thus, any attack by one state against the electronic networks of another state, intended to disrupt the operations of public and private activities and facilities of the targeted state, falls under this concept. See: Dakhlef Sofiane, *op. cit.*, p. 308. Also refer to: Hossam Jasem Mohammed Ahmed Al-Dulaimi, *Technological Development and Its Impact on State Sovereignty*, Master's thesis, Faculty of Law and Political Science, Anbar University, Iraq, 2018, p. 114.
- 21- Cybersecurity is the ongoing effort to protect the networks and data of institutions and individuals from unauthorized use or any harm or intrusion that may affect the network. For more on this topic, see: Mohammed Saad Mahmoud, *Cyber Warfare: Its Tools, Fuel, and Losses*, p. 2, available at: <https://www.Noor-Book.com>.

22- Mohammed Atef Imam Ibrahim, *Cyberspace and Its Impact on National Security: The Case of Electronic Wars*, Democratic Arab Center, published in April 2022, available at: <https://democraticac.de/?page-id=60141>.

23- Dakhlef Sofiane, *op. cit.*, p. 309.

24- Vladimir Szoke-Pellet, *State Cyber Attacks and the Notion of Aggression in International Law*, Master's Thesis in Public International Law, Aix-Marseille University, Faculty of Law and Political Science, 2017/2018, p. 14.

25- The prohibition of the use of force aligns with another principle in the Charter, which is the principle of non-interference in the internal or external affairs of another state. This has been affirmed by the International Court of Justice in several cases, as it reinforces and complements the principle of respecting state sovereignty over its territory. Intervention is considered an internationally unlawful act, as it constitutes an assault on the sovereignty and independence of states and poses a serious threat to the international public order in contemporary society. See: Article 2, paragraph 7 of the United Nations Charter. Also refer to: International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, 27 June 1986, Summary of Judgments and Advisory Opinions of the International Court of Justice 1948–1991, United Nations Publications, New York, 1999, p. 212, available at: <https://www.icj-cij.org/ar>

26- Dakhafi Sofiane, *op. cit.*, p. 313. See also: Szoke-Pellet, Vladimir. (2018). *Les cyberattaques étatiques et la notion d'agression en droit international* [State cyberattacks and the notion of aggression in international law] (Master's thesis, Aix-Marseille University, Faculty of Law and Political Science), p. 07.

27- The court concluded that the applicable law regarding the matter before it, which has the greatest direct relevance, is the law related to the use of force as stated in the United Nations Charter, alongside the law applicable to armed conflict. The court also noted that the correct application of the law should take into account the unique characteristics of nuclear weapons, particularly their destructive power, their capacity to cause immeasurable human suffering, and their potential to harm future generations. Therefore, it emphasized that there are no provisions specifically mentioning certain weapons. See: International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion issued on 8 July 1996, Summary of Judgments and Advisory Opinions of the International Court of Justice 1992–1996, United Nations Publications, New York, 1998, p. 2016, available at: <https://www.icj-cij.org/a>

28- Commentary on Paragraph 1 of the Explanation of Rule 69 of the "Tallinn" Manual on International Law Applicable to Cyber Warfare, prepared by a group of international experts, 2013, translated by Ali Mohammed Kazem Al-Mousawi, 2017, available at: <https://www.academia.edu>.

29- It has been considered that serious cyberattacks constitute an armed attack, even in the absence of personal injuries, similar to conventional attacks that do not result in injuries or property damage. There is no basis for reaching a different conclusion regarding cyberattacks against civilian systems. See: 32nd International Conference of the Red Cross and Red Crescent, Geneva, Switzerland, 8-10 December 2015, Report on International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, document prepared by the International Committee of the Red Cross.

Also refer to: Dakhlef Sofiane, *op. cit.*, p. 314.

30- Chapter 14 of the Tallinn Manual on International Law Applicable to Cyber Warfare.

31- International humanitarian law prohibits indiscriminate attacks directed at military and civilian targets without distinction, and measures must be taken to minimize civilian damage to the greatest extent possible. See: Ali Abdullah Al-Sadiq, *Cyber Weapons in Light of Contemporary International Law*, Series of Papers, no. 23, Future Studies Unit, Bibliotheca Alexandrina, Egypt, 2016, p. 96.

- 32- Ben Nasser Belkacem, Haidara Mohammed, *Cyber Attacks and Their Response in Light of Contemporary International Law*, *Journal of Human Rights and Public Freedoms*, no. 4, June 2017, p. 202.
- 33- Ali Abdullah Al-Sadiq, *op. cit.*, p. 101.
- 34- Ben Nasser Belkacem, Haidara Mohammed, *op. cit.*, p. 203. Also refer to: Ali Abdullah Al-Sadiq, *op. cit.*, p. 122.
- 35- Cordula Drouguie, "There Is No Legal Void in Cyberspace," interview dated 16 August 2011, International Committee of the Red Cross, available at: <https://www.icrc.org>, accessed on 28 June 2024 at 16:30.
- 36- In this regard, experts in international law call for the development of international responsibility rules to ensure that those affected by the damages resulting from cyber warfare attacks are not obstructed from receiving just compensation. See: Talal Yassin Al-Eissa, Oday Mohammed Anab, *International Responsibility Arising from Cyber Attacks in Light of Contemporary International Law*, *Zarqa Journal for Research and Human Studies*, vol. 19, no. 1, 2019, pp. 90-91.
- 37- Available at: <https://www.un.org/ar/ga/63/resolutions.shtml>.
- 38- Available at: https://www.unodc.org/pdf/crime/a_res_56/121a.pdf.
- 39- Available at: <https://documents.un.org/doc/undoc/gen/n17/038/58/pdf/n1703858.pdf?token=QF3h4BNluqCQH8X8FZ&fe=true>.
- 40- Available at: <https://rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174>.
- 41- Zghib Amina, Ziani Saleh, *Evaluating the Strategic Doctrine of NATO: From Military Containment to Cyber Containment – Changes in Performance and Maintaining the Role*, *Journal of Legal and Political Research*, vol. 8, no. 3, 2023, p. 10.
- 42- *Ibid.*, p. 11.
- 43- Amira Abdel Azim Mohammed Abdel-Gawad, *op. cit.*, p. 512.
- 44- The TRIPS Agreement: The Agreement on Trade-Related Aspects of Intellectual Property Rights, abbreviated as TRIPS, is an international agreement administered by the World Trade Organization (WTO) that sets minimum standards for laws concerning various forms of intellectual property (IP).
- 45- The Berne Convention: The Berne Convention for the Protection of Literary and Artistic Works (in English: Berne Convention) is a global agreement focused on protecting the intellectual rights of authors and others. It was first held in Bern, Switzerland, in 1886. The convention has been amended in various conferences and discussions, with the latest version adopted in Paris on September 28, 1979.
- 46- Ben Ali Ben Jeddou, *Challenges of Cybersecurity in Combatting Cybercrime*, *Algerian Journal of Cybersecurity*, vol. 7, no. 2, 2022, p. 310.
- 47- Available at: <https://rm.coe.int/budapest-convention-in-arabic/1680739173>.
- 48- Article (30) of the first edition of the Tallinn Manual defines a cyber operation as "an electronic operation, whether defensive or offensive, that may cause injury or death to individuals, or damage or destruction to facilities." See: Sharif Nasim Qilta Bakhit, *The Tallinn Manual: Cyber Attacks and the Prohibition of the Use of Force in International Law*, article published on the Arab Center for Cyber Space Research website, dated 25 November 2017 (last accessed on 28 June 2024 at 17:00): available at: https://accronline.com/article_detail.aspx?id=28958
- 49- *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Michael N. Schmitt (ed.), 2013, pp. 45-46.
- 50- In this regard, the court ruled in the Nicaragua case that the arming and training of the Contras by the United States to fight the legitimate government of Nicaragua constitutes an unlawful use of force. For more on this topic, see: Sharif Nasim Qilta Bakhit, *The Tallinn Manual: Cyber Attacks*

and the Prohibition of the Use of Force in International Law, *op. cit.*, available at: https://accronline.com/article_detail.aspx?id=28958

51- Paragraph 4 of Article 2 of the United Nations Charter states that all members of the organization shall refrain, in their international relations, from the threat of the use of force or from using force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.

52- Article 51 of the United Nations Charter states that the natural right of states, individually or collectively, to defend themselves is acknowledged in the event of an armed attack against a member of the United Nations, until necessary measures are taken to maintain international peace and security.

53- Marco Roscini, *Worldwide Warfare, Jus ad Bellum, and the Use of Cyber Force*, *Max Planck Yearbook of United Nations Law*, vol. 14, 2010, p. 130.

54- Boutlata Widad, Boukoro Manal, *Cyber Attacks on Critical Infrastructure: A Study in Light of Public International Law*, *Journal of Human Rights and Public Freedoms*, vol. 7, no. 2, 2022, p. 344.

55- *Ibid.*, p. 344.

Bibliography:

A - Books:

1. Eihab Khalifa. *Electronic Power and the Dimensions of Transformation in the Characteristics of Power*. Alexandria, Egypt; 2014.
2. Amira Abdel Azim Mohamed Abdel Gawad. *Cyber Risks and Ways to Confront Them in Public International Law*. Egypt; 2020.
3. Boutlata Wedad & Boukoro Manal. *Cyberattacks on Critical Infrastructure: A Study in Light of Public International Law*. Algeria; 2022.
4. Bellasel Bent Nabi Suleiman & Amrouch El-Hussein. *Cyber Threats and Cybersecurity in the Arab World*. Algeria; 2022.
5. Ben Nasser Belkacem & Haidara Mohamed. *Cyberattacks and Their Confrontation in Light of Contemporary International Law*. Algeria; 2017.
6. Ben Aliya Ben Jeddo. *Challenges of Cybersecurity in Facing Cybercrime*. Algeria; 2022.
7. Alaa Eldin Farhat. *Cyber Warfare and the Future of Global Security*. Algeria; 2022.
8. Hanan Drissi. *Cyber Warfare: A Shift in Combat Methods and Stability in Fields and Objectives*. Algeria.
9. Cordula Droege. "No Legal Vacuum in Cyberspace". International Committee of the Red Cross, Geneva, Switzerland. (consulted on 28/06/2024 at 16:30). Available at: <https://www.icrc.org>.
10. Lamya Ben Tala. *Cyber Threats and Crimes: Their Impact on National Security and Strategies to Combat Them*. Algeria; 2020.
11. Mohamed El-Saghir Kawja. *Cyberattacks: Reality and Ways to Confront Them*. Algeria; 2022.
12. Hamad Saad Mahmoud. *Cyber Warfare: Tools, Fuel, and Losses*. (consulted on day/month/year). Available at: <https://www.Noor-Book.com>.
13. Mohamed Atef Imam Ibrahim. *Cyberspace and Its Impact on National Security: Cyber Wars as a Model*. Arab Democratic Center, Egypt; 2022. (consulted on day/month/year). Available at: <https://democraticac.de/?page-id=60141>.

14. Zgheib Amina & Ziani Salah. *Assessment of NATO's Strategic Doctrine: From Military Containment to Cyber Containment – Change in Performance and Continuity in Role*. Algeria; 2023.

B - Theses:

1. Vladimir Szoke-Pellet. *State Cyberattacks and the Notion of Aggression in International Law*. Master's Thesis, Public International Law, Aix-Marseille University, France; 2017/2018.

C - Newspaper articles:

1. Davis Brown. *Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*. Harvard International Law Review, Vol. 47, USA; 2006.
2. Michael Schmitt. *Bellum Americanum: The Law of Armed Conflict into the Next Millennium*. Naval War College, Newport, USA; 1998.
3. Schmitt, M. N. *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*. Columbia Journal of Transnational Law, Vol. 37, USA; 1999.
4. Scott J. Shakleford. *State Responsibility for Cyberattacks: Competing Standards for a Growing Problem*. CCD COE Publications, Tallinn, Estonia; 2010.
5. Marco Roscini. *Worldwide Warfare: Jus ad Bellum and the Use of Cyber Force*. Max Planck Yearbook of United Nations Law, Vol. 14, Germany; 2010.

E - Websites:

1. Cordula Droege. "No Legal Vacuum in Cyberspace". International Committee of the Red Cross, Geneva. Available at: <https://www.icrc.org>
2. Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013). Available at: https://accronline.com/article_detail.aspx?id=28958
3. Walter Peretti. *Sovereignty Tested by Cyberattacks on the Supply Chain*. Conference of Grandes Ecoles, France, September 28, 2021. Available online: <https://www.cge.asso.fe/liste-actualites/La-souveraineté-à-lepreuve-des-cyberattaques-supply-chain/>