Pegem Journal of Education and Instruction, Vol. 16, No. 2, 2026 (pp. 846-866)

RESEARCH ARTICLE WWW.PEGEGOG.NET

Cyberattacks in Light of the Contemporary International Regulatory

Dr. Hayat Ferd

University of Akli Mohand Oulhadj, Bouira, Algeria
Email: h.ferd@univ-bouira.dz

Received: 17/11/2025 ; Accepted: 15/04/2025 ; Published: 23/06/2026

Abstract:

This paper explores the concept of cyberattacks, cyberspace and related terminology, and examines their characteristics in the context of rapid technological development, It analyzes the impact of cyberattacks on the contemporary international system, particularly their implication for state security and stability, as well as issues of international responsibility and the adequacy of existing international law.

This paper concludes that cyberattacks are a major security threat targeting critical infrastructure beyond national borders, It also highlights the challenges of attributing attacks and enforcing international responsibility, emphasizing the need for stronger international cooperation and updated legal frameworks to enhance global security.

Keywords: Cyberattaks- contemporary International system- International responsibility

Introduction

Over the past decades, the concept of security has undergone fundamental transformations driven by the political, technological, and economic developments experienced worldwide. Security is no longer limited to its traditional dimension associated with protecting the state from external military threats; rather, it has expanded to encompass multiple dimensions within what is known as the concept of human security, which focuses on protecting individuals, states, and societies from various risks and threats. The United Nations Development Programme (UNDP) has identified seven main dimensions of human security: economic security, food security, health security, environmental security, personal security, community security, and political security. With the rapid advancement of information and communication technologies, a new dimension has emerged that is no less important than these dimensions: cybersecurity, which has become one of the fundamental pillars of national and international security in the digital age.

In light of the increasing reliance on information systems and digital networks in managing various vital sectors of states, cyberspace has emerged as a new arena for interaction, competition, and conflict. This has led to the emergence of non-traditional

security threats, primarily in the form of cyberattacks. These attacks have become a growing threat to the security and stability of states due to their ability to target critical infrastructure, disrupt essential services, penetrate military and economic systems, and inflict significant damage without the need for conventional military force.

In this context, the world is currently witnessing a new form of strategic competition among states based on the development of cyber capabilities and electronic software with military and security applications. This reflects the shift of international conflict into a new digital domain where technical, legal, political, and security considerations intersect.

The seriousness of these threats has prompted researchers and international organizations to intensify studies and efforts aimed at understanding the nature of cyberattacks and their impact on international peace and security, particularly in light of evidence indicating that cyberattacks may have consequences comparable to some of the most dangerous security threats known in contemporary international relations.

Accordingly, this study seeks to shed light on the phenomenon of cyberattacks as one of the most prominent emerging security challenges within the contemporary international system by addressing the following research question:

What is the nature of cyberattacks, and how do they affect international security within the framework of the contemporary international system?

Based on this, the following main hypothesis is proposed:

Cyberattacks constitute a new form of non-traditional security threat and have increasingly affected international security through targeting states' critical infrastructures and causing disruptions to international peace and stability.

Sub-Hypotheses

The greater the dependence of states on digital technologies and information systems, the more vulnerable they become to cyberattacks.

Cyberattacks possess characteristics that make them more complex than traditional security threats, particularly regarding the difficulty of identifying their source and attributing responsibility.

Large-scale cyberattacks threaten the national security of states and may extend their effects to regional and international security.

Strengthening international cooperation and developing cybersecurity mechanisms contribute to reducing the risks posed by cyberattacks to international security.

To address the research problem and test the above hypotheses, this research paper has been divided into three main sections as follows:

First: The Concept of Cyber Attacks

Second: Actors in Cyberspace

Third: Cyber Attacks in the Contemporary International System

First: The Concept of Cyber Attacks

1. Cyberspace

The term cyber is derived from the word Cyber, which originates from Cybernetics. It refers to anything related to computers, information technology, virtual reality, and computer culture.[i] Therefore, the term cyber generally refers to the Internet space.

This term was first introduced by the American mathematician Norbert Wiener to describe automatic control, communication, and regulation in both animals and machines, emphasizing mechanisms of self-organization.[ii]

The concept of cybernetics expresses what is known as the digital space, which can be approached from multiple perspectives. It is considered a social space for interaction and exchange; however, it has also become a vital and strategic arena in which numerous conflicts and digital attacks take place.[iii]

The French National Cybersecurity Agency (ANSSI) defines cyberspace as: "a communication environment created through the global interconnection of digital data-processing equipment."

This definition focuses primarily on the technical dimension of cyberspace by emphasizing technical connectivity. Consequently, it limits the concept to technical specialists and excludes the general public and researchers from other disciplines. Moreover, it overlooks the human element, which is an essential component in understanding cyberspace.

Accordingly, cyberspace can be defined as:

"A complex domain, both physical and non-physical, composed of computers, network systems, software, information-processing technologies, and the fundamental processes of data transmission and storage, as well as the users of these components."[iv]

The issue of defining cyberspace remains relative and depends on how each state perceives its national security. For this reason, some scholars consider cyberspace to be the fourth arm of modern armed forces.

Strengthening the conceptual understanding of cyberspace requires analyzing its structural composition, which can be viewed as consisting of three layers:[v]

a. The Physical Layer:

Includes computers, software, and all equipment necessary for interconnection and networking.

b. The Logical Layer:

Consists of programs that translate information into digital data. It involves the transformation of human language into machine language through algorithms, followed by software developed using programming languages.

c. The Information Layer:

Represents the social dimension added to the previous two layers. In the digital environment, an individual may possess multiple digital identities, such as an email address, mobile phone number, and avatars or profiles on social networking platforms.

2. Cyber Attacks

Cyber attacks primarily involve breaching the websites and information systems of states, particularly those related to strategic sectors such as defense, energy, and telecommunications. These attacks may take the form of espionage, service disruption, or the theft of sensitive information, especially from strategic sectors like defense, energy, and communications.

Cyber attacks therefore represent a prominent form of activity in the virtual world, which is fundamentally based on the use of digital data and electronic means of

communication. Over time, the concept has evolved to encompass broader implications aimed at achieving tangible and direct military and security objectives through the penetration of sensitive electronic systems.[vi] Such attacks often target systems that perform critical functions, including the protection of nuclear power plants, electrical facilities, airports, and other transportation infrastructures.

Among the definitions provided by experts in international humanitarian law is that of Shane, who describes a cyber attack as:

"The use of the electromagnetic or electronic spectrum to store, modify, and exchange information directly with control systems connected to infrastructure."

Similarly, Fiorenza defines a cyber attack as:

"Unauthorized access to electronic systems or websites with the aim of destroying, disrupting, or controlling the information contained within them. It constitutes a set of electronic attacks carried out by one state against another."

Schmitt defined it as: "A set of measures adopted by a state to attack hostile information systems with the aim of influencing and damaging them, while simultaneously protecting the information systems of the attacking state."

Zimet and Barry described it as a set of operations related to cyber warfare and psychological manipulation, in addition to targeting the enemy's military communications network and its cyber security operations.

Finally, Marco Roscini defines this concept as: "The use of military cyber capabilities to affect, disrupt, or destroy other websites and information systems, whether they provide civilian or military services."

3. Concepts Related to Cyber Attacks

A. Cybercrime

Cybercrime consists of unlawful electronic activities carried out through computer-based means. It has also been defined as any illegal act committed through electronic media such as computers, mobile devices, communication and information networks, the Internet, and the unlawful use of computer or electronic data in general.

This concept shares with cyber attacks the environment in which it occurs, namely cyberspace. However, the key distinction between the two lies in the legal aspect. An act cannot be classified as a cybercrime in the absence of a legal provision defining it and specifying its constituent elements. In contrast, an act may be considered and described as a cyber attack simply because it occurs within cyberspace, regardless of whether it falls under a specific legal classification.[vii]

B. Cyber Warfare

Cyber warfare is defined as a set of combat methods and means that rely on information and communication technologies and are employed in the context of armed conflicts. It includes attacks and operations conducted through computer networks and data systems by states or organized armed groups during armed conflict. It may also form part of mutual deterrence strategies between conflicting parties.

Cyber warfare is considered the fourth domain of modern warfare, alongside the land, maritime, and air domains, due to its covert nature, its ability to penetrate electronic systems, and its potential to precede conventional military operations. It targets the

critical civilian and military infrastructure of states, including smart networks and Supervisory Control and Data Acquisition (SCADA) systems, which constitute essential pillars for operating vital facilities and enhancing defensive capabilities.

Although there is an overlap between cyber warfare and cyber attacks occurring during armed conflicts, the two concepts are not entirely identical. Cyber attacks may occur during both peacetime and wartime and target digital systems through malicious means to achieve security, military, or political objectives, such as disrupting institutions or destabilizing governments. Cyber warfare, however, is distinguished by the fact that its effects may extend beyond the digital domain to produce tangible physical and kinetic consequences affecting a state's infrastructure and military capabilities.[viii]

C. Cyber Terrorism

Cyber terrorism refers to a type of cyber attack directed against governments, institutions, or societies with the aim of threatening or harming them in pursuit of political, ideological, or religious objectives. Such attacks must produce destructive or disruptive effects comparable in severity to those of traditional terrorist acts and contribute to spreading fear and panic among targeted individuals or groups.

Cyber terrorism is also defined as any activity that employs digital or electronic means to carry out or threaten violence, directly or indirectly, in order to achieve specific political objectives. This activity may take various forms, including disrupting critical systems, sabotaging digital infrastructure, or targeting sensitive data and information in ways that cause serious harm to society or the state.

In this context, researcher Dorothy Denning defined cyber terrorism as attacks or threats directed against computers and information networks with the purpose of influencing governments or societies and coercing them into adopting particular political, religious, or ideological positions or policies. She argues that such attacks should only be classified as cyber terrorism when they reach a level of destruction and disruption capable of generating fear and terror comparable to the effects of traditional physical terrorist acts.[ix]

D. Information Crime and Cybercrime

The increasing expansion of Internet usage across various transactions and electronic activities has created a favorable environment for the emergence of new forms of criminal behavior, commonly referred to as cybercrime. These crimes have been closely associated with the rapid advancement of information and communication technologies and the growing reliance of individuals and institutions on digital systems for data management and exchange.

Cybercrime differs from information crime in terms of its scope and methods of commission. Its emergence coincided with the development of computer systems and information security assessment mechanisms. These crimes rely on the exploitation of computers and electronic networks to gain unauthorized access to information or manipulate data and digital systems for unlawful purposes, typically through the use of two or more devices connected via the Internet.

In contrast, information crime is primarily concerned with attacks against information systems or the data stored and processed within them, whereas cybercrime

encompasses a broader range of criminal acts committed through electronic media and communication networks. Nevertheless, both cybercrime and information crime are perpetrated within the cyberspace environment provided by the Internet.[x]

E. Cybersecurity

The concept of cybersecurity refers to a set of public policies, security measures, risk management strategies, technologies, procedures, and guidelines adopted to protect computers, networks, and the data stored or transmitted through them. Cybersecurity aims to ensure the confidentiality, integrity, and availability of information by addressing various digital threats and risks.

Cybersecurity is also defined as the collection of practices and technologies designed to protect information systems, networks, and software from cyberattacks. Such attacks often seek unauthorized access to sensitive information, its modification or destruction, or its exploitation for illicit activities such as cyber extortion or the disruption of business operations and critical services. Consequently, cybersecurity constitutes one of the fundamental pillars for ensuring business continuity and safeguarding digital infrastructure amid the continuous growth of cyber threats.[10]

Second: Actors of Cyberattacks in Cyberspace

The structure of actors in cyberspace consists of two principal levels. The first is the state level, which includes states as sovereign actors possessing organizational and technical capabilities in the cyber domain. The second is the non-state level, which encompasses various non-governmental actors such as organized groups, private companies, and individuals who play influential roles within cyberspace.[xi]

State Actors

State actors in cyberspace refer to the state's exercise of authority, within a legal and regulatory framework, over the management of this virtual space through its various institutions and agencies, including ministries and security and military bodies. The state is considered a central actor in the governance of cyberspace due to its material, human, structural, and legislative resources that enable it to exert control over this domain.

In this context, many countries have witnessed significant advancements in their cyber capabilities. It has been noted that by 2008, approximately 180 states had developed advanced cyber capabilities, including both offensive and defensive cyber tools and technologies. This development contributed to a shift among some states from a purely defensive approach toward a more offensive posture in cyberspace.

Accordingly, it has become imperative for states to strengthen their capacity to control and manage this vital domain, particularly in light of the growing number of competing actors in cyberspace, some of whom may pose threats to state interests and national security.[xii]

Non-State Actors:

Non-state actors in cyberspace include various individuals, groups, non-governmental organizations, and private companies that have increasingly acquired the ability to influence states' orientations and policies through the use of cyberspace. This development reflects the transformation in the nature of relationships within the digital

environment, where influence is no longer limited to state actors alone but has expanded to include non-governmental entities capable of utilizing digital media to achieve diverse objectives.

In this context, these non-state actors have become capable of exerting direct or indirect influence on decision-making processes, whether through the dissemination of information and the shaping of public opinion, or through the exploitation of digital platforms for mobilization, influence, and pressure. This section examines the most significant of these actors by classifying them and analyzing their roles in cyberspace.[xiii] The most important of these actors are as follows:

A. The Individual

The individual is considered one of the most prominent actors in cyberspace. With the rapid pace of digital transformation, individuals have acquired an increasingly important role and have become capable of generating profound impacts that may even lead to digital revolutions, transforming patterns of communication and interaction within society. In some cases, these individual innovations evolve into tools upon which states and institutions rely for managing their affairs or developing their digital services.

In this regard, the creation of the social networking platform Facebook represents one of the most significant examples of this role. In 2004, Mark Zuckerberg founded the platform, which quickly became one of the largest social networks in the world, eventually attracting more than one billion users globally. This demonstrates the extent of influence that individual actions can have in cyberspace.

The individual can be classified according to the roles or positions they adopt, as follows:

• Internet User

The functional manifestation of the individual in cyberspace lies in their role as a user of the Internet and computer networks, whether these networks are independent or connected to the Internet. This role reflects the individual's ability to interact with the digital environment through various technological tools and applications, enabling access to, exchange, and processing of information through available information systems.

• Citizen

Every individual is a citizen of a state and has the opportunity to participate in public debate through cyberspace, thereby enhancing their presence in the digital public sphere. In this context, every Internet user has the right to contribute equally to this space by expressing opinions, exchanging information, and participating in various interactive activities.

Accordingly, cyberspace is viewed as a suitable domain for promoting participatory democracy, as it offers broad opportunities for participation and interaction among individuals without traditional constraints, thereby reinforcing the principles of equal access to information and freedom of expression.

• Fraudster

An Internet user may engage in unlawful practices, including fraud and deception, which are criminal acts committed through computers and wired or wireless communication technologies. These activities aim to secure illegitimate personal benefits, often financial in nature, by exploiting digital media to deceive victims, manipulate them, or unlawfully obtain money or other advantages.

• Consumer

As a result of developments in media and communication technologies, points of contact with consumers have increased, facilitating commercial transactions and contributing to changes in traditional consumer purchasing habits.

• Unskilled Adopter (Script Kiddie)[xiv]

This refers to an individual who uses codes, scripts, programs, or software developed by others to attack computer systems or networks and to compromise, disrupt, or dismantle websites.

B. The Group

Groups may be either small or large collections of individuals who share common objectives. These include:

• Companies

Cyberspace is a relatively new domain that necessitates its inclusion within companies' strategic roadmaps and planning processes, particularly because it serves both as a source of opportunities and as a reservoir of potential threats.

• Media Organizations

The emergence of cyberspace has brought about a fundamental transformation in the media sector through the convergence of information and communication technologies with traditional media. Conventional media such as print journalism, television, and posters have increasingly been supported by software applications that enable their content to be digitized, processed, and distributed instantly to a wider audience.

Criminal Groups:

Criminal groups have been presented with golden opportunities and enhanced capabilities to develop their tools and methods. They have shifted much of their activity into cyberspace and worked on refining their tactical plans, largely thanks to the dark web, which ensures anonymity. Furthermore, digital transformation has undermined traditional methods of tracking financial movements, as financial transactions are now conducted through complex and rapid electronic channels. This has made financial monitoring and tracking through conventional methods more difficult. Such developments have reshaped financial auditing mechanisms and imposed new challenges on regulatory authorities, requiring them to adapt to the nature of digital financial flows.

Terrorists:

Terrorists have developed numerous methods for exploiting cyberspace, naturally for unlawful purposes. Cyberspace also provides opportunities for gathering intelligence and conducting various activities related to terrorism, which necessitates efforts to counter and prevent such terrorist acts.

Hacktivists:

This category consists of groups of individuals who adopt an ideological commitment that favors direct action through the Internet. They use cyberspace as a means of expression, influence, or protest. In this context, hacking represents the intensive and continuous use of cyberspace, whether through legal or illegal means, to exert pressure, express a public stance, promote a particular ideology, or support a specific political agenda.

Hackers are generally regarded as individuals possessing advanced knowledge and a deep understanding of computer technologies, including how hardware, software, and networks interact. This expertise enables them to exploit technical vulnerabilities or utilize them for various activities. Hackers can be classified into three main categories:

White Hat Hackers: These individuals do not engage in illegal activities and are commonly referred to as ethical hackers. They operate with official authorization and the consent of system owners to identify and disclose security vulnerabilities.

Gray Hat Hackers: These hackers explore and test techniques that may resemble criminal methods. They often search for security vulnerabilities in systems without obtaining prior permission from the owners. Upon discovering weaknesses, they typically report them to the system owners for remediation, often in exchange for financial compensation. Their primary motivation is usually to demonstrate their skills, gain recognition, and receive appreciation for what they consider a contribution to cybersecurity.[xv]

Black Hat Hackers: These are considered the most dangerous type of hackers. They are criminals who infiltrate computer networks with malicious intent. They violate the law and use their skills to cause harm and damage.

Non-Governmental Organizations (NGOs):

Non-governmental organizations may also be considered actors capable of conducting cyberattacks, despite lacking the resources and capabilities of a state. Their capabilities are generally limited compared to those of governments. Consequently, their attacks are usually directed at relatively low-value targets, such as websites, with the aim of achieving modest gains before being detected and subjected to legal action.[xvi]

Third: Cyberattacks under the Contemporary International Legal Order

Contemporary international legal scholarship has addressed cyberattacks as one of the emerging challenges resulting from the development of digital technology, raising a number of fundamental legal issues. The first issue concerns the extent to which the rules of public international law, particularly those of international humanitarian law (IHL), apply to this type of attack. In the absence of explicit legal provisions directly regulating cyberattacks, the question arises as to whether such attacks can be subjected to the existing international legal framework or whether they constitute an area characterized by a relative legislative gap that limits the effectiveness of traditional legal rules in regulating and controlling them.

From another perspective, scholars raise a parallel issue concerning compliance with the principles of legality and legitimacy in the use of cyber means. This involves examining the extent to which cyber operations are governed by the principles of international humanitarian law, particularly the principles of military necessity,

proportionality, and distinction between civilian and military objectives when force is used. This raises questions regarding the application of these principles within cyberspace, a domain characterized by its immaterial nature and the extensive interconnection between civilian and military infrastructures, and the resulting difficulties in legal classification and the determination of international responsibility.[xvii]

Some legal scholars argue that cyberattacks can be legally classified not only within the framework of codified international humanitarian law but also within the broader scope of public international law as a whole. This approach is based on the practical nature of cyberattacks, which demonstrates that they may occur in the context of international or non-international armed conflicts, as well as during peacetime. Consequently, the scope of their legal characterization expands, rendering them subject to various branches of international law depending on the circumstances in which they occur.

Within this framework, this perspective raises several additional legal issues, most notably the question of international responsibility arising from cyberattacks during peacetime, as well as the need to reconsider the concepts of sovereignty and jurisdiction in light of the borderless nature of cyberspace and the difficulty of accurately identifying the source of an act or attributing it to a specific state.

Another highly significant issue concerns the ambiguous nature of attributing cyberattacks. States often refrain from officially acknowledging responsibility for such attacks, while individuals or non-state groups may claim responsibility for them. This creates substantial challenges for the international legal system in identifying the actual perpetrator and establishing international responsibility.[xviii]

In this context, questions arise regarding the legal standards that should be adopted for attributing such acts to states, and whether the criterion of "effective control" or that of "overall control" is sufficient in this regard, or whether a combination of both should be employed depending on the specific circumstances. In other words, the issue concerns determining which standard is more appropriate for establishing international responsibility for cyberattacks: the effective control test, which focuses on the degree of a state's actual direction and supervision over the actors involved; the overall control test, which requires a higher degree of dependency and dominance; or whether the unique nature of cyberspace necessitates a hybrid approach that combines both standards in order to ensure effective legal attribution and achieve international justice.

From the perspective of the legal characterization of cyberattacks, it is evident that the concept of such attacks continues to generate considerable scholarly disagreement. This has given rise to a deeper issue confronting international law specialists, namely how these acts should be legally classified and what legal basis should underpin such classification—whether it should derive from the principles of public international law or from the specific rules and provisions of international humanitarian law.[xix]

This issue becomes even more acute if one accepts the existence of a legal vacuum concerning cyberattacks, meaning the absence of explicit and specific international rules regulating this emerging type of attack. This raises a fundamental question

regarding the applicable legal rules in such situations. The importance of this question continues to grow in light of the expanding use of cyber means and the increasing risks associated with them, which may pose a direct threat to international peace and security and consequently require a reassessment of the adequacy of the existing international legal framework and its ability to keep pace with these developments.

A review of the opinions of specialists relevant to this study reveals a clear divergence of scholarly positions regarding the legal characterization of cyberattacks. One school of thought maintains that the principles and rules established by international humanitarian law are applicable to this type of attack, considering cyberattacks to be an extension of modern methods and means of warfare that should be subject to the same legal constraints governing armed conflicts.

Conversely, another view argues that the historical period during which the rules governing the means and methods of warfare were codified did not sufficiently contemplate the use of electronic systems or cyber means for military purposes. As a result, cyberattacks are not explicitly regulated, and some scholars even contend that they are not encompassed within customary international law. This has sparked debate as to whether cyberattacks fall outside the scope of the existing international legal framework.[xx]

A third perspective emphasizes the historical context in which international treaties were concluded, beginning with the Hague Conventions of 1899 and 1907, followed by the four Geneva Conventions of 1949, and culminating in the Additional Protocols of 1977. According to this view, these legal instruments were drafted at a time when cyberattacks were neither known nor conceivable in their current form. Consequently, proponents of this approach advocate for a reassessment and development of international humanitarian law in order to accommodate the concept of cyberattacks and regulate them within an explicit and comprehensive international legal framework.

It is evident from reading the preamble of United Nations General Assembly Resolution 46/55 of 2000, entitled “Combating the Misuse of Information Technologies,” that the effects of cyberattacks may be exceptionally broad and far-reaching. Such attacks can extend to various aspects of life, thereby creating potential implications for international security, peace, and stability. Nevertheless, the treatment of this phenomenon at the international level remains limited in scope and has not yet evolved into a comprehensive international convention that regulates it precisely or imposes clear restrictions on its use.[xxi]

In other words, despite the recognition of the seriousness of cyberattacks, their legal consequences have not yet been explicitly defined within the framework of a specialized international treaty. This may be attributed, at least in part, to the reluctance of states to relinquish exclusive control over this vital domain. States appear unwilling to transfer this subject matter to binding international regulatory frameworks that could restrict their freedom of action, particularly given that cyberspace has become a fundamental element in enhancing national security and strategic influence.

In this context, the delay of the international community in reaching a comprehensive convention regulating cyberattacks recalls a similar trajectory in the field of nuclear

weapons. That field likewise witnessed significant difficulties in establishing explicit international regulations aimed at prohibition or restriction due to the resistance of nuclear-armed states. This ultimately led to the adoption of alternative regulatory instruments, most notably the Treaty on the Non-Proliferation of Nuclear Weapons (1968) and the Comprehensive Nuclear-Test-Ban Treaty (1996), reflecting a logic of gradual compromise rather than immediate comprehensive regulation in matters characterized by high strategic sensitivity.[xxii]

Based on the foregoing, it appears that the obstacle to classifying cyberattacks as one of the means or methods of warfare stems from the interests of certain states that are leaders in the development and use of such capabilities. In addition, electronic systems possess the ability to translate hostile commands (malicious software programs) into tangible physical effects. In other words, these effects are capable of movement and of causing damage to pre-selected targets within the state that is the victim of a cyberattack. This is commonly referred to as the kinetic effect.

Two principal branches of international law have traditionally been examined when addressing the legal characterization of the use of means and methods of warfare. The first is the concept of Jus ad Bellum, which regulates the circumstances under which a state may resort to armed force. The second is Jus in Bello, which governs how parties engaged in an armed conflict must conduct themselves. The sources of both branches are reflected in Article 38 of the Statute of the International Court of Justice and are found primarily in treaties (written agreements between states) and customary international law (rules derived from "general practice accepted as law" that exist independently of treaty law).

The principal treaty source governing the resort to force is the United Nations Charter, which expressly prohibits all signatory states from using force under Article 2(4), except in two situations: first, when authorized by the Security Council pursuant to a resolution adopted under Chapter VII of the Charter; and second, when a state exercises its inherent right of self-defense in response to an armed attack under Article 51. However, three fundamental realities give rise to complexities and ambiguities regarding the interpretation of the United Nations Charter in the context of cyberattacks.[xxiii]

First, the United Nations Charter was drafted in 1945, long before the very concept of cyberattacks had been conceived. The foundational experience informing the drafting process was that of traditional kinetic conflicts between states. Consequently, the drafters of the Charter could not have anticipated how its provisions might apply to cyber conflicts.

Second, the Charter itself does not provide definitions for several important terms, such as "use of force," "threat of force," and "armed attack." As a result, the meanings of these expressions cannot be understood solely by reference to the Charter's text. Their definitions and interpretations must instead be derived from historical precedents and state practice, including the ways in which individual states, the United Nations, and international judicial bodies have interpreted these terms in specific situations. Given the existing lack of clarity concerning the meaning of these expressions even in the

context of traditional kinetic conflicts, it is unsurprising that their meaning remains even less clear in the context of cyber warfare. It is hoped that future judicial precedents will clarify the content of these concepts, just as they have done in relation to conventional armed conflicts. However, at this stage, it remains entirely uncertain how, or even whether, courts will adjudicate cases involving cyberattacks.[xxiv]

Third, the Charter contains a degree of internal tension. Article 2(4) prohibits the use of force that may harm persons or property, except in cases of self-defense or when authorized by the United Nations Security Council. However, Article 41 permits other measures—specifically economic sanctions—that may also adversely affect persons or property.

The use of operations that were not envisioned by the drafters of the United Nations Charter—namely cyber operations—may give rise to such a conflict. The other exception is embodied in Article 51 of the United Nations Charter, which states that: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations…". According to the content of this article, a state has the right to resort to the use of force in self-defense in response to any armed attack.

It follows that the scope of the right of self-defense is not limited to traditional attacks carried out through known military means and methods. Rather, it may also extend to attacks conducted through information technology and cyber means of a military nature, provided that such attacks reach the threshold of an "armed attack" under international law standards.[xxv]

The law of war is largely based on the provisions of the Geneva Conventions and their customary law counterparts. Among the principal principles of the law of war are:

The Principle of Military Necessity: Military operations must be intended to assist in defeating the enemy militarily and must serve a concrete military purpose.

The Principle of Distinction: Military operations must be directed only against military objectives and not against civilian targets.

The Principle of Proportionality: Incidental losses involving civilian deaths, injuries, or damage to civilian objects must not be excessive. The exercise of this right requires that the measures taken be proportionate to the nature and degree of the threat or attack and maintain a balance with the anticipated military advantage of the response.

Like the United Nations Charter, the Geneva Conventions remain silent regarding cyberattacks as a method of warfare. The question of how the aforementioned principles apply in situations involving cyber conflict raises several challenges. The following hypothetical cases are intended to highlight some important issues:[xxvi]

Under the Geneva Conventions and their Additional Protocols, with respect to the principle of distinction, parties to a conflict must distinguish between civilians and combatants, and between civilian objects and military objectives. In the context of cyber warfare, an attack on an adversary's information technology system or network must be intended to achieve a specific military advantage (rather than merely a political or economic one). Military forces may transmit a significant portion of their communications through networks primarily used for civilian purposes. Similarly,

military bases often rely on the host country's electrical grid. Does this mean that communication and electricity networks become legitimate military targets?
Provisions relating to precautions against the effects of attacks require the party targeted by an attack to protect civilians and civilian objects under its control from the effects of cyberattacks.
Under the provisions relating to proportionality, a certain degree of collateral damage is permissible, provided that the expected collateral damage is not excessive in relation to the anticipated military advantage.
The provisions concerning the prohibition of perfidy stipulate that military forces may not pretend to be protected entities under the law, such as hospitals. This rule is intended to preserve the distinction between civilian and military entities.
In situations of international armed conflict, a civilian operator enjoys immunity from attack unless he or she "takes a direct part in hostilities," in which case that individual becomes a legitimate military target. Given that civilians are likely to play a major role in carrying out certain types of cyberattacks, this issue becomes particularly significant.
Fourth: International Responsibility Arising from Cyberattacks
In recent years, specialized legal studies have increasingly examined the possibility of attributing international responsibility to a state or to non-state actors accused of carrying out cyberattacks against a state or against other non-state actors.[xxvii]

1. At the International Level:

With the growth of commercial and financial activities over the global information network, the world has witnessed a significant increase in data flows and a substantial expansion in the volume of commercial transactions and financial transfers conducted via the Internet. This development has contributed to the broadening of legislation and regulatory frameworks in countries that recognize the importance of the Internet economy, encompassing various areas such as consumer protection, personal data protection, the security of financial transfers, the determination of jurisdiction, as well as the protection of intellectual property rights and privacy, in addition to other issues related to liability for services and their quality.[xxviii]
In this context, issues of Internet governance have also become increasingly prominent, alongside efforts aimed at combating cybercrime and mitigating its negative impact on the development of electronic transactions and the use of information and communication technologies (ICTs). Furthermore, issues related to the use of electronic money and mobile money, secure payment mechanisms, and methods for storing and using digital funds as virtual payment cards or gift cards are expected to gain increasing importance.
In addition, labor disputes arising from remote work arrangements are growing, accompanied by the expanding use of information and communication technologies, including social networks and internal workplace networks. This development raises new legal concerns regarding the protection of employees' privacy and the safeguarding of their rights.
In a related context, international organizations, particularly the International Telecommunication Union (ITU), continue to emphasize the necessity and importance

of strengthening cybersecurity. Cybersecurity occupies a central position within the ITU's various programs and action plans. Similarly, the United Nations has treated information and communication technologies, especially the Internet, as instruments for social and economic development and effective means of achieving development goals. Consequently, Internet-related issues have become part of the concerns of the Economic and Social Council (ECOSOC) within the framework of addressing development-related matters. Meanwhile, the Commission on Crime Prevention and Criminal Justice is responsible for monitoring international efforts aimed at combating cybercrime and transnational crimes.[xxix]

Within the same framework, cooperation has emerged between the United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU) to support Member States in addressing the growing threats posed by cybercrime and reducing its associated risks. This cooperation is based on a Memorandum of Understanding signed between the two organizations on the sidelines of the World Summit on the Information Society Forum, reflecting the international community's commitment to strengthening institutional coordination in the field of cybersecurity and developing joint mechanisms to combat crimes related to information and communication technologies.[xxx]

The Council of Europe adopted the Convention on Cybercrime, which entered into force in 2004, while encouraging states to accede to it following its adoption in 2001. The provisions of this Convention are largely consistent with the requirements for combating cybercrime, as they oblige States Parties to establish national contact points operating on a continuous-service basis, ensuring round-the-clock readiness to respond to requests originating from outside their borders and enhancing rapid response and international cooperation in the fight against cybercrime.

In this regard, when a state is the source of the criminal act under investigation, it is required to preserve traffic data related to communications and make such data available to the requesting state when the effects of the crime occur within its territory, in accordance with the rules governing international judicial cooperation. In practical terms, this necessitates the enactment of specialized national legislation to facilitate procedures for investigation, inquiry, prosecution, and the seizure of communications data. It also requires the introduction of the necessary amendments to criminal laws to ensure their compatibility with extradition requirements, information exchange mechanisms, and the enhancement of the effectiveness of international cooperation in combating cybercrime.[xxxi]

ICANN also plays a pivotal role in enhancing cybersecurity through its management of the Domain Name System (DNS) and the associated technical and regulatory mechanisms, as well as through the development of programs and initiatives that contribute to supporting the stability of Internet infrastructure.[xxxii]

In a parallel context, most developed countries have adopted advanced preventive and defensive policies to counter cyberattacks. Major countries such as the United States, Australia, and the United Kingdom have allocated substantial financial investments to strengthen their cybersecurity systems and ensure the stability of the digital

environment. This trend reflects the importance these countries place on establishing trust, security, and stability in this vital field, given the close interconnection between the global economy, daily life, essential services, and cyberspace. It also reflects the continuous threats facing cyberspace, which affect security, defense, and international relations as a result of intrusions and attacks targeting networks, information systems, and databases.[xxxiii]

Within this framework, the United States administration was quick to establish a specialized military command dedicated to cyberspace security. This command undertakes multiple responsibilities, including protection, conducting cyber exercises to assess the effectiveness of defenses, measuring response capabilities to attacks, identifying vulnerabilities, and training forces on response mechanisms. These efforts are carried out under a strategy developed by the U.S. Department of Defense in 2011 to organize operations in cyberspace. Similarly, former British Prime Minister Gordon Brown announced the establishment of a specialized unit to combat cybercrime, reflecting the growing international focus on securing the digital environment and addressing its escalating risks.

With the emergence of cloud computing, major corporations and governments alike are preparing to bring about a fundamental transformation in the ways data are stored, processed, and exchanged within cyberspace. This shift is driven by increasing reliance on models that host information in digital environments beyond the users' direct control. The transition is associated with several considerations, most notably operational costs, service quality, and the protection and security of information.

In this context, some stakeholders have begun allocating financial and regulatory provisions within their budgets for cloud computing services, while also developing internal policies and strategies aimed at establishing appropriate legal and administrative frameworks. These measures are intended to regulate contracts related to such services and to establish effective governance structures. Moreover, leaders in industrial and commercial sectors have called on the European Commission to develop a comprehensive legislative framework governing cloud computing services.[xxxiv]

As traditional services such as email, text messaging, and business management systems migrate to cloud computing environments, this transformation is expected to expand further to include the management of electronic wallets, financial and banking services, and numerous governmental activities, including transportation, the energy sector, and others. This development makes it necessary to reconsider the definition of legal rights and obligations in a manner that ensures the smooth flow of information while simultaneously limiting unfair practices that service providers may adopt to generate illegitimate profits.[xxxv]

There is also a growing need to adopt a new approach to information protection based on the level of data sensitivity and in accordance with relevant international standards and benchmarks. In this regard, experts emphasize the importance of establishing clear policies for regulating access to information and protecting data, particularly in light of the continuing lack of harmonization among different national legislations. This situation creates legal challenges related to data transfers, contract regulation, service-

level requirements, and maintenance obligations, thereby necessitating the development of modern legal frameworks that take all of these elements into account collectively.[xxxvi]

1. At the Arab Level:

With regard to cybercrime and information technology crimes, many Arab countries have, until today, refrained from enacting specific legislation addressing cyber and information crimes. Tunisia was the first Arab country to amend its Penal Code in 1999 to encompass information technology crimes. Subsequently, several Arab countries enacted specific or related laws, including:

The Information Crimes Act issued in Sudan in 2007.

The UAE Federal Law No. 2 of 2006, issued in Dubai, which preceded the Sudanese law.

The Anti-Cybercrime Law issued by the Saudi Council of Ministers on March 7, 2007.

The Temporary Information Systems Crimes Law issued in Jordan in 2010.

The Omani Royal Decree that amended the Penal Code to include computer-related crimes.

Circular No. 4 of 2006 in Lebanon concerning the protection of software programs and the fight against software piracy.[xxxvii]

2. At the National Level:

Algeria is among the countries that have sought, in recent years, to address the legislative gap in combating cybercrime through amendments to its existing legal framework. In this context, Law No. 15-04 of November 10, 2004, amending the Penal Code, was enacted. The legislator dedicated Section Seven Bis to criminalizing acts affecting automated data processing systems.[xxxviii]

Article 394 Bis 1 provides for the punishment of any person who fraudulently introduces data into an automated data processing system, or unlawfully deletes or modifies such data. Article 394 Bis 2 penalizes any person who intentionally and fraudulently designs, researches, collects, provides, publishes, or trades in data stored, processed, or exchanged through an information system when such data may be used to commit the offenses stipulated in this section. The penalties also extend to the possession, disclosure, publication, or use of data obtained through any of the cybercrimes provided for by law.

Article 394 Bis 3 establishes aggravated penalties when the offenses target national defense or public institutions and bodies governed by public law, given the seriousness of attacks against these legally protected interests.[xxxix]

As part of strengthening the legal framework for combating cybercrime, Law No. 09-04 of 2009 was subsequently enacted, establishing specific rules for the prevention and suppression of crimes related to information and communication technologies. This law constituted a comprehensive legal framework for preventing and combating this type of crime.

At the institutional level, Algeria has established several specialized bodies and agencies to combat cybercrime, most notably:

The National Authority for the Prevention and Fight Against Crimes Related to Information and Communication Technologies.
The Center for the Prevention of Computer and Cyber Crimes under the National Gendarmerie.
The National Service for Combating Cybercrime under the General Directorate of National Security.[xl]

Conclusion

In conclusion, this study has shown that cyberattacks have become one of the greatest challenges facing states and societies in light of rapid digital transformations. Examining the concepts of cybersecurity and cyberattacks reveals that cyberspace is no longer merely an environment for information exchange; rather, it has become a strategic domain where security, economic, political, and military dimensions intersect, leading to the emergence of new forms of threats that transcend traditional boundaries.

Furthermore, the analysis of cyberattacks demonstrates that such attacks are no longer limited to individuals or private companies. Instead, they have become tools used by governments and non-governmental organizations to target critical infrastructure, gather intelligence, conduct espionage activities, and influence domestic stability as well as international relations. This situation gives rise to complex legal issues concerning the attribution of responsibility for these attacks, the identification of the perpetrating actor, and the extent to which international legal rules apply to actions conducted in cyberspace.

On the other hand, the study indicates that international responsibility for cyberattacks depends on the ability of the international community to develop clear and effective legal rules capable of addressing these threats while maintaining a balance between state sovereignty and the protection of global cybersecurity. Moreover, the transnational nature of these attacks necessitates enhanced international cooperation, the exchange of expertise and information, and the unification of efforts to establish a robust legal and technical framework capable of preventing cyber risks and mitigating their consequences.

Addressing cyberattacks cannot be achieved solely through the development of technical and security measures; it also requires the modernization of national and international legislation, as well as the consolidation of principles of responsibility and accountability in cyberspace. Such efforts must be aligned with contemporary challenges and aimed at protecting the vital interests of both states and individuals. Therefore, building a secure and stable cyberspace remains a collective responsibility

that requires coordinated national and international efforts to confront the growing risks posed by the digital revolution of the twenty-first century.

References

[i]Al-Rubay'ah, Saleh bin Ali bin Abdulrahman. Digital Security and User Protection from Internet Risks, Vision 2030, Communications and Information Technology Commission, Kingdom of Saudi Arabia.
[ii] Al-Mawsili, Nour Amir. Cyberattacks in Light of International Humanitarian Law. Master's Qualification Thesis, Specialization in International Humanitarian Law, Syrian Virtual University, 2021, p. 8.
[iii] Qadir, Ismail. Managing Psychological Warfare in Cyberspace: The New American Strategy in the Middle East. International Conference on the Globalization of Political Media and the Challenges of National Security in Developing Countries, Kasdi Merbah University, 11 April 2017.
[iv] Badran, Abbas. Cyber Wars: Engagement in a Changing World. E-Government Studies Center, Beirut, 2010, p. 4. Available at: http://najishukri.wordpress.com/cyberwarbook

[v] Belferd, Lotfi Lamine. Cyberspace: Architecture and Actors. Algerian Journal of Political Studies, ENSSP, Issue 5, Algeria, 2016, pp. 148–150.
[vi] Ghejati, Souhila, and Amira Rahem. Cyberattacks and Their Impact on Threatening International Peace and Security. Master's Dissertation in Public Law, Department of Law, Faculty of Law and Political Science, University of 08 May 1945 Guelma, 2023–2024, p. 17.

[vii] Aboud, Salem Mohammed. Fundamentals of Cybersecurity. Dar Al-Doctor for Legal and Economic Sciences, Baghdad, 2022, p. 64.

[viii] Lotfi, Wafaa. International Efforts in Combating Cyberterrorism Crimes: The Malaysian Experience as a Model.

[ix]Ibrahim, Khaled Mamdouh. Cybercrime Security. University Press, Alexandria, 2008, p. 56.

[x] Lotfi, Wafaa. Ibid., p. 8.

[xi]Qadir, Ismail. Ibid.

[xii] Boughazi, Abdelkader. Cyber Deterrence: An Approach to Nature, Actors, and the Constraints of International Law. Algerian Journal of Law and Political Sciences, Vol. 10, No. 1, 2025.

[xiii] Belferd, Lotfi Lamine, and Amahand Berkouk. Cyberspace: Actors and Threats. Afak Journal for Sciences, Vol. 9, No. 3, 2024, p. 624.

[xiv] Ibid., p. 625.

[xv]Website: https://me.kaspersky.com/resource-center/definitions/hacker-hat-types, accessed on 25 April 2026 at 18:12.

[xvi] Paul Cornish et al., Cyberspace and the National Security of the United Kingdom: A Chatham House Report, March 2009, p. 15.

[xvii] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, p. 873.

[xviii] Ahmed Oubais Al-Fatlawi, Cyber Attacks: Its Concepts and Arising International Responsibility in the Light of Contemporary International Organization.

[xix] Ibid.

[xx] Ibid.

[xxi] Matthew Evangelista, "Cooperation Theory and Disarmament Negotiations in the 1950s," World Politics Journal, Vol. 42, No. 4, July 1990, p. 515.

[xxii]Ahmed Oubais Al-Fatlawi, Op. Cit., p. 35.

[xxiii] Website: https://www.icrc.org/ar/war-and-law/treaties-customary-law/customary-law. Article by Jean-Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law, Volume I: Rules, International Committee of the Red Cross, Cambridge University Press, Cambridge, 2005.

[xxiv] Isabelle Robinson and Aileen Nolan, Cyber Conflict and International Humanitarian Law, selected from the International Review of the Red Cross, Vol. 94, 2012, p. 524.

[xxv] Website: "Report: 13% Increase in Online Sales in 2011" http://www.al7ll.com/vb/thread22429.html

[xxvi]E-Commerce Growing Like Hell – http://www.brainsins.com/us/blog/ecommerce-growing/1459

[xxvii] J.P. Morgan: Global E-Commerce Revenue to Grow by 19 Percent in 2011http://techcrunch.com/2011/01/03/j-p-morgan-global-e-commerce-revenue-to-grow-by-19-percent-in-2011-to-680b/E-money or M-money.

[xxviii] International Telecommunication Union (ITU), Cybersecurity Guide for Developing Countries, 2007, Executive Summary.

[xxix] Resolution 60/252, 27 April 2006, adopted by the United Nations General Assembly – World Summit on the Information Society: "Reaffirming the potential of information and communication technologies as powerful tools to foster socio-economic development and contribute to the realization of the internationally agreed development goals, including the Millennium Development Goals."

[xxx] Economic and Social Council Resolution 1992/22: Implementation of General Assembly Resolution 46/152 Concerning Operational Activities and Coordination in the Field of Crime Prevention and Criminal Justice, E/1992/92, 30 July 1992.

[xxxi]UN and ITU Team Up to Fight Cybercrime, by Messaging News Staff. On 19 May 2011, the ITU, the United Nations agency for information and communication technologies, established new global partnerships aimed at making cyberspace a safer and more secure environment for consumers, businesses, and, most importantly, children and young people.

[xxxii] A Memorandum of Understanding (MoU), signed between the ITU and the United Nations Office on Drugs and Crime (UNODC) at the WSIS Forum in Geneva, provides for cooperation between the two organizations in assisting ITU and UN Member States in mitigating the risks posed by cybercrime. http://www.messagingnews.com/short-takes/un-and-itu-team-fight-cybercrime

[xxxiii] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG
[xxxiv]PricewaterhouseCoopers, Cyber Security M&A: Decoding Deals in the Global Cyber Security Industry, November 2011.

[xxxv] The United States Establishes a Military Command for Cyberspace. According to a Pentagon spokesperson: "Cybersecurity risks are among the most serious economic and national security challenges of the 21st century."

[xxxvi]http://www.elwatan.com/Les-USA-se-dotent-d-un
[xxxvii]www.defense.gov/news/d20110714cyber
[xxxviii]British Cyberspace Now Protected by Former Hackers. http://techno.branchez-vous.com/actualite/2009/06/le_cyberspace_anglais_desormais

[xxxix] European Commission: Industry Calls for a True Digital Single Market in Recommendations on the European Cloud Strategy.

[xl] Hanan Kharbash, "The Role of Social Media Networks in Shaping Awareness of the Terrorism Phenomenon," Political Trends Journal, Arab Democratic Center, Berlin, Germany, Issue 3, p. 143.