

Dirassat & Abhath
The Arabic Journal of Human
and Social Sciences



مجلة دراسات وأبحاث
المجلة العربية في العلوم الإنسانية
والاجتماعية

EISSN: 2253-0363
ISSN : 1112-9751

Cyber Threats and Their Implications for International Security: A Study of the Concept and Countermeasures

التحديات السيبرانية وانعكاساتها على الأمن الدولي: دراسة في المفهوم وآليات المواجهة

Dr. Lakehal Soumia

Lecturer Class B ,Faculty of Law and Political Science Ziane Achour University of Djelfa,
soumia.lakehal@univ-djelfa.dz.

د. لكحل سمية

أستاذ محاضر "ب"، جامعة زيان عاشور الجلفة ، كلية الحقوق والعلوم السياسية قسم القانون العام،
soumia.lakehal@univ-djelfa.dz

Abstract:

This study addresses cyber threats as one of the most prominent challenges posed by the digital revolution and the rapid development of information and communication technology, given their direct impact on international security and peace, as the growing reliance on cyberspace has led to the emergence of various risks, including cyberattacks, cyber espionage, targeting of critical infrastructure, and theft of sensitive data and information. The importance of this topic lies in the increasing severity of these threats and their expanding cross-border scope, as well as the complex legal and security issues they raise. The study aims to examine the implications of cyber threats on international peace and security, analyze the most significant challenges hindering efforts to address them, and review the most important international and regional mechanisms adopted to counter them. The study concluded that cyber threats have become a real danger to the stability of states, and that efforts to combat them remain limited due to the absence of a comprehensive international legal framework and the difficulty of attributing responsibility for cyberattacks, which calls for strengthening international cooperation and developing legal and institutional frameworks for cybersecurity.

Keywords: Cyber threats, Cybersecurity, International peace and Security, Implications and challenges, International cooperation.

المخلص:

تناول هذه الدراسة التهديدات السيبرانية بوصفها من أبرز التحديات التي فرضتها الثورة الرقمية والتطور المتسارع في تكنولوجيا المعلومات والاتصال لما لها من آثار مباشرة على الأمن والسلم الدوليين، حيث أدى الاعتماد المتزايد على الفضاء السيبراني إلى بروز مخاطر متنوعة تمثلت في الهجمات الإلكترونية والتجسس السيبراني واستهداف البنى التحتية الحيوية وسرقة البيانات والمعلومات الحساسة، وتكمن أهمية الموضوع في تنامي خطورة هذه التهديدات واتساع نطاقها العابر للحدود، إلى جانب ما تثيره من إشكالات قانونية وأمنية معقدة، وتهدف الدراسة إلى دراسة انعكاسات التهديدات السيبرانية على الأمن والسلم الدوليين، وتحليل أبرز التحديات التي تعيق مواجهتها، واستعراض أهم الآليات الدولية والإقليمية المعتمدة للتصدي لها، وقد خلصت الدراسة إلى أن التهديدات السيبرانية أصبحت تمثل خطراً حقيقياً على استقرار الدول، وأن فعالية مكافحتها ما تزال محدودة بسبب غياب إطار قانوني دولي شامل وصعوبة إسناد المسؤولية عن الهجمات الإلكترونية، مما يستدعي تعزيز التعاون الدولي وتطوير الأطر القانونية والمؤسسية الخاصة بالأمن السيبراني. الكلمات المفتاحية: التهديدات السيبرانية، الأمن السيبراني، الأمن والسلم الدوليين، انعكاسات وتحديات، التعاون الدولي.

1. INTRODUCTION

The digital revolution and the rapid development of information and communication technology have brought about fundamental shifts in the nature of the threats facing states and societies. Security risks are no longer confined to traditional land, sea, and air domains, but have extended to cyberspace, which has become a new arena for conflict and competition

among various international and non-state actors, the growing reliance on digital systems and information infrastructure has led to the emergence of escalating cyber threats targeting individuals, institutions, and states alike, making cybersecurity one of the fundamental pillars of national and international security.

The severity of these threats is compounded by their cross-border nature, the difficulty in

identifying perpetrators and holding them legally accountable, as well as the economic, political, and security damage they cause, which may undermine the stability of states and the integrity of their critical infrastructure, in the face of these challenges, there has been a growing need to develop legal and institutional frameworks and to strengthen international cooperation in order to build an effective system to counter cyber threats and mitigate their effects.

Accordingly, this study aims to elucidate the implications of cyber threats on international security and peace, identify the most significant challenges hindering their mitigation, and highlight the key international and regional mechanisms adopted to address them.

To achieve these objectives, the following research question was posed: How can the international community address cyber threats and mitigate their impact on international peace and security in the absence of a comprehensive and binding international legal framework?

To address the subject of this study, the appropriate methodology for this type of research was adopted, namely the descriptive-analytical approach, this involves presenting concepts related to cyberspace, cybersecurity, and cyber threats, and outlining their characteristics and implications for international peace and security, followed by an analysis of the various legal and institutional mechanisms adopted to address them and an assessment of their effectiveness in mitigating their risks.

To address the research problem, the study was divided into two main sections:

- 1- The Concept of Cybersecurity and Cyber Threats
- 2- The Implications of Cyber Threats on International Security and Peace, and the Challenges and Mechanisms for Addressing Them

2. The Concept of Cybersecurity and Cyber Threats

In the modern era, cyberspace has

become one of the most critical domains upon which states and institutions rely to conduct their various activities, driven by the rapid development of information and communication technology. However, alongside this growing reliance, a range of risks and threats targeting information systems and networks in various forms has emerged. These threats have evolved to become more complex and dangerous due to their dynamic nature and ease of cross-border execution. Therefore, cybersecurity has become an absolute necessity to protect data and information and ensure their security and continuity in the digital environment. Accordingly, in this section, we will address the concept of cybersecurity, followed by the concept of cyber threats .

2.1. The Concept of Cybersecurity

Before addressing the definition of cybersecurity, we must first define cyberspace, which refers to the virtual digital domain within which various forms of electronic interaction and exchange take place through an interconnected and complex technical infrastructure that enables the digital simulation of many real-world activities and processes, this space is based on a vast network of servers and electronic systems interconnected via modern communication media, allowing for the transcendence of spatial constraints and political borders, while also contributing to enhancing communication efficiency and developing electronic transactions in their various forms⁽¹⁾ , the U.S. Department of Defense has defined cyberspace as a domain that relies on the use of electronic means and the electromagnetic spectrum to store, modify, and transmit data across communication networks and their associated infrastructure. Cyberspace has become one of the most critical domains upon which modern militaries rely, and has therefore been described as the fourth branch of the military alongside the Army, Navy, and Air Force. It is also considered a new dimension of modern warfare due to its growing influence in conflict management. Cyber power relies on a set of integrated

elements, including technological advancement, economic and industrial capabilities, as well as human resources, military strength, and the will of the state. which means that coordination among these elements helps enhance a state's ability to influence other states and achieve its national objectives, whether through the use of pressure or through political influence and persuasion. Based on this concept, cyberspace has become a domain in which various actors-whether civilian, military, or terrorist-carry out their various activities and operations⁽²⁾.

As for the concept of cybersecurity, there is no single, universally accepted definition; however, it can be defined as providing protection for the various interconnected components of cyberspace through networks, by securing the information technology infrastructure—which includes the Internet, communication networks, computer systems, and network-connected devices, as well as the associated software, applications, and control devices, with the aim of ensuring data integrity and the secure continuity of electronic systems⁽³⁾.

Cybersecurity is also defined as the set of tools, policies, and procedures aimed at protecting information and electronic systems from various digital risks and threats, this includes the implementation of security measures and guidelines, as well as reliance on training and modern technical practices, thereby ensuring the safe use of technology, the protection of the digital environment, and the regulation of access to data and digital resources⁽⁴⁾.

In its report on telecommunications reform trends for the period 2010–2011, the International Telecommunication Union defined cybersecurity as a set of measures and mechanisms that include security policies and procedures, risk management, training, best practices, and modern technologies, aimed at protecting the cyber environment and ensuring the security of information systems and the data of organizations and users⁽⁵⁾.

Cybersecurity also refers to the set of

measures and procedures taken by security agencies and relevant authorities to protect information and electronic systems from various digital threats and breaches , this type of security aims to ensure the confidentiality and integrity of data, guaranteeing its timely access by authorized parties while preventing any unauthorized access, The scope of cybersecurity also extends to protecting the physical aspects related to devices, networks, and software, in addition to protecting data and information from cyberattacks and intentional damage that may target them⁽⁶⁾.

From the above, it can be said that cybersecurity represents an integrated system comprising a set of tools, procedures, and mechanisms aimed at protecting software, computer systems, and cyberspace in general from various attacks, breaches, and digital threats, which may compromise the security and stability of nations⁽⁷⁾.

The cybersecurity system is based on achieving three main objectives known in the field of information security as the information security triad or the CIA triad, which form the foundation of data and electronic system protection. The first objective is confidentiality, which means ensuring that no unauthorized person can view or access protected information and data, the second objective is integrity, which means preserving the integrity of information and protecting it from any unauthorized modification or alteration that could affect its accuracy or authenticity. The third objective is availability, which aims to ensure that information and systems remain available to authorized users in a timely manner and without interruption, together, these principles contribute to strengthening the security of the digital environment and mitigating various cyber risks and threats⁽⁸⁾.

Consequently, cybersecurity has become a strategic issue receiving increasing attention from major international powers, foremost among them the United States, China, and Russia, due to its importance in protecting the vital interests of states and strengthening their national security. Many countries have

also moved to establish units and departments specializing in cyber warfare within their national security frameworks, in addition to traditional security mechanisms aimed at combating cybercrime, digital fraud, and other threats associated with cyberspace. This is due to the significant expansion of modern societies' reliance on information and communication technology across various fields, which in turn has led to the emergence of increasing risks and challenges targeting networks and information systems, consequently, cyberattacks, hacking, and digital espionage have become among the most prominent threats to national security in the contemporary international environment⁽⁹⁾.

2.2. The Concept of Cyber Threats (Cybercrime)

The concept of cyber threats has undergone several stages of development, a fact reflected in the variety of terms used to describe it over time, in line with technological advancements and the expansion of technology's applications. Initially, these phenomena were referred to as "computer misuse," The concept soon evolved to become more specific with the use of the term "computer fraud," before the term "cybercrime" emerged, broadening the scope to include various illegal acts related to information. Subsequently, the term "computer crimes" was used, followed by the expression "high-tech crimes," which emphasized the advanced technological aspect of these acts. The term "hacker crimes" also became common to refer to specific types of intrusions, followed by "Internet crimes" with the spread of the World Wide Web, until usage settled at the current stage on the term "cybercrime" as the most comprehensive and accurate description of this type of crime. This term consists of two basic words: "crime," which denotes an unlawful act, and "cyber," which refers to the digital space, reflecting the close link between criminal behavior and the electronic environment⁽¹⁰⁾.

There are numerous legal definitions of cybercrime, depending on the different

perspectives adopted by researchers and legal scholars, yet they all converge on the connection between this type of crime and the use of technology and the digital space. Some view cybercrime as being committed through the use of a computer or other modern technology to attack another computer or similar electronic system, with a communication network enabling the criminal act to be carried out, in another vein cyber threats have been defined as criminal activity in which computer technologies are used directly or indirectly, whether as a tool for committing the crime or as a target of the attack. Some legal scholars have also sought to broaden the scope of the concept, defining cybercrime as any unlawful behavior or conduct contrary to legal and ethical norms that occurs via information networks and targets various interests such as money, data, knowledge, trust, and reputation, making it one of the most prominent crimes of the digital age associated with rapid technological development⁽¹¹⁾.

In comparative law, the concept of cybercrime is associated with unlawful acts arising in the digital environment or linked to technological development. It is defined as a set of behaviors and activities criminalized by law, in which there is a close connection between the criminal act and technological progress and the digital revolution⁽¹²⁾, as for Algerian legislation, the legislature addressed the concept of cybercrime in Article 2 of Law No. 09-04 concerning special rules for the prevention and combating of crimes related to information and communication technologies⁽¹³⁾, expanding its scope to include crimes targeting automated data processing systems as defined in the Penal Code, as well as any crime committed or aided by the use of an information system or an electronic communications system, this legislation was enacted to keep pace with technological changes and the new patterns of criminal activity associated with the digital environment that have emerged as a result.

Cybercrime differs from traditional crimes in terms of its nature and the means by which it is committed, as it is characterized by the absence of direct physical confrontation between the perpetrator and the victim; it can be carried out remotely via digital media without the need for a physical presence at the scene of the crime. It is also difficult to detect and prove due to the ability to conceal or delete digital traces and manipulate electronic evidence, which further complicates investigative and prosecutorial procedures. Another notable characteristic is that it transcends geographical boundaries; it is not limited to a specific region but can affect multiple countries simultaneously. Additionally, it is characterized by rapid execution and relatively low costs compared to traditional crimes.

Cyber threats take various forms depending on their objectives and methods. Among the most prominent is cyber espionage, which involves attempts to hack into systems and websites to obtain confidential information or sensitive data, we also see cyberterrorism through the exploitation of the digital space at to spread extremist ideas, issue threats, or extort individuals and institutions by demanding ransom. Furthermore, these threats include targeting a country's critical infrastructure—whether civilian or military—which can lead to system disruptions and a weakening of operational efficiency, as well as the theft of government or military information and the manipulation of electronic data through forgery, destruction, or unlawful reuse⁽¹⁴⁾.

As for cybercriminals, they vary depending on their motives, goals, and level of technical expertise; Some engage in such acts out of curiosity or for fun and are often classified as amateurs, while there is a category of hackers who seek to test their technical capabilities and demonstrate their skills in breaching information systems and networks. In contrast, another group deliberately seeks to cause harm, whether through data theft, tampering with information, or disrupting electronic

systems; they are usually referred to as "crackers." Cybercrimes also include a category of individuals obsessed with digital technologies who aim to bypass security systems and breach electronic safeguards⁽¹⁵⁾. The issue is not limited to individuals; cybercrime extends to organized crime networks that employ digital means to achieve financial gain or expand influence and control, as well as extremist groups that exploit cyberspace to spread their ideas or serve political, religious, or ideological objectives⁽¹⁶⁾, furthermore some governments have begun to rely on cyber means for espionage and the collection of political, military, or economic intelligence.⁽¹⁷⁾

Consequently, perpetrators of this type of crime are characterized by a high level of technical knowledge and the ability to hack into networks, bypass security systems, and circumvent passwords. This has led some researchers in the legal and criminal fields to describe them as "white-collar criminals" due to the technical and skill-based nature of their criminal activities.

3. The Implications of Cyber Threats on International Security and Peace, and the Challenges and Mechanisms for Addressing Them

Since cyberspace has today become an open arena where international interests intersect and threats intertwine, and since it has become a significant factor in the balance of international security and peace, this has led to the emergence of multiple repercussions of cyber threats affecting various political, economic, and security aspects of states. Furthermore, the cross-border nature of these threats has complicated efforts to address them at the international level, as the international community has faced significant challenges that hinder the ability to effectively regulate this space, particularly in the absence of a comprehensive and binding legal framework. This situation has prompted many states and organizations to seek various mechanisms and methods to address these growing risks. Accordingly, in this

section, we will examine the implications of cyber threats on international peace and security and the challenges of addressing them, followed by mechanisms for countering these threats.

3.1. The Implications of Cyber Threats on International Security and Peace and the Challenges of Addressing Them

Since cyberspace is no longer merely a technical space for communication and information exchange, but has transformed into a strategic arena where considerations of security, power, and influence among states intersect, this transformation has led to the emergence of escalating cyber threats that have a direct impact on the stability of international security and peace. These implications are manifested in the targeting of critical infrastructure, the disruption of essential systems, and the impact on the economic and political security of states. Furthermore, the cross-border nature of these threats has complicated the issue of assigning responsibility and effectively addressing these risks, as international practice has revealed real challenges that hinder the establishment of a comprehensive response system, particularly in light of technological disparities and existing legislative gaps.

3.1.1 The Impact of Cyber Threats on International Security and Peace

The digital realm has become a pivotal arena of confrontation in today's world, as cyberattacks dominate the landscape of contemporary conflicts due to their high effectiveness and limited costs compared to traditional armed conflicts; indeed, their destructive repercussions may exceed in scale the losses caused by conventional wars. A combination of structural factors fuels these threats and expands their scope, foremost among them the growing intertwining of the international relations system and cyberspace, as well as the erosion of state authority and the decline of its dominance in the context of accelerating globalization. Added to this is the increasing reliance of states on digital infrastructure to manage their critical facilities, resulting in

security vulnerabilities that can be exploited at relatively low cost, making cyber warfare a preferred strategic option for many international actors.

Cyber threats are no longer merely hypothetical risks; they have become a real existential challenge that strikes at the very heart of states' national security, as they continuously target the fundamental pillars of critical infrastructure—such as energy production and distribution systems, water, transportation, and communications networks, all the way to sensitive facilities such as nuclear reactors and chemical complexes. Statistical figures underscore the scale of this phenomenon and its rapid growth, as specialized studies confirm that cyberspace is subjected to over a thousand attacks per minute, while cybercrime is now taking a heavy toll on the global economy with massive and escalating losses, driven by its high effectiveness and low costs compared to traditional armed conflicts, as for individual and collective repercussions, available statistical data reveals that 2014 alone witnessed a large-scale security breach affecting the data of more than 1.3 billion people worldwide, a figure that clearly illustrates the immense scope of these threats and their growing ability to undermine the collective security system and destabilize it⁽¹⁸⁾.

Documented facts also reveal the depth of the impact of cyber threats and their severity; In 2010, the computer virus known as “Stuxnet” resulted in the complete paralysis of approximately 1,000 centrifuges at Iran's Natanz nuclear facility, a prime example of the capability of digital weapons to target strategic infrastructure. In the same vein, in June 2017, Ukraine was subjected to a coordinated cyber operation that simultaneously affected the energy and financial services sectors, while U.S. power grids were also not spared from similar attacks, cyberattacks can be classified into two main categories: The first are intelligence-gathering operations aimed at breaching information systems and stealing data, and the second are destructive attacks

aimed at disrupting or damaging adversary systems, particularly government institutions and critical infrastructure of a strategic nature⁽¹⁹⁾.

Cyber espionage occupies a prominent position within the spectrum of cyber threats, given the extremely serious repercussions it has on international relations and stability, as possessing advanced cyber capabilities is no longer merely a competitive advantage but has become an essential prerequisite for exerting influence in the digital realm and safeguarding national sovereignty in all its dimensions. The massive espionage scandal that followed the intelligence leaks released by American analyst Edward Snowden in 2013 revealed an unprecedented scale of electronic surveillance and monitoring operations carried out by major powers on a broad international scale. These operations even targeted leaders of allied nations in Europe, leading to severe diplomatic tensions and redrawing the boundaries of trust among strategic partners on the international stage⁽²⁰⁾.

3.1.2 International Challenges in Addressing Cyber Threats

Cyber threats today pose a real challenge to the international community, given their complex and rapidly evolving nature. The absence of a unified international legal framework and the technological disparity among states have further compounded the difficulty of addressing them.

3.1.2.1 The Legislative Vacuum and Shortcomings of International Law

The international treaty framework is one of the most significant shortcomings in the system for addressing cyber threats, as it lacks sufficient flexibility to respond rapidly to the ever-changing dynamics of this constantly evolving domain. This is clearly evident in the failure of UN efforts to draft a binding international convention that regulates this phenomenon and establishes governing rules within the UN framework. The existing international legal system suffers from deep structural gaps that prevent it from adequately addressing cyber

threats. The international legal order still lacks any specialized legal instrument that provides a precise definition of cyberspace and regulates international interactions within it, whether between states or between states and non-state actors. This legislative vacuum extends to the development, possession, and deployment of cyberweapons in peacetime, in the absence of any binding legal restrictions governing this field or regulating the power of the major tech companies that produce them, leaving these matters subject to doctrinal interpretations of principles of international humanitarian law such as proportionality and necessity. Further complicating the picture is the lack of clear international standards governing the issue of legitimate defense in cyberspace and its conditions and limits. As for accountability, the problem of attributing international responsibility to attackers remains a formidable obstacle, particularly when targeted states resort to secrecy and non-disclosure, as was the case in the attacks that targeted Iran's telecommunications sector in 2020. Furthermore, obscuring the identity of the attackers hinders the classification of the conflict and the determination of legal responsibilities⁽²¹⁾.

3.1.2.2 The Disparity in Technological Capabilities Among States and Its Impact on National Security

The sharp disparity in technological levels among the world's nations represents one of the most significant obstacles to strengthening the international framework for countering cyber threats. Countries that rely on importing technology from abroad find themselves in a vulnerable position, as their relationship with supplier nations shifts from a mere technical partnership to a form of disguised security dependency, more precisely, advanced technology—which is supposed to be a tool for strengthening national sovereignty and fortifying national security—often turns into a gateway for infiltrating strategic decision-making and deepening dependence on foreign powers, thereby stripping the concept of security

independence of its actual substance.

From this perspective, there is an urgent need to re-examine defense policies to ensure that the security system is freed from the constraints of dependence on foreign suppliers, this can be achieved by making sustainable investments in the national scientific research and technological development sector, thereby enabling the building of genuine indigenous capabilities in the field of cybersecurity, a state that possesses independent national technology is better equipped to confront advanced digital threats, and has greater freedom to formulate its defense strategies free from any external pressures or dictates, this also requires moving beyond traditional approaches to protecting information and electronic networks and transitioning toward more innovative defense models capable of adapting to the rapidly changing nature of contemporary cyber threats⁽²²⁾.

3.2. Mechanisms for Addressing Cyber Threats

In light of the escalating cyber threats and their growing impact on international security, states and international and regional organizations have moved swiftly to establish legal, technical, and institutional mechanisms to address these threats. These mechanisms fall into two main categories: institutional international and regional efforts and international cooperation through agreements concluded in this regard.

3.2.1 International and Regional Institutional Efforts to Address Cyber Threats

International and regional organizations, led by the United Nations, have devoted significant attention to countering cyber threats in light of their growing severity and expanding scope. These efforts have manifested in the establishment of specialized mechanisms and institutions to enhance cooperation and information exchange among states, and a range of initiatives have emerged aimed at developing response capabilities to these threats at the international and regional levels.

3.2.1.1 Efforts by the United Nations

The United Nations has shown increasing interest in combating cybercrime, recognizing it as one of the most significant challenges brought about by the digital revolution and the rapid advancement of information and communication technology. The United Nations has recognized that addressing this type of crime is not limited to relying on technical means or traditional criminal penalties but also requires the development of legal and legislative frameworks commensurate with its specific nature. In this context, the United Nations General Assembly adopted Resolution 65/230, which mandated the formation of a group of experts to prepare a comprehensive study on cybercrime, with the aim of identifying its various dimensions and proposing effective ways to strengthen international cooperation in combating it⁽²³⁾, the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Vienna from April 10 to 17, 2000, also addressed the issue of crimes related to modern technologies and computers, during which a plan of action was adopted that included a set of measures and recommendations aimed at developing prevention and combating mechanisms and strengthening cooperation among states in this field.

It should be noted that the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from April 12 to 19, 2015, highlighted the urgent need for effective measures to combat cybercrime and identified a number of additional steps that states must take to address this crime. The conference emphasized the need to develop specialized tools and programs to facilitate the response to this type of crime and limit its spread, stressing that effectively combating it requires states to develop their capabilities in the areas of preventive security, counter-investigation, and the establishment of digital criminal justice, the conference also attached great importance to building the capacity of law enforcement agencies to investigate cybercrimes, collect

digital forensic evidence, and handle it using approved scientific methods. Regarding multilateral frameworks, the African Regional Preparatory Meeting recommended working toward the drafting of a specialized international convention on cybercrime in the context of the Thirteenth Conference, concerning the issue of cross-border data access, the conference acknowledged the obstacles faced by law enforcement agencies in accessing data stored outside their territorial jurisdiction, while emphasizing that such access must be limited, verifiable, proportionate to its purpose, and subject to adequate oversight, thereby ensuring the protection of human rights, the rule of law, and the sanctity of privacy. The conference also highlighted the importance of involving the private sector as an active partner in the fight against cybercrime, while calling for enhanced cooperation with academia across various disciplines.

To complement the United Nations' efforts in this area, it has issued a comprehensive guide on computer-related crimes, which is subject to periodic review and updating and includes a precise definition of the issue, a comprehensive definition of these crimes, and mechanisms for addressing them⁽²⁴⁾.

3.2.1.2 The International Criminal Police Organization

The International Criminal Police Organization (Interpol) occupies a distinguished position in the global framework for combating cross-border cybercrime in all its forms and manifestations, thanks to the advanced mechanisms it provides for tracking down and apprehending the perpetrators of such crimes, within a framework that respects and does not conflict with the principle of national sovereignty of member states. The organization's roots date back to September 7, 1923, when its foundations were first laid, and it has evolved over the decades to include 195 member states today, making it one of the most widespread and representative international security organizations, its mission centers on

building bridges of communication and exchanging information between national police and judicial authorities and their counterparts around the world, thereby enabling effective security coordination in addressing transnational crimes⁽²⁵⁾.

Recognizing the growing challenges posed by the digital realm, the organization established a specialized unit in 2003 to combat cybercrime, and worked in close coordination with the G8 countries to develop effective strategies to combat this type of crime, which manifested in a series of concrete practical measures, most notably the establishment of an integrated electronic communications center operating at the level of police departments in member states and facilitating the flow of security information in real time, it also ensured that member states were provided with a specialized guide on cybercrime, including the necessary training curricula to qualify personnel involved in combating it, reflecting a firm commitment to building institutional capacity at the international level⁽²⁶⁾.

3.2.1.3 European Union Efforts

At the European regional level, the European Union is among the most advanced and proactive regional blocs in addressing cybercrime. It has not merely acknowledged the gravity of the issue but has moved to establish a comprehensive institutional framework to combat it. In this context, the EU established the European Cybercrime Centre within Europol in 2013, with the aim of strengthening on-the-ground security responses and enhancing the role of law enforcement agencies in combating cybercrime across the European Union, by unifying intelligence and investigative efforts among member states and exchanging digital forensic information in real time. In addition, the establishment of Eurojust in February 2002 and its official launch in April 2003 added an indispensable judicial dimension to this system, as it undertakes the task of judicial coordination among member states and facilitates cooperation in the criminal prosecution of

cross-border crimes, including cybercrimes. These initiatives reveal an early European awareness of the seriousness of digital threats and a firm political will to institutionalize the response and make it more effective and coordinated at the regional level⁽²⁷⁾.

3.2.1.4 African and Arab Regional Efforts

At the African level, the African Union took a significant legislative step by concluding a specialized agreement on cybersecurity and the protection of personal data, on the sidelines of the Malabo Summit held in Equatorial Guinea on June 27, 2014. This agreement is based on a set of integrated strategic objectives, foremost among which is supporting and updating the legislative and regulatory frameworks of member states to align with the requirements of the digital age, as well as establishing strict security standards that contribute to creating a reliable cyberspace suitable as a secure environment for digital transactions, combating cybercrime in all its forms, and safeguarding personal data from any unlawful infringement or exploitation.

At the Arab level, efforts did not stop at merely acknowledging the risks but were translated into concrete institutional initiatives. In 1996, the Council of Arab Ministers of Justice adopted the Unified Arab Penal Code, which included explicit provisions regarding violations of individual rights resulting from information processing operations, in an early recognition of the legal dimensions of cybercrime. In the same vein, the Council of Arab Interior Ministers contributed to strengthening the regional security cooperation framework by establishing the Arab Criminal Police Bureau, which plays a pivotal role in coordinating joint Arab security efforts in the fight against crime, including cybercrimes⁽²⁸⁾.

3.2.2. International Cooperation Through Agreements to Counter Cyber Threats

In light of the escalation of cross-border cyber threats, countries have moved to strengthen cooperation among themselves by concluding agreements to organize joint

efforts to combat cybercrime, mitigate its effects, and standardize response methods, thereby enhancing the effectiveness of the response at the international level.

3.2.2.1. The Budapest Convention on Cybercrime

The Budapest Convention, concluded in 2001, represents a milestone in the history of international cooperation to combat cybercrime, as it is the first binding international instrument dedicated to criminalizing criminal acts committed through or via computer networks. Thirty countries, along with Canada, Japan, South Africa, and the United States of America, have acceded to it. To this day, the Convention retains its status as the primary international reference in this field and remains open for accession by states wishing to join its legal framework.

In terms of content, the Convention comprehensively addresses three core, interrelated areas. Substantively, it establishes a broad criminal framework covering a range of cybercrimes, foremost among which are unauthorized access to information systems, data manipulation and destruction, electronic forgery, and digital fraud, in addition to crimes related to pornographic content. Procedurally, the Convention established detailed mechanisms regarding the preservation and safeguarding of digital data, as well as procedures for search, seizure, and surveillance of communications, thereby enabling law enforcement agencies to effectively investigate these crimes. Finally, regarding international cooperation, the Convention establishes rules governing extradition and mutual legal assistance among States Parties, making it a comprehensive legal instrument that integrates criminalization, prosecution, and cooperation into a single, coherent framework⁽²⁹⁾.

3.2.2.2. The Tallinn Manual (The International Legal Framework for Cyber Operations in Times of Conflict)

The Tallinn Manual, published in 2013, occupies a central position in the international cyber law framework, as it is

the most comprehensive and detailed document interpreting the rules of international law applicable to cyber warfare. This manual was developed in response to a call by the North Atlantic Treaty Organization (NATO), which entrusted its preparation to a select group of international experts with the aim of examining the applicability of international humanitarian law to cyberattacks and establishing the legal framework governing state responsibility for cyber operations launched from government infrastructure or directed by the state⁽³⁰⁾.

In terms of content, the guide comprises ninety-five articles distributed across seven main rules, which are in turn divided into specialized sections, each addressing an aspect of engagement in cyberspace and the resulting rights and duties of the warring parties, the guide addresses a range of sensitive issues and complex legal challenges associated with cyber warfare, such as defining the concept of armed conflict in the digital domain, frameworks for managing cyber military operations, rules of engagement and their regulations, determining the status of combatants in this domain and the legality of targeting them, as well as the challenges of using drones in cyber contexts and other fundamental concepts related to this emerging field⁽³¹⁾.

4. CONCLUSION

In concluding our study of cyber threats and their implications for international security, it has become clear that cyberspace has become a fundamental component of the contemporary international security environment, and the threats and challenges it faces are a source of growing concern for states and international organizations. It has also been concluded that cyber threats are no longer merely isolated technical crimes, but have evolved into tools capable of affecting national security and international stability by targeting critical infrastructure, strategic data, and the economic interests of states. The study also concluded that addressing these threats continues to face a range of legal, technical, and institutional challenges

that limit the effectiveness of international efforts in this field. The study reached a set of findings and recommendations, primarily as follows:

Findings:

- ✓ Cyberspace has become a new strategic domain that directly impacts international security and peace.
- ✓ Cyberattacks pose a growing threat to states' critical infrastructure and their security and economic institutions.
- ✓ Cyber espionage stands out as one of the most serious forms of cyber threats due to its political, security, and diplomatic implications.
- ✓ The international legal system suffers from a clear deficiency in regulating cyberspace due to the absence of a comprehensive and binding international convention in this field.
- ✓ The difficulty in identifying the perpetrators of cyberattacks and attributing international responsibility to them represents one of the most significant challenges in combating these threats.
- ✓ Disparities in technological capabilities among states undermine international efforts to achieve balanced and effective cybersecurity.
- ✓ International and regional organizations, led by the United Nations, Interpol, and the European Union, have contributed to the development of various mechanisms to address cybercrimes and threats.
- ✓ The Budapest Convention and the Tallinn Manual are among the most prominent international initiatives aimed at strengthening the legal framework governing cyberspace.

Recommendations:

- Work toward concluding a comprehensive international agreement under the auspices of the United Nations to regulate cyberspace and define rules of international responsibility for cyberattacks.
- Strengthen international cooperation and the exchange of information and

expertise among states to address cross-border cybercrimes and threats.

- Support national cybersecurity capabilities through investment in scientific research and technological development.
- Develop national legislation in line with technological advancements and modern patterns of cybercrime.
- Strengthening training programs for law enforcement agencies, judges, and specialists in the field of digital evidence.
- Encouraging public-private partnerships in the protection of digital infrastructure and the enhancement of cybersecurity.
- Expand cooperation between security agencies, universities, and research centers to develop innovative solutions to address cyber threats.
- Raise public awareness of cyber risks and foster a culture of digital security among all segments of society.

4. Bibliography List :

1. Books:

- Adel Abdel-Aal Ibrahim Kharashi (2015), Challenges of International Cooperation in Combating Cybercrime and Ways to Overcome Them, Dar al-Jami'ah al-Jadidah for Publishing and Distribution, Alexandria, Egypt.
- Ali Ziad Ali (2020), Conflict and Geosbary Security in the International Arena (A Study of Digital Engagement Strategies), Amjad Publishing and Distribution, Amman, Jordan.
- Kawthar Mazouni (2022), Cybercrime, 1st ed., Dar al-Khaliduniya Publishing, El Koba, Algeria.
- Najat Ben Makki (2017), Criminal Policy to Combat Cybercrime, Dar Al-Khaliduniya for Publishing and Distribution, El Koba, Algeria.
- Youssef Manasra (2018), Crimes Against Automated Data Processing Systems: Their Nature, Forms, and International Efforts to Combat Them—A Comparative Study, Dar Al-Khaliduniya for Publishing and Distribution, Algeria.

2. Journal article :

- Abderrahmane Rafrafi (2025), "Personal Data Protection and Cybersecurity: An Analysis from the Perspective of International Law," Al-Fikr Journal, University of Mohamed Khider, Biskra, Vol. 20, No. 1.
- Amal Bidi (2022), "United Nations Efforts in Combating Cybercrime," Journal of Research in Law and Political Science, Ibn Khaldoun University of Tiaret, Vol. 08, No. 01.
- Fayza Ahmed Al-Husseini Mujahid (2023), "Cybersecurity Awareness: A Luxury or a Necessity in the Information Age," Research and Education Journal, National Institute for Educational Research, Vol. 13, No. 02.
- Hayat Hamidi, Nasima Tayleb (2022), A Conceptual Introduction to Cybersecurity, Madar Journal of Digital Communication Studies, University of Algiers 3, Vol. 02, No. 02.
- Mohamed Ahmed Labib Ahmed, Haitham Mohamed Bahaa Al-Qadi, and Mustafa Ahmed Kamal (2024), "The Role of International and Regional Agreements in the Field of Cybersecurity and the Egyptian State's Position Thereon," Journal of Governance and the Prevention and Combating of Corruption, Egypt, Issue 1, Vol. 1.
- Mohamed Al-Said Bouflih (2024), "Frameworks for International Cooperation to Address Cyber Threats," Journal of Applied Legal Studies, University of the Brothers Mentouri, Constantine, Vol. 01, No. 02.

- Moussa Ben Taghri (2022), "Cyberwarfare and International Humanitarian Law," Journal of Judicial Precedent, Mohamed Khider University of Biskra, Vol. 12, Special Issue.
- Rawan Bint Atiyah Allah Al-Sahafi (2020), "Cybercrimes," Comprehensive Multidisciplinary Electronic Journal, Jeddah, Saudi Arabia, Issue 24.
- Rima Younes, Amal Fiash (2026), "Cybersecurity in the Kingdom of Saudi Arabia: Realities, Challenges, and Vision 2030," Journal of Legal and Economic Research, University Center of Aflo, Vol. 09, No. 02.
- Samir Bara (2017), "Cybersecurity in Algeria: Policies and Institutions," Algerian Journal of Human Security, University of Batna 1, Vol. 02, No. 02.
- Sharifa Kalaa (2022), Cybersecurity and the Challenges of Espionage and Cyberattacks on States via Cyberspace, Journal of Law and Humanities, Ziane Achour

University of Djelfa, Vol. 15, No. 01.

- Wedad Boutlaa, Manal Boukourou (2022), "The Conflict in Cyberspace and Its Impact on International Peace and Security—New Challenges, Threats, and Ways to Address Them," Journal of Legal and Social Sciences, Ziane Achour University of Djelfa, Vol. 07, No. 04.

3. Legal documents:

- Law No. 09-04, dated August 5, 2009, containing specific rules for the prevention and combating of crimes related to information and communication technology, Official Gazette of Algeria, Issue 47, dated August 16, 2009.
- Report of the Joint Inspection Unit on Cybersecurity in United Nations System Organizations, United Nations, Geneva, 2021.

5. Citations:

2030," Journal of Legal and Economic Research, University Center of Aflo, Vol. 09, No. 02, p. 620.

(6)- Sharifa Kalaa, op. cit., p. 298.

(7)- Fayza Ahmed Al-Husseini Mujahid (2023), "Cybersecurity Awareness: A Luxury or a Necessity in the Information Age," Research and Education Journal, National Institute for Educational Research, Vol. 13, No. 02, p. 60.

(8)- Report of the Joint Inspection Unit on Cybersecurity in United Nations System Organizations, United Nations, Geneva, 2021, p. 8.

(9)- Sharifa Kalaa, op. cit, pp. 298–299.

(10)- Mohamed Al-Said Boufli (2024), "Frameworks for International Cooperation to Address Cyber Threats," Journal of Applied Legal Studies, University of the Brothers Mentouri, Constantine, Vol. 01, No. 02, p. 10.

(11)- Rawan Bint Atiyah Allah Al-Sahafi (2020), "Cybercrimes," Comprehensive Multidisciplinary Electronic Journal, Jeddah, Saudi Arabia, Issue 24, pp. 8–9.

(12)- Youssef Manasra (2018), Crimes Against Automated Data Processing Systems: Their Nature, Forms, and International

(1)- Ali Ziad Ali, Conflict and Geosbary Security in the International Arena (A Study of Digital Engagement Strategies), Amjad Publishing and Distribution, Amman, Jordan, 2020, pp. 53–54.

(2)- Sharifa Kalaa (2022), Cybersecurity and the Challenges of Espionage and Cyberattacks on States via Cyberspace, Journal of Law and Humanities, Ziane Achour University of Djelfa, Vol. 15, No. 01, pp. 294–295.

(3)- Hayat Hamidi, Nasima Tayleb (2022), A Conceptual Introduction to Cybersecurity, Madar Journal of Digital Communication Studies, University of Algiers 3, Vol. 02, No. 02, p. 04.

(4)- Samir Bara (2017), "Cybersecurity in Algeria: Policies and Institutions," Algerian Journal of Human Security, University of Batna 1, Vol. 02, No. 02, p. 258.

(5)- Rima Younes, Amal Fiash (2026), "Cybersecurity in the Kingdom of Saudi Arabia: Realities, Challenges, and Vision

Efforts to Combat Them—A Comparative Study, Dar Al-Khaliduniya for Publishing and Distribution, Algeria, p. 269.

(13)- Law No. 09-04, dated August 5, 2009, containing specific rules for the prevention and combating of crimes related to information and communication technology, Official Gazette of Algeria, Issue 47, dated August 16, 2009.

(14)- Wedad Boutlaa, Manal Boukourou (2022), "The Conflict in Cyberspace and Its Impact on International Peace and Security—New Challenges, Threats, and Ways to Address Them," Journal of Legal and Social Sciences, Ziane Achour University of Djelfa, Vol. 07, No. 04, p. 814.

(15)- Mohamed Saïd Bouflih, op. cit, p. 15.

(16)- Kawthar Mazouni (2022), Cybercrime, 1st ed., Dar al-Khaliduniya Publishing, El Koba, Algeria, p. 346.

(17)- Mohamed Saïd Bouflih, op. cit, p. 15.

(18)- Abderrahmane Rafrafi (2025), "Personal Data Protection and Cybersecurity: An Analysis from the Perspective of International Law," Al-Fikr Journal, University of Mohamed Khider, Biskra, Vol. 20, No. 1, p. 369.

(19)- Sharifa Kalaa, op. cit, pp. 300–301.

(20)- Ibid, p. 303.

(21)- Wedad Boutlaa, Boukoro Manal, op. cit, pp. 819–820.

(22)- Sharifa Kalaa, op. cit, p. 309.

(23)- Youssef Manasra, op. cit, p. 279.

(24)- Amal Bidi (2022), "United Nations Efforts in Combating Cybercrime," Journal of Research in Law and Political Science, Ibn Khaldoun University of Tiaret, Vol. 08, No. 01, pp. 309–310.

(25)- Youssef Manasra, op. cit, p. 278.

(26)- Adel Abdel-Aal Ibrahim Kharashi (2015), Challenges of International Cooperation in Combating Cybercrime and Ways to Overcome Them, Dar al-Jami'ah al-Jadidah for Publishing and Distribution, Alexandria, Egypt, p. 25.

(27)- Najat Ben Makki (2017), Criminal Policy to Combat Cybercrime, Dar Al-Khaliduniya for Publishing and Distribution, El Koba, Algeria, p. 146.

(28)- Mohamed Al-Said Bouflih, op. cit, pp. 20–21.

(29)- Mohamed Ahmed Labib Ahmed, Haitham Mohamed Bahaa Al-Qadi, and Mustafa Ahmed Kamal (2024), "The Role of International and Regional Agreements in the Field of Cybersecurity and the Egyptian State's Position Thereon," Journal of Governance and the Prevention and Combating of Corruption, Egypt, Issue 1, Vol. 1, pp. 141–142.

(30)- Moussa Ben Taghri (2022), "Cyberwarfare and International Humanitarian Law," Journal of Judicial Precedent, Mohamed Khider University of Biskra, Vol. 12, Special Issue, pp. 210–211.

(31)- Mohamed Saïd Bouflih, op. cit, pp. 22–23.