CYBER THREATS AND CYBERSECURITY: EMERGING THREATS IN CYBER SPACE AND STRATEGIES TO COUNTER THEM

DR. SAMEUT AMINA[1]

[1]Lecturer class A, Faculty of Law and Political Science, Hassiba Ben Bouali University, Chlef, Laboratory Comparative private law (Algeria).

The E-mail Author: a.sameut@univ-chlef.dz

Received: 19/02/2024 **Published: 08/03/2025**

Abstract:

With the advancement of technological means and information systems, as well as the evolution of new forms of warfare and security threats, information and communication technology has become a focal point for countries across all sectors. Cybersecurity threats now pose a significant danger at both the national and international levels. Their severity is exacerbated by their ability to transcend traditional national boundaries and the global proliferation of networks, shifting from physical reality to digital space.

This study aims to highlight the various threats emanating from cyberspace and their impact on security stability. It seeks to outline the measures taken to address these threats by establishing a legal framework for prevention and response, as well as appropriate sanctions to mitigate the impact of these emerging crimes, which target individuals, data and States, causing them significant losses in various sectors. Such threats represent the stark reality of "electronic colonization" in its most egregious forms.

This research paper examines the effectiveness of legislative policy in mitigating cybersecurity threats, as well as strategies to combat them.

***Keywords**: cybersecurity, cyber threats, cyberspace, emerging crimes, cyber espionage.*

INTRODUCTION:

The world of information and communication technology has imposed numerous threats and challenges across various fields, as it encompasses all aspects of life. It is considered one of the latest scientific applications, and like any application, it has many benefits and drawbacks. Misuse has led to the emergence of new security threats impacting both the state and the individual. Traditional political borders can no longer effectively confront the dangers posed by these cyber threats. This has necessitated a reevaluation of the fundamental assumptions regarding security threats globally and the mechanisms for addressing them, resulting in a debate about the nature and components of security and the need to expand its definition by incorporating new variables.

Consequently, these cyber threats have become a real danger to society, characterized by their ease of execution by users of information technology and communications, transcending national borders, and their global network proliferation, transforming from the physical realm to the virtual world.

Significance of the study:

The importance of this study lies in its examination of cyber threats and their basic concepts, and in highlighting the role of cybersecurity in addressing these new challenges. Recently, there has been a growing interest among researchers and professionals in cybersecurity issues and threats in cyberspace, due to the worsening effects that threaten the stability of nations and individuals, especially in light of the evolving criminal methods that have led to new forms of crime related to digital technology.

Objectives of the study:

The objective of the study of this topic is to shed light on the various threats emanating from cyberspace, considering it a significant issue at the international and national levels, due to the multitude of conflicts and tensions at the internal, regional and international levels. It aims to reveal the forms of threats in the digital world, to identify the strategies adopted to confront them, to understand the legal texts related to

cybersecurity, and to explore the extent to which national legislation is in line with international treaties and conventions in the cyber domain.

Research Question:

In light of the widespread digital revolution and the various challenges it has brought, which have affected all sectors, the following question can be posed: To what extent has legislative policy been successful in addressing cybersecurity threats?

This main question can be broken down into several sub-questions:

1. How effective is the legislative role in mitigating these cyber threats?

2. What methods are being used to confront these emerging threats in cyberspace?

Methodology of the study In order to answer the questions posed, this study employs both descriptive and analytical methodologies. The descriptive approach is reflected in the examination of cybersecurity and the challenges of facing cybersecurity threats and how to prevent them. The analytical methodology is manifested in the analysis of various legal texts and scholarly opinions related to the subject of the study.

The topic "Cyber Threats and Cybersecurity: Emerging Threats in Cyberspace and Strategies for Addressing Them" is further detailed as follows:

- Chapter One: Conceptual Introduction to Cyber Threats and Cybersecurity.

- Chapter Two: Strategies for Addressing Cybersecurity Threats.

Finally, the topic concludes with a summary that includes a series of findings and recommendations derived from this study.

Chapter One: Conceptual Introduction to Cyber Threats and Cybersecurity

The issue of cyberspace has become one of the most significant concerns for countries worldwide as it has emerged as a parallel reality to the physical world. Many conflicts and disputes between nations have shifted from the traditional realm to the digital realm.

Before delving into these concepts, it is important to define cyberspace, which refers to the environment in which computer networks exist and through which electronic communication takes place. Frederick Mayor defines it as: "A new human and technological environment for expression, information, and exchange, consisting primarily of individuals from different countries, cultures, languages, and professions, interconnected by a communications infrastructure that enables the digital exchange and transfer of information". Thus, the term "cyber" is used in conjunction with "space" to refer to a prominent expression in the information age, and this concept is broader and more inclusive than just the Internet.

Section 1: Defining the Concept of Cyber Threats

There are numerous direct threats with high impact and likelihood of occurrence, including "cyber attacks," which can take more advanced forms such as cyber warfare, often occurring within the context of political instability, and cyber terrorism. This group represents direct sources of threat to the national security of states.

Subsection 1: Definition of Cyber Threats

To elaborate on cyber threats, they should be defined both linguistically and terminologically as follows:

First - Linguistic Definition of Threat:

A threat is derived from the verb "هدد" (to threaten), meaning to impose harm or damage. Thus, a threat pertains to anything that may disrupt the process of building security or diminish the feeling of safety[1].

It is also defined as "a statement or expression of intent to harm, destroy, or punish in revenge or intimidation." According to the dictionary "Le Petit Robert", it refers to the manner in which terror is etched on someone's face, with the intention of instilling fear of the harm intended.

Second - Terminological Definition of Electronic Threats:

These refer to attacks carried out using electronic mechanisms and networks, such as the internet and computers, aimed at damaging other electronic devices or networks or stealing the information contained within them[2].

They are also defined as the exploitation of computers and information technology to sabotage and destroy the information infrastructure of adversaries, disrupt air defense networks, and infiltrate email systems of state leaders for espionage, according to a systematic plan.

Subsection 2: Forms of Cyber Threats

These attacks can manifest in the following forms:

First - Cyber Attacks:

Cyber attacks constitute some of the most significant threats and challenges to security. They occur over the internet with the intent to destroy, spy, or forge, whether via computers or smartphones. The scope can extend to include devices not connected to the internet, such as generators and motors, which can be destroyed via computer viruses, leading to severe losses, especially if they target state infrastructure[3].

Types of cyber attacks vary according to several criteria, including the method of execution, the targeted audience, the ultimate goal, or the involved actors. The types of cyber attacks can be categorized according to specific criteria as follows:

1. **By Method Used:**

The methods for executing cyber attacks are diverse, including:

- Phishing Attacks: This attack relies on social engineering by enticing the victim to open a link containing malicious software that infects the device or uses viruses to disrupt service networks.

- DDoS Attacks:Flooding the victim with thousands of messages and requests, ultimately leading to service interruptions, whether for a website or a specific governmental or private electronic service.

- Backdoors:Deliberate vulnerabilities left by the system designer on victim devices for the purpose of espionage and surveillance or information gathering[4].

2. By targeted sector:

Cyber-attacks can be carried out by infiltrating ordinary individuals for extortion, targeting private companies to violate intellectual property rights and patents, or attacking the financial and banking sector to damage the national economy or steal funds through cyber fraud and scams. They may also target government services or security agencies to steal intelligence information, military plans, or weapons designs, as well as media institutions[5].

3. According to the goal of the attack:

The goal may be “financial,” such as hacking bank accounts and stealing money; “military,” such as infiltrating military systems; “political,” expressing anger over political decisions or actions; or “human,” showing sympathy for a humanitarian cause[6].

4. According to participating actors:

These attacks are carried out by armed forces and cyber armies as part of military and political conflicts between states, by organized crime groups for theft and money laundering, or by “terrorist groups” as a form of cyber terrorism.

Second ,Cyber Terrorism:

Cyber terrorism poses a clear threat to national security, as evidenced by the use of smart technologies in carrying out cyber terrorist attacks. This includes the use of cyberspace, drones, and robotic systems for such attacks, as well as the use of 3D printers to manufacture weapons[7].

One of the first to use the term "cyberterrorism" was Barry Collin in the 1980s, who found it difficult to provide a comprehensive definition of technological terrorism. However, he adopted a definition of cyber terrorism as "an electronic attack aimed at or directed against governments in pursuit of political, religious, or ideological goals, where the attack has a destructive and damaging effect equivalent to the physical acts of terrorism[8].

Third: Cyber Warfare

Cyber warfare refers to actions taken by nation-states to penetrate the information systems and networks of other countries with the aim of causing damage and destruction. "Herch" defines it as "the penetration of foreign networks to sabotage or dismantle those networks and render them inoperative.[9]"

When defining cyber warfare, it is essential to acknowledge the intellectual contributions of several scholars in the study of electronic warfare, such as John Arquilla and David Ron, who define cyber warfare as "an action or preparation for military operations based on informational principles and mechanisms, which implies disabling or destroying the information and communication systems of the targeted enemy state."

From a legal point of view, electronic warfare can be defined as a system based on terror, distributed through the Internet, aimed at carrying out various acts to intimidate the security of individuals, groups, institutions and states, to exhaust them economically and to plunge them into psychological and social crises resulting from what is known as silent terrorism. This concept comes from a Western perspective and represents a soft, silent war that takes various forms, such as communication between armies and their leaders, weakening transportation and logistical supply networks, attacking economic information, embarrassing politicians, and manipulating technical and artistic content.

The state is the primary actor in cyber warfare, and some nations are beginning to prepare for this type of conflict, either by creating cyber armies within their armed forces, or by entering into political and military agreements not to launch cyber attacks, such as the agreement between the United States and China in 2015[10]. An example of cyber warfare occurred between the United States and Iran in 2009, which has led to the concept of cybersecurity dominating the national security strategies of the United States and the United Kingdom since 2010.

Section Two: Defining Cybersecurity

The term "cyber" refers to everything related to computer networks, the Internet, and cyberspace, which means electronic space (cyberspace). It includes everything related to computer networks, the Internet, various applications (such as WhatsApp, Facebook, and hundreds of other applications), and all the services they provide (such as online money transfers, online shopping, and thousands of services in various walks of life worldwide).

Section One: Definition of Cybersecurity

Cybersecurity refers to the protection of assets through information technology, such as hardware and software, collectively known as ICT (Information and Communication Technologies).

The term cybersecurity implies taking the necessary measures to protect cyberspace from cyber attacks. This is achieved through a range of technical, organizational and managerial means aimed at preventing unauthorized access to electronic information and its illegal and improper use. Thus, cybersecurity aims to ensure the continuity of systems and the information they contain, protecting it with the utmost privacy and confidentiality by following the necessary measures and procedures to protect data[11].

1. Linguistic Definition of Cybersecurity

The term "cybersecurity" consists of two words: "security" and "cyber."

- Security: This refers to the opposite of fear, meaning safety and protection. The root of the verb (to be secure) conveys the meaning of safety and protection.

- Cyber: The term "cyber" has become one of the most widely used terms in the international security lexicon. The word "cyber" is of Greek origin, derived from "kybernentes," meaning the person who steers a ship, and

used metaphorically to refer to a "governor" or controller. Some historians attribute its origin to the American mathematician Norbert Wiener (1894-1964), who used it to express the concept of automatic control.

Section Two: Terminological Definition of Cybersecurity

"Cybersecurity" is defined as "a set of measures taken in the defense against cyber attacks and their consequences, including the implementation of necessary countermeasures." This definition aligns with the authors Neittaanmaki Pekka and Lehto Martti in their book "Cyber Security: Analytics, Technology and Automation", where they describe cybersecurity as "a collection of measures taken in defense against computer hacker attacks and their consequences, involving the implementation of required countermeasures.[12]"

The U.S. Department of Defense has provided a precise definition of "cybersecurity," considering it to encompass "all regulatory measures necessary to ensure the protection of information in all its physical and electronic forms from various crimes: attacks, sabotage, espionage, and incidents." Meanwhile, the European declaration views "cybersecurity" as "the ability of an information system to resist attempts to breach data.[13]"

Section Two: Concepts Related to Cybersecurity

There are numerous concepts related to cybersecurity, the most important of which include:

1. Cyber Deterrence: Cyber deterrence is defined as "the prevention of harmful actions against national assets in cyberspace and assets supporting space operations."

2. Cyber Attack: Cyber attacks are defined as "an act that exploits the capabilities and functions of a computer network for national or political purposes by exploiting a specific vulnerability that allows the attacker to manipulate the system.[14]" 3. Cyber Crime: This refers to a collection of illegal acts and activities that are conducted or disseminated through electronic equipment, devices, or the Internet[15].

4. Information Security: Information security comprises a set of technical and administrative measures that include processes and mechanisms taken to prevent any unauthorized or unintentional intrusion, spying, or hacking to misuse or exploit electronic information and data present in communication and information systems. It also ensures the security, protection, confidentiality and privacy of citizens' personal data, and includes the continuous protection of computer equipment and information and communication systems and services from any alteration or damage[16].

Section Two: Methods for Addressing Cybersecurity Threats

Algeria has prioritized cybersecurity, similar to other countries that have hastened to revise their security policies and incorporate new methods and mechanisms to address these issues, alongside developing the infrastructure related to digital technologies. To this end, Algeria has initiated special programs to combat cyber threats and limit their spread, establishing new agencies that align their roles and capabilities with the changes occurring in this field. Cyber protection has become an essential part of any defense system, securing and protecting its informational domain and ensuring a safe cyberspace for all stakeholders. This focus is grounded in the following key pillars:[17]

Section One: Legislative Response Policy to Cybersecurity Threats

To address cybersecurity threats, Algerian legislators have enacted a series of legal texts, including Law No. 04-15 amending and supplementing the Penal Code, along with several specific laws related to the subject matter. The details are as follows:

Subsection One: Addressing Cybersecurity Threats in the Algerian Penal Code

The Algerian legislator issued Law No. 04-15, which includes amendments to the Penal Code[18]. The seventh section is dedicated to crimes against automated data processing systems and consists of eight articles. Article 394 bis deals with the punishment of anyone who unlawfully accesses or remains in any part of an automated data processing system, or attempts to do so. Article 394 bis 1 establishes penalties for anyone who unlawfully

enters data into an automated data-processing system or removes or alters data therein. Article 394 bis 2 prescribes penalties for anyone who intentionally and unlawfully:

- Designing, researching, collecting, making available, publishing or trading in data stored, processed or transmitted by means of an information system that could lead to the commission of the offences referred to in the first paragraph.

- Possession or Disclosure: Possession, disclosure, publication or use for any purpose of data obtained from any of the offences referred to in this section is prohibited.

- Article 394 bis 3: This article states that the penalty provided for in this section shall be doubled if the crime is directed against national defense or public bodies and institutions, without prejudice to the application of more severe penalties.

- Article 394 bis 4: The legislator emphasized that the legal person who commits one of the specified crimes shall be punished with a fine equal to five times the maximum fine prescribed for natural persons.

- Article 394 bis 5: Whoever participates in a group or conspiracy for the purpose of preparing one or more of the specified crimes, and this preparation is manifested by one or more material acts, shall be punished with the penalties prescribed for the crime itself.

- Article 394 bis 6: It stipulates that, while preserving the rights of those acting in bad faith, there shall be confiscation of the devices, software and means used, as well as the closure of the websites that are the subject of any of the punishable crimes, in addition to the closure of the premises or place of exploitation, if the crime was committed with the knowledge of the owner.

- Article 394 bis 7: This article stipulates that an attempt to commit one of the listed crimes is punishable by the penalties applicable to the crime.

Subsection Two: Addressing Cybersecurity Threats in Special Laws

Law No. 09-04, which contains regulations for the prevention and combat of crimes related to information and communication technology[19], specifies the concept of this law in Article Two as follows:

- Crimes Related to Information and Communication Technologies: These are crimes that affect automated data processing systems as defined in the Penal Code, as well as any other crime committed or facilitated through an information system or electronic communications network.

- Information System: Any separate system or group of interconnected or linked systems, where one or more of them process data automatically in accordance with a specific program.

- Information Data: Any representation of facts, information, or concepts in a form suitable for processing within an information system, including the appropriate programs that enable the information system to perform its function.

- Service Providers: Any public or private entity that provides users with the ability to connect via an information system and/or an electronic communications network, as well as any other entity that processes or stores information data for the benefit of the mentioned communication service or its users.

- Traffic Data: Any data related to communication via an information system produced by it as part of a communication chain, indicating the source of the communication, the recipient, the route taken, the date, volume, duration of the communication, and the type of service.

- Electronic Communications: Any transmission, sending, or receiving of signs, signals, writings, images, sounds, or various information by any electronic means.

Article Three of this law clarifies its scope of application, stating that, subject to legal provisions ensuring the confidentiality of correspondence and communications, the provisions for protecting public order or the requirements of investigations or ongoing judicial inquiries may apply, in accordance with the rules set forth in the Code of Criminal Procedure and this law. It establishes technical arrangements for monitoring electronic

communications, collecting and recording their content in real-time, and conducting search and seizure operations within information systems[20].

In addition, Article Four outlines the circumstances under which electronic surveillance is permitted. Article Five of the same Law grants authorized persons the right to access an information system or a part of it, as well as the stored information data, for inspection purposes, even remotely, and to access information storage systems[21].

Article Six explicitly states the possibility of seizing data relevant to the investigation and the need to ensure its security, as well as the possibility of reconstructing such data to make it usable for investigative purposes, provided that this does not affect its content.

This law also includes provisions that establish general rules related to postal and electronic communications[22].

Section Two: Addressing Cybersecurity Threats Through Specialized Structures

Specialized structures comprise centers and units established to confront cybersecurity threats and their preparedness for action, which will be discussed as follows:

Subsection One: Cybercrime Prevention Center of the National Gendarmerie

This center focuses on analyzing data and information related to cybercrimes, identifying the perpetrators, whether individuals or groups, to secure and maintain information systems, especially those used in official institutions, banks, and households. Established in 2008, it is the only specialized agency in Algeria for this purpose. Its goal is to secure the information system for the benefit of public safety and serves as a documentation center located in Bir Mourad Raïs.

One of the center's objectives is to assist other security agencies in carrying out their duties. The National Gendarmerie has managed to provide qualified and competent personnel, including IT engineers and legal experts, through continuous and distinguished training, international and national meetings, and the exchange of expertise with other countries. This is aimed at achieving a proper understanding of cybercrime and combating it. In this context, the center processed more than 100 cybercrime cases in 2014 and over 500 digital cases in 2015, including 300 crimes related to Facebook and 20 digital crimes involving breaches of official websites of private and public institutions, targeting their automated data processing systems.

Subsection Two: National Institute of Forensic Evidence and Criminal Science of the National Gendarmerie

This is a public institution of an administrative nature directly under the supervision of the Minister of National Defense. It was established by Presidential Decree No. 04-183 of June 26, 2004 and serves as an instrument inspired by practical experience and modern analysis supported by appropriate technologies. The main service provided by this Institute is the support of the judiciary and the assistance to the investigative units within the framework of the judicial police functions[23].

In order to perform its tasks effectively, the National Institute of Forensic Evidence and Criminal Science has several specialized departments, including the Fingerprint Department, the Computer Science Department and the Environmental Department.

Subsection Three: Central Department for Combating Cybercrime of the National Police Directorate

In response to the need for cybersecurity and the fight against security threats in cyberspace, the security services established the Central Department for Combating Cybercrime. This department adapted the security formation of the Judicial Police Directorate, which initially consisted of a unit that formed the core of a special security formation to combat electronic crime at the General Directorate of National Security, established in 2011.

Subsequently, the Central Department for Combating Crimes Related to Information and Communication Technologies was created by a decision of the Director General of National Security and added to the organizational structure of the Judicial Police Directorate in January 2015.

Subsection Four: National Authority for the Prevention and Combat of Crimes Related to Information and Communication Technologies

This is an independent administrative authority established under the Ministry of Justice, operating under the oversight of a committee chaired by the Minister of Justice. The committee primarily includes government members concerned with the issue, security officials, and two judges from the Supreme Court appointed by the Supreme Judicial Council. The authority comprises judges, officers, and agents from the judicial police affiliated with military intelligence, the National Gendarmerie, and the National Police, in accordance with the provisions of the Code of Criminal Procedure. This authority was formed by Presidential Decree No. 15-261.

In 2019, a new Presidential Decree No. 19-172 was issued, repealing Decree No. 15-261, reclassifying it as a public institution with an administrative nature, endowed with legal personality and financial independence, under the authority of the Ministry of National Defense. However, this classification was later revised by Presidential Decree No. 20-183, which described it as an independent administrative authority with legal personality and financial independence, placed under the authority of the President of the Republic. This same description was reiterated in Presidential Decree No. 21-439[24].

The authority is tasked with proposing elements of the national strategy for the prevention and combat of crimes related to information and communication technologies, activating and coordinating prevention operations, and assisting judicial authorities and judicial police in combating these crimes. This is achieved through information gathering, providing expertise, and ensuring preventive monitoring of electronic communications to detect crimes related to terrorism, sabotage, and threats to state security.

CONCLUSION:

From the above discussion, it is clear that the topic of "Cyber Threats and Cybersecurity: Emerging Threats in Cyberspace and Methods of Addressing Them" is a pressing issue that warrants attention and study. It is essential to focus on understanding how to adapt legal frameworks, identify prevention strategies, and develop responses to these threats. This will contribute to guiding legislators in establishing a legislative policy aimed at criminalizing these threats, determining appropriate penalties, and clarifying legal responsibilities.

Cybersecurity is a significant challenge both nationally and internationally, especially with the increase in cyber threats. Like many other countries, Algeria has sought to protect its information systems and national security through security agencies and units since adopting e-governance and digital governance. Cybersecurity has become a fundamental component of the contemporary security framework, which national defense must achieve in light of the growing incidence of cybercrime and threats.

In view of the escalation of serious threats arising from the misuse of the Internet, which has led to a new pattern of cybercrime and various challenges affecting the stability and security of society, several findings and recommendations can be summarized from this study:

1. Strengthen the legal framework: It is critical to develop comprehensive laws that specifically address cybercrime and cybersecurity to provide a clear legal basis for action.

2. Increase awareness and training: Increased awareness and training for law enforcement and the public on cyber threats and prevention strategies is necessary to mitigate risks.

3. Foster international cooperation: Collaboration with other countries and international organizations can enhance capabilities to effectively combat cyber threats.

4. Invest in technology and resources: Providing sufficient resources for cybersecurity infrastructure and technology is essential to protecting information systems and responding quickly to threats.

5. Establish rapid response teams: Establishing specialized units equipped to handle cyber incidents can improve response times and minimize damage from cyber attacks.

By addressing these areas, Algeria can strengthen its cybersecurity posture and better protect its national interests in the face of evolving cyber threats.

First: Key Findings from This Study

1. Cyber Space Challenges: Cyberspace has imposed various challenges on countries worldwide, creating new boundaries of power between nations.

2. National Cybersecurity Strategies: The emergence of cyber threats has led countries to adopt strategies aimed at achieving national cybersecurity in light of current challenges.

3. Technological Advancements: With the development of wireless internet technologies, criminals no longer need to sit behind wired computers to commit crimes, necessitating security agencies to prepare with the latest technologies to counter these cyber threats.

4. Reconsideration of Sovereignty: Cyber threats, attacks, espionage, and electronic breaches have compelled nations to reconsider their complete sovereignty and borders, which become vulnerable if hacked or attacked.

Second: Key Recommendations from This Study

1. Raise cybersecurity awareness: It is critical to promote cybersecurity awareness through campaigns targeting Internet users and encouraging them to take the necessary precautions to ensure a minimum level of security. This includes educating them about encryption mechanisms, necessary precautions when using social media, and fostering a culture of timely reporting to enable relevant authorities to address cyber threats.

2. Establish a national cybersecurity agency: A national agency should be established to ensure cybersecurity and protect data infrastructure from cyber threats.

3. International cooperation framework: An international system based on cooperation among countries should be established, working together within a unified policy and legal framework to combat cyber threats.

4. Training specialized military and security units: Military and security units should be trained and equipped to monitor communications infrastructure, identify potential risks and cyber threats, and develop countermeasures.

5. Establish National Arbitration Bodies: National specialized bodies should be established to address cybersecurity threats and provide pre- and post-adjudication services for any electronic activity for which individuals may seek assistance.

List of Sources and References I - List of Sources First:

Dictionaries

1. Ibn Manzur, Muhammad bin Makram, Lisan al-Arab, Dar Al-Ma'arif, Cairo, 2016.

Second: Legal texts:

1. Law No. 04-15 dated 27 Ramadan 1425 (November 10, 2004), amending and supplementing Decree No. 66-156 on the Penal Code.

2. Law No. 09-04 of 14 Sha'ban 1430 (August 5, 2009), concerning special provisions for the prevention of and fight against crimes related to information and communication technologies, published in the Algerian Official Gazette, number 47, dated 25 Sha'ban 1430 (August 16, 2009).

3. Law No. 18-04, dated 24 Sha'ban 1439 (May 10, 2018), concerning general rules on postal and electronic communications, published in the Official Gazette, Algeria, Issue 27, May 2018.

4. Law No. 18-07 dated 25 Ramadan 1439 (June 10, 2018), concerning the protection of natural persons in the context of the processing of personal data, published in the Official Gazette, Algeria, Issue 34, June 10, 2018.

5. Presidential Decree No. 04-183 of 8 Jumada al-Awwal 1425 (June 26, 2004), establishing the National Institute of Forensic Evidence and Criminal Science for the National Gendarmerie and defining its basic law, published in the Official Gazette of Algeria, number 41.

6. Presidential Decree No. 21-439 of 2 Rabi' al-Thani 1443 (November 7, 2021), reorganizing the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, published in the Official Gazette of Algeria, No. 86 of 6 Rabi' al-Thani 1443 (November 11, 2021), p. 5.

First: Legal

Books:

1. Aws Majid Ghaleb Al-Awadi, Cyber Information Security, Al-Bayan Center for Studies and Planning, Beirut, 2016.

2. Hassan Emad Makawy, Modern Communication Technology in the Information Age, Egyptian Lebanese House, Cairo, 4th edition, 2005.

3. Tarek Ibrahim Al-Dasouqi Ateyah, Information Security (The Legal System for Information Protection), Dar Al-Jamea Al-Jadida for Publishing, Cairo, 2009.

4. Mouna Al-Ashqar Jbour, Cyber Security: Challenges and Requirements for Confrontation, Arab Center for Legal and Judicial Research, Beirut, 2012.

5. Noran Shafiq, The Impact of Cyber Threats on International Relations: A Study in the Dimensions of Electronic Security, Arab Knowledge Office, Cairo, 2014.

Second: Scientific Articles

1. Ahmed Abois Ni'mah Al-Fatlawi, "Cyber Attacks: Their Concept and Emerging International Responsibility in Light of Contemporary International Regulation," Al-Muhqiq Al-Hilli Journal of Legal and Political Sciences, University of Babylon, Faculty of Law, Iraq, Issue 4, Year 8, 2016.

2. Ismail Jabourbi, "The Role of Cybersecurity in Countering Electronic Threats: A Case Study of Algeria," Transformations Journal, University of Ouargla, Algeria, Issue 2, December 2020, Volume 3.

3. Al-Mokhtar Al-Majidri, "Electronic Terrorism: Issues of Criminal Evidence and Combating It," Journal of Political Sciences and Law, Democratic Arab Center, Berlin, Germany, Issue 14, 2019, Volume 3.

4. Belkhalem Mohammed, "Emerging Economic Crimes," Journal of Legal and Political Research and Studies, Issue 05, 2013.

5. Houssein Rabii, Mahmoud, and Samar, "Cyber Wars: Risks and Strategies for Achieving International and Domestic Cybersecurity," Algerian Journal of Human Security, University of Batna 1, Algeria, Issue 02, Year Seven, Volume 07, July 2022.

6. Hakim Gharib, "New Security Threats and the Logic of Building Defense and Security Policies," Political Horizons Journal, Issue 2, 2022, Volume 6.

7. Rawaan Bint Atiyah Allah Al-Sahafi, "Cyber Crimes," Comprehensive Multidisciplinary Electronic Journal, Issue 24, May 2020.

8. Sharifa Kalaa, "Cybersecurity and the Challenges of Espionage and Electronic Breaches of States through Cyberspace," Journal of Rights and Human Sciences, Issue 01, Volume 15, 2022.

9. Adel Abdel Sadiq, "The Danger of Cyber Wars in Cyberspace," Ahram Computer Internet and Communications Journal. Cairo, 2017.

10. Mohammed Ahmed Al-Mashhadani, "Economic Crimes: Types, Methods of Combating, and Prevention," Journal of Legal Sciences ,Volume 20, Issue 01, 2005.

11. Mohammed Suwailem, "On Terrorism and Electronic Terrorism: Ambiguities of the Concept and Overlapping Approaches," Journal of Extremism and Armed Groups, Democratic Arab Center, Berlin, Germany, Issue 1, Year 1, May 2019.

12. Mohammed Mseika, “Cyberspace and National Security Challenges for States,” Journal of Legal and Social Sciences, University of Zian Achour, Djelfa, Issue 04, Volume 07, December 2022.

13. Nawal Belharbi, “New Security Threats and Ways to Counter Them: What Role for Smart Borders?” Legal and Political Research Journal, Issue 1, June 2022, Volume 7.

14. Yasmin Bel’asal Bint Nabi, Hussein Amroush, “Electronic Threats and Cybersecurity in the Arab World,” Numerous Academic Journal, University Center of Maghnia, Algeria, Issue 2, Volume 2, 2021.

Third: Scientific Events

1. Younes Arab, “Computer and Internet Crimes – An Overview of the Concept, Scope, Characteristics, Images, and Procedural Rules for Prosecution and Evidence,” Paper presented at the Arab Security Conference, Arab Center for Studies and Criminal Research, Abu Dhabi, 2002

Fourth: Websites

1. - Al-Quds Al-Arabi, “Cybersecurity Occupies High Authorities in Algeria: Talk of ‘Attempts at Hacking, Sabotage and Espionage’”, published on the website on 10/29/2023 at 18:00. [Al-Quds Al-Arabi](https://www.alquds.co.uk/)

III - Foreign Language References

1. Dan Craiyen et al. “Defining Cybersecurity,” Technology Innovation Management Review, Montreal, Canada, October 2014.

2. Jean de Maillard, Un monde sans loi, Stock, France, 2001.

3. James Johnson, “Artificial Intelligence & Future Warfare: Implications for International Security,” Defense & Security Analysis, No. 02, Vol. 35, 2019.

4. Maecel Leclerc, La criminalité organizée. La Documentation Française, Paris, France, 1996.

Footnotes:

[1]- Ibn Manzur, Muhammad bin Makram, Lisan al-Arab, Dar Al-Ma'arif, Cairo, 2016.

[2]- Yasmin Bel'Assal, Bint Nabi, and Al-Hussein Amrouch, "Electronic Threats and Cybersecurity in the Arab World," Numerous Academic Journal, University Center Maghnia, Algeria, Issue 2, Volume 2, 2021, pp. 163-164.

- Nouran Shafiq, The Impact of Electronic Threats on International Relations: A Study of the Dimensions of Cybersecurity, Arab Office for Knowledge, Cairo, 2014, p. 40.

[3]- Maecel Leclerc, Organized Crime, La Documentation Française, Paris, France, 1996, p. 100.

[4]- Muhammad Msekka, "Cyberspace and the Challenges of National Security for States," Journal of Legal and Social Sciences, Zian Achour University, Djelfa, Issue 04, Volume 07, December 2022, p. 455 and beyond.

[5]- Rawan Bint Atiah Allah Al-Sahafi, "Cyber Crimes," Comprehensive Multidisciplinary Electronic Journal, Issue 24, May 2020, p. 08.

[6]- Hassan Emad Makawi, Modern Communication Technology in the Information Age, Egyptian Lebanese Publishing House, Cairo, 4th Edition, 2005, p. 28.

[7]- Al-Mukhtar Al-Majidri, "Cyber Terrorism: Challenges of Criminal Evidence and Suppression," Journal of Political Science and Law, Democratic Arab Center, Berlin, Germany, Issue 14, 2019, Volume 3, p. 257.

[8]- Muhammad Suwailem, "On Terrorism and Cyber Terrorism: Ambiguities of the Concept and Intersection of Approaches," Journal of Extremism and Armed Groups, Democratic Arab Center, Berlin, Germany, Issue 1, Year 1, May 2019, p. 21.

[9]- Houssein Rabie, Mahmoud, and Samar, "Cyber Wars: Risks and Strategies for Achieving International and Internal Cybersecurity," Algerian Journal of Human Security, Batna 1 University, Algeria, Issue 02, Year Seven, Volume 07, July 2022, p. 176.

[10]- Adel Abdel Sadiq, "The Danger of Cyber Wars in the Electronic Space," Al-Ahram Computer, Internet, and Communications Journal, Cairo, 2017, p. 27.

Dan Craiyen et al., "Defining Cybersecurity," Technology Innovation Management Review, Montreal, Canada, October 2014, p. 14.

[11]- Aws Majid Ghalib Al-Awadi, Cyber Information Security, Al-Bayan Center for Studies and Planning, Beirut, 2016, p. 06.

[12]- Nawal Belharbi, "New Security Threats and Ways to Address Them: What Role for Smart Borders?" Legal and Political Research Journal, Issue 1, June 2022, Volume 7, p. 1169.

[13]- Ahmed Abis Ni'mat Al-Fatlawi, "Cyber Attacks: Their Concept and the Emerging International Responsibility in Light of Contemporary International Regulation," Al-Muhqiq Al-Hilli Journal for Legal and Political Sciences, University of Babylon, Faculty of Law, Iraq, Issue 4, Year 8, 2016, p. 30.

[14]- Yunus Arab, "Computer and Internet Crimes – An Overview of the Concept, Scope, Characteristics, and Procedural Rules for Prosecution and Evidence," Paper presented at the Arab Security Conference, Arab Center for Criminal Studies and Research, Abu Dhabi, 2002, p. 08.

[15]- Reda Mahdi, "Cyber Crimes and Mechanisms for Combating Them in Algerian Legislation," Eliza Journal for Research and Studies, Issue 2, 2021, Volume 6, p. 113.

[16]- See also: Tarek Ibrahim Al-Dessouki Attia, Information Security (The Legal System for Information Protection), Dar Al-Jami'a Al-Jadida Publishing, Cairo, 2009, p. 50.

[17]- Al-Quds Al-Arabi, "Cybersecurity Occupies High Authorities in Algeria: Discussions on 'Attempts at Intrusion, Sabotage, and Espionage'," published on the website on 29/10/2023 at 18:00. [Link](https://www.alquds.co.uk/)

[18]- Law No. 04-15 dated 27 Ramadan 1425, corresponding to November 10, 2004, amending and supplementing Order No. 66-156 containing the Penal Code.

[19]- Law No. 09-04 containing special rules for preventing and combating crimes related to information and communication technologies, dated 14 Sha'ban 1430, corresponding to August 5, 2009, Official Gazette, Algeria, Issue 47, published on 25 Sha'ban 1430, corresponding to August 16, 2009, p. 5.

[20]- See: Article 3 of Law No. 09-04 mentioned above.

[21]- Article 4 of Law No. 09-04 mentioned above identifies these cases as follows:

- To prevent actions described as terrorism or sabotage, or crimes affecting state security.

In the case of information about a potential attack on an information system that threatens public order, national defense, state institutions, or the national economy.

For the purposes of investigations and judicial inquiries, when it is difficult to reach a result concerning ongoing investigations without resorting to electronic surveillance.

In the framework of executing requests for mutual legal assistance.

In the framework of executing requests for mutual legal assistance.

[22]- Law No. 18-04 dated 24 Sha'ban 1439, corresponding to May 10, 2018, which sets general rules concerning postal services and electronic communications, published in the Official Gazette, Algeria, Issue 27, May 2018.

[23]- Presidential Decree No. 04-183 dated 8 Jumada al-Awwal 1425, corresponding to June 26, 2004, establishing the National Institute of Criminal Evidence and Criminal Science for the National Gendarmerie and defining its basic law, Official Gazette, Algeria, Issue 41, p. 18.

[24]- Presidential Decree No. 21-439 dated 2 Rabi' al-Thani 1443, corresponding to November 7, 2021, reorganizing the National Authority for the Prevention of Crimes Related to Information and Communication Technology and Combatting Them, Official Gazette, Algeria, Issue 86, published on 6 Rabi' al-Thani 1443, corresponding to November 11, 2021, p. 5.