Cybercrime and cybersecurity challenges in Algeria

Slimane Nebbar
PhD in Political Science and International Relations, university Mohamed khider Biskra-Algeria, slimane-nebbar@univ-biskra.dz

Received: 18/05/2026 *Accepted: 08/06/2026* *Published:10/06/2026*

Abstract:

The research aims to describe and analyze Algeria's experience in confronting cybercrime and the challenges it faced in achieving cybersecurity. The increase in cybercrimes' ratio in Algeria during the last decade has led to the establishment of legal institutes that penalizes the misuse of modern technologies. Algeria has also initiated the legislation and establishment of several entities and agencies responsible for investigation and monitoring. These units have varied responsibilities depending on the security authorities they are affiliated with. The results have shown that the evolution of cybercrimes and their forms in recent years has led to the formation of specialized establishments.

Keywords: cybercrime; cyber security; challenges;security establishment.

Corresponding author**: SLIMANE NEBBAR, **e-mail:** **slimane-nebbar@univ-biskra.dz

1. INTRODUCTION

The Internet and modern technologies have rendered a great service to humanity by granting it a passport to openness toward the world. They have also provided new forms of communication and data management, while enhancing the efficiency and speed of electronic services. On the flip side, this digital environment has engendered numerous unethical and illegal challenges that have frequently impacted the psychological state, mindset, and behavior of both individuals and collectives.

A shift in the system of values, concepts, and behaviors has accompanied the evolution of digital devices and the global proliferation of the Internet. The electronic environment has come to pose a threat to the security of individuals and society, driven by the perceived freedom, anonymity, and the ability to infringe upon others that it affords internet users. Consequently, this has led to a rise in the rates and sophistication of cybercrime, affecting the security of individuals, society, and the State.

The advancement of technology has coincided with the growth of emerging transnational crimes, posing a threat to nations and compelling them to formulate strategies and regulations to mitigate cybercrime and enforce cybersecurity. Algeria, like other nations, has undertaken the responsibility to counter this phenomenon by drafting legal systems and legislative frameworks that penalize anyone who threatens the security of individuals and the State. Furthermore, it has established specialized centers tasked with investigating, tracking perpetrators, and preventing and responding to cybercrime.

2. Research Problem (Problematique)

Algeria is among the countries affected by cybercrime in all its forms, which continues to pose an electronic threat detrimental to both cybersecurity and national security. To counter this type of crime, Algeria has adopted a set of mechanisms, including drafting legislative texts and establishing security agencies tasked with investigating and conducting enforcement operations to control cybercrime and achieve cybersecurity.

This article is a descriptive-analytical study of the reality of cybercrime in Algeria and the mechanisms the Algerian State has adopted to confront it. The core research question is formulated as follows:

- **What are the mechanisms adopted by Algeria to confront the challenges of cybercrime and achieve cybersecurity?**

To answer this central question, the study is structured around the following core elements:

- Defining the concepts **of cybercrime and cybersecurity**.
- Analyzing the rates and forms of cybercrime in Algeria in recent years.
- Examining the newly introduced legal frameworks that penalize cybercriminals.
- Outlining the mandates of the security centers and agencies established by Algeria to confront cybercrime challenges.

3. Defining Cybercrime

The term informational, digital, electronic, or cybercrime is a modern concept composed of two elements: the first is "crime," and the second is "cyber" or "electronic," which is used to describe concepts related to computing or the information age. As Dr.Tariq Abdel-Wahab Selim describes it, these are "silent crimes" that require neither physical force, violence, nor conventional weapons. (سليم، 1997، صفحة 150).

Cybercrime is therefore defined as "any illicit conduct associated with the misuse of computers, resulting in the realization of unlawful objectives."(المحلاوي، 2016، صفحة 40).

The responsibility for defining cybercrime has fallen to legal jurisprudence, drawing on general principles of law while adapting to the novel elements inherent to electronic offenses. Consequently, a multitude of definitions have emerged: some narrowly conceptualize cybercrime by focusing on its typology, while others categorize it by the perpetrator's profile. Conversely, broader definitions expand the scope of cybercrime to encompass all illicit activities and practices involving information and communication technologies (ICT), computer systems, electronic devices, and the Internet. (بهلول، 2018، صفحة 283).

Cybercrime is defined as any criminal offense committed utilizing a computer via an internet connection, aimed at network intrusion and sabotage, falsification, forgery, theft, embezzlement, piracy, and the infringement of intellectual property rights. It is also defined as "a crime resulting from the input of fraudulent data into systems, the misuse of outputs, in addition to other acts that constitute more technically complex offenses, such as unauthorized computer modification."(عريان، 2010، صفحة 03).

The multiplicity of conceptual definitions for cybercrime is directly linked to the diverse analytical perspectives adopted by researchers. Some definitions are strictly legal, while the typologies, mechanisms, or subject matters of the crime determine others. Furthermore, some concepts are categorized by the perpetrators—whether individuals, organizations, or governments. In contrast, alternative interpretations focus on criminal intent, such as violating the rights of others and inflicting informational, material, or intellectual harm.

4. Definition of Cybercrime in Algerian Legislation

Today, cybercrime has proliferated to such an extent that countering it, which directly impacts national security, has become an absolute necessity. Consequently, numerous national and international legislations have been amended; this category of crime has been codified as a punishable offense under the law, and sanctions have been imposed to curb its expansion.

Under the 2004 amendment to the Penal Code, the Algerian legislator sought to criminalize cybercrimes, which had begun to proliferate within Algerian society. Consequently, a dedicated section was introduced outlining sanctions applicable to offenses involving attacks on automated data processing systems. In 2009, the first legal text specifically addressing cybercrime and its prevention was enacted, introducing the terminology of "offenses related to information and communication technologies." These were defined as "offenses involving attacks on automated data processing systems as specified in the Penal Code, as well as any crime committed or facilitated through an information system or an electronic communication network."

In 2021, an additional and more complex definition was introduced: "An offense related to information and communication technologies of a highly complex nature is defined, under this law, as a crime that—owing to the multiplicity of perpetrators, accomplices, or victims, or due to the broad geographical scope of its commission, the gravity of its consequences or resulting damages, its organized or transnational character, or its infringement upon public order and security—requires the deployment of special investigative techniques, specialized technical expertise, or recourse to international judicial cooperation."*(Ordinance No. 21-11 of August 25, 2021, supplementing Ordinance No. 66-155 of June 8, 1966, sustaining the Code of Criminal Procedure, Article 211 bis 25).* Comparing this text with its predecessor, this definition offers a more precise scope, emphasizing the number of parties involved in the crime, its geographical dimension, the magnitude of its impact on individuals, institutions, and public security, as well as the necessity for specialized investigative tools and international cooperation to confront the multifaceted dimensions of cybercrime.

5. Definition of Cybersecurity

Cybersecurity is defined as the science of protecting information against potential threats, or the barrier that prevents attacks on it. This is achieved by deploying the necessary tools and means to safeguard information from internal or external risks. It encompasses the standards and protocols implemented to prevent unauthorized access to information transmitted via communications, ensure the authenticity and integrity of these communications, and protect against potential risks arising from the exploitation of system vulnerabilities and weaknesses. (2019 ،شوابكة).

6. Components of Cybersecurity

The terms "cybersecurity" and "cybercrime" often imply that confidential information has been compromised. In reality, maintaining data confidentiality is merely one dimension of security. Experts in the field assert that computer and information security rests upon three pillars of equal significance, known as **the CIA Triad**: **Data Confidentiality**, **Data Integrity**, **and Data Availability**.

7. Procedural Rules for the Prevention and Countering of Cybercrime in Algerian Legislation

In 2009, **Law No. 09-04 of August 5,** 2009, was enacted, outlining specific rules for the prevention and countering of offenses related to information and communication technologies. At the time, this was considered the Algerian government's definitive first step toward confronting cybercrime. The legislation was drafted by an elite group of legal scholars, with the active participation of experts and professionals specialized in electronic media from various sectors. The law comprises 19 articles distributed across 6 chapters, covering the scope of application, surveillance of electronic communications, the judicial conditions for such surveillance, and procedural rules governing digital search and seizure.

To detect and combat cybercrimes, the Algerian legislator established a set of procedural rules mandated under Law No. 09-04, which include:

7.1 Surveillance of Electronic Communications

The legislator operates under the principle of the legal protection of personal data, a right enshrined in the Constitution, the supreme law of the land. This falls within the general framework governing the legal protection of individuals' private lives, which necessitates safeguarding their personal data against violations arising from automated processing. (أمحمدي، 2017، صفحة 73) ،...and it established an exhaustive list of specific cases where recourse to electronic surveillance is legally permitted, namely:

- **Prevention of acts classified as terrorism, sabotage, or offenses against state security.**
- **If intelligence/information is available regarding a potential attack on an information** system in a manner that threatens public order, national defense, state institutions, or the national economy.
- **For judicial investigations and inquiries,** when it proves difficult to achieve a breakthrough in the ongoing investigation without resorting to electronic surveillance, it may be necessary to resort to it.
- **Within the framework of executing requests for mutual international judicial assistance.** (المادة (04) من القانون 09-04).

Given the gravity of this measure and its potential infringement on individuals' privacy, the legislator stipulated that electronic surveillance is strictly prohibited without a written warrant issued by the competent judicial authority. Furthermore, the first case—concerning acts classified as terrorism, sabotage, or offenses against state security—was subject to special procedures. These fall under the jurisdiction of the Attorney General at the Algiers Court of Justice, and are executed by judicial police officers of the National Body for the Prevention and Countering of Information and Communication Technology-Related Offenses.

7.2 Search of Information Systems

To combat cybercrimes and within the framework of the provisions of the Code of Criminal Procedure, the legislator authorized judicial authorities and judicial police officers to gain access—including remote access—for the purpose of searching:

- **An information system, or any part thereof, as well as the digital data stored within it.**
- **An information storage system.**(المادة (05) من قانون 09-04).

In this regard, the legislator was keen to facilitate international cooperation, emphasizing the importance of rendering international assistance in combating cybercrimes, in accordance with the provisions of international conventions and the principles of reciprocity.

The Algerian legislator has, in general, addressed the legislative vacuum in the field of cybercrime through **Law No. 04, which** amends the Penal Code. This law criminalized specific acts associated with the automated processing of data, namely:

- **The Offense of Unauthorized Access or Intrusion:** This crime is committed as soon as fraudulent and unauthorized access to an information system is established, whether such access or the presence within the system affects the entire infrastructure or merely a portion thereof. This is codified **in Article 394** bis of the Penal Code.

The Offense of Digital Forgery: The criminal activity in this offense is restricted to the acts of inputting, erasing, or modifying data. It is not legally required for these actions to occur collectively to constitute criminal activity; the material element (*actus reus*) of the crime is established by committing any single act independently. However, the common denominator among all these acts is that they involve manipulating data within the data processing system—either by entering new, fraudulent data or by erasing and modifying existing records. (خثير، 2010، صفحة 123).

- **The legislator reaffirmed the penalization of these offenses in Article 394 bis 1.**
- **The Offense of Data Misappropriation (Seizure of Data):** This constitutes one of the most prevalent crimes in the virtual world, as codified **in Article 394 bis 2**.
- **The Offense of Data Destruction and Erasure:** The Algerian legislator addressed this crime **in Article 394 bis 1**of the Penal Code.
- **The Offense of Computer Fraud (Digital Fraud):** This is governed by **Article 394 bis 2/1**.

Internet Activities Embodying Harmful Content and Illicit Conduct:

The provisions of Section Seven bis of the Penal Code, **particularly Article 394 bis 2/2**, criminalize acts of possession, disclosure, and dissemination involving automated data for unfair competition, espionage, terrorism, incitement to debauchery, and all other illicit acts, prescribing penalties of both imprisonment and fines. Furthermore, **Article** 394 mandates an ancillary penalty consisting of the closure of websites that serve as the locus or subject of any offense stipulated under Section Seven bis of the Penal Code. (قانون 04-15 ، 10 نوفمبر2004).

7.3 Seizure of Digital Data

The Algerian legislator granted the authority to search—upon discovering stored data within an information system that proves useful in uncovering cybercrimes or identifying their perpetrators—the leverage to copy the target data. Furthermore, the auxiliary data necessary for

understanding such information shall be subject to seizure in accordance with legally prescribed rules, in instances where it is deemed unnecessary to seize the entire information system. (04-09 من القانون (06) المادة).

These laws make it evident that Algeria, like other nations, has made significant legislative efforts to address cybercrime. However, critics argue that the practical enforcement of these statutory provisions remains limited, owing to oversight of the technical dimensions essential to classifying such crimes and determining appropriate penalties for their perpetrators; in most instances, sanctions have been confined to monetary fines. Consequently, one researcher concluded that, despite the immense efforts deployed by the Algerian legislature to counter cybercrime, these efforts remain insufficient to achieve the desired objective. Given the rapid and continuous evolution characterizing this phenomenon (2022 ،عيمور)،

Some argue that deficiencies within the legislative and regulatory framework, coupled with the laws' failure to encompass the diverse constitutive elements of the digital space, alongside a disproportionate reliance on deterrent measures and preventive protocols to curb piracy, demonstrate a lack of command over information and communication technologies (ICTs) (2019 ،بوازدية).

Consequently, technological advancement outpaces legislative frameworks and legal deterrence mechanisms at a significantly faster rate. This reality compels key actors to prioritize continuous updates to training programs while ensuring the availability of institutional competency and specialization.

8. Forms of Cybercrime in Algeria

In 2009, Algeria established a specialized division within the Sub-Directorate of Scientific and Technical Police to combat cybercrime, focusing on digital forensics. The departments of the General Directorate of National Security (DGSN) recorded numerous cybercrime cases. Specifically, 515 cases were processed during 2012, including 126 cases involving the illegal exploitation of digital tools, 154 related to mobile telephony, and 103 concerning photographs and videos.

During the first half of the same year, the Central Cybercrime Unit processed 15 cases involving violations of personal privacy (compared to 6

cases processed in the entirety of 2012), 4 cases of defamation (8 cases in 2012), 11 cases of extortion (4 cases in 2012), 1 case of identity theft (4 cases in 2012), and 24 cases related to hacking/piracy (10 cases in 2012). The specialized digital forensics division notes that the vast majority of offenses involve modern technologies, particularly computers, the Internet, and mobile phones. Furthermore, over 100 cases were recorded during the first 9 months of 2014, most of which pertained to fraud and swindling targeting individuals.

In the first half of 2015, security services recorded 417 cybercrime cases, which encompassed identity theft, fraud and swindling, digital forgery, sabotage of personal and public data, extortion using hacked images or information, defamation, and electronic theft. The proliferation of such cases is attributed to the exponential increase in Internet use across all social demographics, leading to a rise in both the number of cyber-piracy and fraud victims and the overall volume of cybercriminals.(لطرش و بن عزوز، 2016).

Data analysis of the recorded offenses revealed that cyber-defamation and insult ranked at the forefront, accounting for more than 55 percent. Crimes against public security followed this, then offenses violating privacy and the disclosure of secrets, and finally, extortion, fraud, swindling, sexual exploitation, acts contrary to public decency, and similar offenses.(باشوش، 2021).

Furthermore, a study conducted by "Djamila Ben Abed and Fatima Ben Abed" indicated that 126 cybercrimes were recorded in 2017 within the Wilaya of Laghouat. Among these, offenses of defamation, solicitation (allurement), and coercion (threats) accounted for 20 percent and were categorized as offenses infringing upon the supreme interest of the country. This was followed by a rate of 15.87 percent, totaling 20 crimes representing "unresolved cases" (non-prosecution cases). These are instances where a formal complaint was filed against the perpetrators but subsequently withdrawn, such as cases of solicitation, insult, and defamation. This phenomenon is attributed to the fact that the perpetrator is frequently a relative or an acquaintance of the plaintiff. (بن عابد و بن عابد، 2022).

Statistics for 2018 recorded the highest proportion in "defamation cases," ranking at the top with a rate of 13.54 percent, totaling 42 crimes that

involved defaming individuals and tarnishing their reputations. This was followed by a rate of 7.41 percent, totaling 23 crimes consisting of "insult cases"—whether committed through written text, drawings, or printed materials disseminated via electronic or voice mail. Defamation and slander cases accounted for 6.77 percent, totaling 21 cases involving the publication of misinformation about individuals or institutions for public denunciation or the spreading of rumors. Furthermore, 17 cases, representing a rate of 5.58 percent, were categorized as "infringements upon the privacy of individuals" without their knowledge or consent, involving posting offensive comments about them or threats and extortion (بن عابد و بن عابد، 2022).

- Statistics for 2018 recorded the highest proportion in "defamation cases," ranking first at 13.54 percent, totaling 42 crimes that defamed individuals and tarnished their reputations. This was followed by a rate of 7.41 percent, totaling 23 crimes consisting of "insult cases"—whether committed through written text, drawings, or printed materials disseminated via electronic or voice mail. Defamation and slander cases accounted for 6.77 percent, totaling 21 cases involving the publication of misinformation about individuals or institutions for public denunciation and the spread of rumors. Furthermore, 17 cases, representing a rate of 5.58 percent, were categorized as "infringements upon the privacy of individuals" without their knowledge or consent, involving posting offensive comments about them or threats and extortion (بن خليفة و عبد القادر، 2017).

9. Mechanisms for Countering Cybercrime and Achieving Cybersecurity in Algeria

In preparation for confronting cybercrime, which has aggressively penetrated cyberspace, Algeria—like all other nations—began formulating legal frameworks to regulate its spread and impact. Furthermore, the state established specialized bodies to track and investigate digital offenses. Consequently, specialized entities and departments were created under the National Security apparatus, the National Gendarmerie, and the General Staff of the People’s National Army (ANP).

9.1 Entities Affiliated with the National Security Apparatus

These entities emerged following the law published in the Official Gazette of the Algerian Republic (Issue No. 47, August 16, 2009), which mandated, in its fifth chapter, the establishment of the National Body for the Prevention and Countering of Information and Communication Technology-Related Offenses.

A. The National Body for the Prevention and Countering of Information and Communication Technology-Related Offenses: This body was established, and its core mandates were defined within Chapter Five, specifically under Articles 14 to 17, which encompass:

- **Activating and** coordinating operations dedicated to the prevention and countering of offenses related to information and communication technologies.
- **Assisting judicial** authorities and judicial police departments in their ongoing criminal investigations.
- **The legislation** underscored, in its final chapter, the principle of international judicial cooperation and mutual assistance based on reciprocity, as well as the exchange of intelligence with foreign counterparts, aiming to gather all pertinent data necessary to identify and locate perpetrators of ICT-related crimes.

In light of the escalating importance of modern communication technologies for both individuals and institutions (public and private) and the concurrent rise in cyber offenses, this body was established by presidential decree in 2009. Its objective is to ensure optimal management of these crimes and to confront cyber threats effectively, regardless of their origin. It is tasked with countering harms that may compromise information security, the dissemination of rumors, or any damage targeted at critical infrastructure, espionage, and the exploitation of cyberspace for terrorist recruitment, while delivering technical reports to the competent authorities.

The body operates in close coordination with national institutions concerned with cybersecurity (The People's National Army, the Police, and the Judiciary), as well as with counterpart organizations abroad, whether state-affiliated or within regional and international organizations. Furthermore, specific operational units within the security apparatus are tasked with practical, hands-on intervention to confront digital crimes.

At the level of the National Security apparatus, three specialized units are mandated with cyber research and criminal investigation: the **Central Scientific Police Laboratory in Algiers**, the **Regional Scientific Police Laboratory in Constantine**, and the **Regional Scientific Police Laboratory in Oran**. All these entities assume responsibility for investigating, tracking, and analyzing all types of digital evidence. (رابح، 2004).

Specialized departments dedicated to cybercrimes have been established at the level of the Security Directorates across all wilayas (provinces). Among the most prominent of these are the following:

B. The Central Department for Countering Cybercrime Affiliated with the National Security Directorate: In response to cybersecurity prerequisites and to confront the security challenges arising from cybercrimes, and by a decision of the Director General of National Security, the security services established the Central Cybercrime Department at the level of the General Directorate of National Security (DGSN) in 2011. This department was integrated into the organizational structure in 2015 to extend its reach across all wilayas.

The department operates through specialized investigators who handle cybercrime-related complaints at the provincial level using state-of-the-art equipment. Furthermore, it processes similar international cases through close cooperation between this department and counterpart services in numerous countries worldwide. (المصلحة المركزية للجريمة الالكترونية في مواجهة مجرمي العالم الافتراضي، 2016).

The mandates of this department include:

- **Providing criminal law** protection for information.

- **Operating within designated jurisdictions**(local and national), with the capacity for international cooperation in countering cybercrime by defining jurisdictional boundaries.
- **Monitoring and keeping** pace with technological advancements that characterize cybercrime.
- **Countering network intrusions,** piracy, and cyber-espionage.
- **Conducting searches of information** systems pursuant to judicial warrants.
- **Combating** violations of personal and private correspondence.
- **Programming and** organizing internal and external training courses.
- **Investigating** cases of cybercrime.

Algeria ranked **23rd globally** among 29 nations in cybersecurity readiness. At the Arab regional level, it **ranked 10th** in terms of its commitment to the measures outlined in the **Global Cybersecurity Index (GGCI)** (2022 ،بن جدو).

In general, these institutional bodies emerged as a direct response to the escalating rates of cybercrime in all its forms throughout the past decade.

9.2 Entities and Units Affiliated with the General Command of the National Gendarmerie

The entities affiliated with the National Gendarmerie, alongside the various regional departments of the judicial police under its command, play a pivotal role in countering cybercrime by leveraging highly skilled human resources. At the central level, specialized entities have been formed, which can be outlined as follows:

A. **The National Institute of Forensic Science and Criminology of the National Gendarmerie (INCC):** The institute comprises eleven specialized departments across various distinct fields, all of which guarantee expertise, training, instruction, and the provision of comprehensive technical

assistance. Among these, the Department **of Informatics and Electronics is** mandated to process, analyze, and present digital evidence to aid the judiciary while simultaneously providing technical support to investigators. The department is equipped with advanced apparatus, such as a restoration and repair station for damaged devices, information networks, and data visualization/processing equipment.

The Institute is classified as a public institution under the direct authority of the Minister **of National Defense**. Its primary mandates include conducting scientific examinations within the framework of preliminary investigations and executing research on crime detection using high-precision technology. It encompasses several specialized services, including the Informatics **Service**, which is tasked with monitoring, tracking, and investigating network intrusions and cyber-piracy, as well as the reverse-engineering and deconstruction of malicious software. (2004 ،رابح).

The Institute was established pursuant to Presidential **Decree No. 04/133**, dated June 26, 2004, and became fully operational as of January 1, 2009. The interim period between 2004 and 2009 was dedicated to training human resources and acquiring the necessary scientific and technical equipment. The Institute fulfills requests issued by the judicial authority, judicial police officers, and legally empowered authorities, particularly during the processing of complex cases.

It is tasked with achieving cybersecurity by deploying state-of-the-art software and tools, employing specialized human resources in communication technology, networks, and informatics, and detecting cyber-piracy operations. Furthermore, the Institute organizes professional proficiency courses and postgraduate training programs specializing in forensic sciences. It encompasses numerous specialized departments and services that monitor, track, and investigate network intrusions and cyber-piracy operations, as well as detect stolen data and dismantle malicious software. (2019 ،عطية).

Among its primary mandates in the field of cybersecurity are:

- **Expanding and developing comprehensive** databases.
- **Conducting forensic expertise and** scientific examinations within the framework of preliminary inquiries and judicial investigations.
- **Guaranteeing scientific assistance during** complex investigations by deploying advanced forensic police methodologies.
- **Promoting applied research and** investigative methods that have proven effective.
- **Participating in symposia, lectures, and conferences at** both national and international levels.(بارة، 2017).

Cyber threats have necessitated the establishment of specialized departments and bodies, as well as the mobilization of all physical and human resources to counter the risks posed by cybercrime to national security.

B. **The Center for the Prevention of Cybercrime and Computer-Related Offenses of the National Gendarmerie:** Established in 2008, this center is tasked with securing information systems to serve public security. It functions as a documentation and intelligence hub for analyzing data on cybercrimes and identifying their perpetrators, thereby securing the information systems of official institutions, banks, corporations, and individuals alike. It also aims to assist other agencies in performing their duties, particularly in the following areas:

- **Guaranteeing permanent and continuous monitoring of** the Internet.
- **Conducting electronic communications surveillance within** the boundaries permitted by law for the benefit of National Gendarmerie units and judicial authorities.
- **Assisting territorial units of** the National Gendarmerie in detecting offenses associated with information and communication technologies and gathering digital evidence.

- **Participating in cyber-investigation operations for** the benefit of National Gendarmerie units and judicial authorities.
- **Participating in the suppression and deterrence of cybercrimes through** close cooperation with various security services and national bodies.

In 2015, the Center processed approximately 240 cybercrime cases. These encompassed offenses of coercion (threats), offenses against public order, network intrusion crimes, sexual harassment of minors and inciting them to violate public decency, insulting national symbols and institutions, fraud, swindling, and infringements upon the sanctity of private life.(بارة، 2017).

9.3 Entities Affiliated with the General Staff of the People's National Army (ANP)

A. **The Cyber Defense and Systems Security Monitoring Service:** Established in 2015, this service is mandated with ensuring the formulation and execution of the general policy for cyber defense, alongside elevating the security standards of newly developed systems. Furthermore, its responsibilities encompass updating and enforcing the regulatory framework governing cyber defense, safeguarding weapon systems, and maintaining strategic coordination with relevant national entities. (2020 ،جنادي).

The mandates of this service can be specified as follows:

- **Safeguarding military defense systems**(weapons, communications, radars, etc.) against network intrusions and cyberattacks.
- **Securing military installations and** the nation's sovereign geographic domains (land, air, and sea).
- **Coordinating with competent civilian entities tasked** with achieving cybersecurity across various sectors (economic, financial, political, etc.).
- **Detecting and countering espionage** operations.

- **Combating cyber-terrorism,** regardless of the perpetrators involved (state actors, organizations, or individuals).
- **Participating in the formulation of** the state's general policy aimed at achieving cybersecurity.

Among the findings of these specialized services, it is evident that cybercrime in Algeria is proliferating at an exponential rate. Adjudicated figures underscore this trend: in 2017 alone, more than 2,500 cybercrimes were registered. The most prominent of these (accounting for 70 percent) involved violations of personal freedoms, online threats, the dissemination of explicit images, extortion, and cyber-piracy, among others. (بوازدية، 2019).

Despite the establishment of all these security bodies, and in the face of escalating cybercrime figures that continued to threaten national and cyber security—coupled with the inadequacy of these institutions to counter attacks targeting state institutions fully—it became imperative to adopt an effective, long-term strategy. This led directly to the creation of a National Cybercrime Jurisdiction (National Penal Pole for Countering Information and Communication Technology-Related Offenses).

9.4 The National Cybercrime Jurisdiction (Penal Pole)

In light of the evolution of cybercrime, the diversification of its forms, and its growing threat to public order, national security, and society as a whole, the Algerian legislator—in the latest amendment to the Code of Criminal Procedure via Ordinance **No. 21-11 dated August 25, 2021**—established the National **Penal Pole for Countering Information and Communication Technology-Related Offenses**. This Pole represents a specialized judicial authority mandated with adjudicating cybercrimes.

Article 211 bis 22 stipulates: *"There shall be established at the level of the court located at the headquarters of the Algiers Court of Justice, a national penal pole specialized in the prosecution, investigation, and adjudication of information and communication technology-related offenses and associated crimes. It shall also have jurisdiction to rule on the offenses provided for in this chapter if they constitute misdemeanors."*

The Public Prosecutor at the National Penal Pole, as well as the investigating judge and the president of the same Pole, hold exclusive

jurisdiction over the prosecution, investigation, and adjudication of offenses related solely to information and communication technologies, alongside associated crimes, namely:

- **Offenses undermining state** security and national defense.
- **Crimes involving the dissemination and promotion of** malicious news or propaganda that threaten public order and security, and that possess an organized or transnational character.
- **Offenses infringing upon automated** data processing systems belonging to public administrations and institutions.
- **Crimes of trafficking in** persons or human organs, or migrant smuggling.
- **Crimes of discrimination and** hate speech.

Ensuring efficiency in countering and managing this category of crimes requires elevating the effectiveness of law enforcement agencies tasked with combating cybercrime. This necessitates the provision of specialized units within the judicial police, alongside continuous training and professional qualification. (بن يونس، 2022).

The establishment of this Pole was necessitated by a series of social and political transformations within Algerian society, particularly following the Hirak (popular movement) since 2019. This period witnessed escalating waves of public resentment and the proliferation of ideals of freedom, which characterized the core of digital discourse, especially among the youth. Consequently, this led to the registration of numerous offenses categorized as threats to state security, alongside a widespread surge in violations targeting individual privacy and the social, cultural, and even historical sanctities of Algerian society, ultimately undermining state security, its national symbols, and official institutions.

In light of the data provided by the International Telecommunication Union (ITU) annual report (November 2017), which ranked global nations in the field of cybersecurity based on the "level of commitment of countries worldwide to implementing and developing various cybersecurity

technologies," the index categorized nations into three distinct tiers: initiating (underdeveloped), maturing (developing), and leading (advanced) nations. In this context, Algeria ranked 68th globally out of 164 countries included in the report and 9th among 22 Arab nations (2019 ،بوازدية).

Hence, cybersecurity readiness and achievement depend on the acquisition of modern technologies and a thorough understanding of their security architectures.

10. Conclusion

Definitions of cybercrime have proliferated across diverse conceptual lenses. Some emphasize the instrument utilized—namely, the computer—as the differentiating factor between cyber offenses and traditional crimes. Others focus on the perpetrator, while a third perspective centers on the intent of the crime, specifically the infringement upon others to inflict digital, financial, or intellectual harm.

Cyber threats are continually escalating as methods for accessing confidential data for modification, theft, or destruction become more advanced. These threat methodologies can be classified into three primary vectors: network intrusion, social engineering, and malicious software (malware). Algerian legislation defines cybercrime as offenses related to information and communication technologies, characterized as infringements upon automated data processing systems as stipulated in the Penal Code, as well as any crime committed or facilitated through an information system or an electronic communication network. The 2021 legislation underscored the imperative of assessing the number of parties involved in the crime, its geographical scope, and its impact on individuals, institutions, and public security, alongside specialized investigative mechanisms and international cooperation to confront multifaceted forms of cybercrime.

The distinct nature of cybercrime lies in the perpetrators' ability to remain anonymous and evade punishment, necessitating specialized mechanisms and countermeasures. In Algeria, "the crime of defamation and insult" ranks as the most widespread form of cybercrime, driven by anonymity and victims' reluctance to report offenses. Investigations have revealed that the majority of perpetrators are from the victim's family, a trend

compounded by a lack of public awareness of cybersecurity legislation that penalizes the misuse of modern technology.

Algeria has initiated the formulation of legal frameworks to regulate the pace and expansion of this phenomenon, establishing specialized state bodies to track and investigate digital offenses within both the National Security and the National Gendarmerie apparatuses. Furthermore, the state established the National Penal Pole for Countering Information and Communication Technology-Related Offenses, mandated to prosecute, investigate, and adjudicate these crimes.

Ultimately, it can be concluded that while modern communication tools have advanced rapidly, this evolution has been accompanied by widespread adoption by individuals and institutions alike. Consequently, cybercrime has evolved into a criminal phenomenon that mirrors technological advancements, particularly when exacerbated by a deficient understanding of information security mechanisms and the laws penalizing their misuse. Therefore, it is imperative to implement the following recommendations:

- **Developing cybersecurity legislation in** tandem with continuous technological advancements.
- **Acceding to international conventions in** the field of information systems protection, thereby fostering strategic coordination and cooperation with regional and international cybersecurity experts, while organizing scientific conferences and training workshops to leverage global expertise.
- **Guaranteeing continuous training and** capacity-building for human resources tasked with investigation and prosecution, including computer engineers, legal professionals, and judges.
- **Raising public awareness and sensitization,** particularly within educational institutions, by integrating curricular content that highlights the risks of modern technology, especially those threatening the core value systems of children.

- **Establishing specialized media channels tasked** with disseminating awareness across all socialization institutions, most notably the family and the school.
- **Engaging and activating civil society organizations to combat** cybercrime and mitigate its adverse impacts on individuals and society.

11. Bibliography List:

1. **Books :**

- بارة، سمير. (2017). " الأمن السيبراني في الجزائر: السياسات والمؤسسات ". المجلة الجزائرية للأمن الإنساني، الجالد02(ع02)، ص273.
- بن جدو، بن علية. (2022). " تحديات الأمن السيبراني لمواجهة الجريمة الالكترونية ". المجلة الجزائرية للأمن الإنساني، الجولد07(ع02)، ص317.
- بن خليفة، أحمد والأمير عبد القادر، محفوظة. (2017). " الجريمة الإلكترونية وآليات التصدي لها. مجلة الامتياز لبحوث الاقتصاد والإدارة "، المجلد01(ع01)، ص163.
- بن عابد، جميلة وبن عابد، فطيمة. (2022). " الالكترونية في المجتمع الجزائري: دراسة وصفية عن تطور الظاهرة في ولاية الأغواط". مجلة البحوث القانونية والاقتصادية، المجلد05(ع02)، ص.ص272، 275-276.

- بن يونس، فريدة. (2022). " استحداث قطب جزائي وطني لمكافحة الجرائم السيبريانية ومتابعتها- قراءة في الأمر21-11 ". مجلة الدراسات القانونية والاقتصاد، المجلد05(ع01)، ص.ص1709-1710.
- بوازدية، جمال. (2019). " الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والآفاق المستقبلية ". مجلة العلوم القانونية والسياسية، المجلد10(ع01)، ص1280.
- جنادي، إسماعيل. (أوت 2020). " الدفاع السيبراني من أهم تحديات الجيش الوطني الشعبي ". مجلة الجيش الشعبي الجزائري، (ع635)، ص31.
- خثير، مسعود. (2010). الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات. الجزائر: دار الهدى.
- رابح، سعاد. (2004). " ضوابط مكافحة الجريمة المعلوماتية. مجلة القانون العام الجزائري والمقارن "، المجلد02(ع01)، ص.ص266-288.
- شوابكة، عدنان عواد. (2019). "دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف". مجلة دراسات وأبحاث، المجلد11(ع04)، ص168.
- عطية، إدريس. (2019). "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري". مجلة مصداقية، المجلد01(ع01).
- عيمور، راضية. (2022). " الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري ". المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد06(ع01)، ص106.
- الغثير، خالد بن سليمان. (2009). أمن المعلومات: بلغة مسيرة، تقديم محمد بن إبراهيم السويل. الرياض: مكتبة الملك فهد الوطنية.
- لطرش فيروز وبن عزوز حاتم. (2016). " الجريمة الالكترونية في الجزائر من جريمة فردية إلى جريمة منظمة ". مجلة آفاق للعلوم، المجلد01(ع1)، ص.ص330-331.
- المحلاوي، أنيس حسيب السيد. (2016). الخبرة القضائية في الجزائر المعلوماتية. الإسكندرية: دار الفكر الجامعي.
- نافع زينب وشعباني، مجيد. (2020). " تحديات الحكومة الالكترونية في الجزائر: الجريمة الالكترونية نموذجا ". مجلة العلوم الاقتصادية والتسيير والعلوم التجارية، المجلد12(ع01)، ص.ص783-784.

2. Journal article :

- الجمهورية الجزائرية الديمقراطية الشعبية. (16 أوت 2009). الجريدة الرسمية، (ع47).
- قانون 04-15. (10 نوفمبر2004). المواد (394) مكرر2، (394) مكرر6.
- قانون العقوبات. (10 نوفمبر2004). القانون 04-15 المؤرخ في 10نوفمبر2004، المعدل والمتمم للأمر 66-156، المؤرخ في 08 جوان 1966. الجريدة الرسمية، (ع71).
- القواعد الخاصة بالوقاية. (05 أوت 2009). المادة (02) الفقرة الأولى من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية، (ع47)، 05.
- المادة (04) من القانون 09-04.
- المادة (05) من قانون 09-04.
- المادة (06) من القانون 09-04.

3. Seminar article:

- أمحمدي، آمنة بوزينة. (2017). " إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائرية وقانون الوقاية من جرائم الإعلام) ". الملتقى الوطني الأول حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، 29 مارس، الجزائر العاصمة: مركز جيل البحث العلمي.
- سليم، طارق عبد الوهاب. (1997). الجرائم المرتكبة بواسطة الانترنت وسبل مكافحتها. تونس: د.د.ن.
- بهلول، سمية. (2018). دور الإدارة الالكترونية في تفعيل أداء الجماعات الإقليمية في الجزائر. رسالة دكتوراه غير منشورة في العلوم القانون (تخصص إدارة محلية)، جامعة الحاج لخضر باتنة، الجزائر.

- عريان، أمير الفونس. (2010). " الجرائم الالكترونية في البنوك- وكيفية معالجتها ". ورقة مقدمة للمؤتمر الثاني حول الجرائم المستحدثة: كيفية إثباتها ومعالجتها. مصر: المركز القومي للبحوث الاجتماعية والجنائية.

4. Internet websites:

- باشوش، نوارة. (2021). الإجرام الالكتروني.. أرقام مرعبة . https://www.echoroukonline.com.
- المصلحة المركزية للجريمة الالكترونية في مواجهة مجرمي العالم الافتراضي. (2016). https://www.djazairess.com/essalam/52564