

Institutional and technical mechanisms for cyber defense in Algeria

BOUARAR ADEL ^{1*}

¹ University Yahia Fares - Médéa , bouarar.adel@univ-medea.dz

Received: 12/04/2026

Accepted: 31/05/2026

Published:30/06/2026

Abstract:

The article highlights the reality of cybersecurity in Algeria by tracing the evolution of cybercrime, its various forms, and the state's institutional and legal responses, The widespread use of the internet and modern technologies has led to an increase in electronic threats targeting individuals, institutions, and national security.

To address these challenges, Algeria adopted a comprehensive strategy that includes updating legislation and creating specialized bodies such as the Center for the Prevention of Cybercrime, the National Institute of Forensic Evidence, the Central Department for Combating Cybercrime, and the National Authority for the Prevention of Cybercrime. Additionally, a Cyber Defense Department was established to protect vital infrastructures, along with a National Judicial Division specializing in cybercrime.

Despite these efforts, there remains a pressing need to strengthen coordination among institutions, develop specialized expertise, and enhance international cooperation to counter the growing cyber threats.

Keywords: cybersecurity; cybercrime; Electronic threats; Criminology; Cyber defense.

** Corresponding author*

Introduction:

Over the past decade, the world has witnessed a remarkable technological boom in the fields of media and communication. This revolution has given rise to vast cyberspaces where various entities—individuals, institutions, companies, administrations, and even governments—interact continuously. By 2021, the number of internet users worldwide had reached 4.9 billion, representing 63% of the global population. This surge was further fueled by the lockdowns imposed during the COVID-19 pandemic over the previous years.

The interaction of such a massive number of users has inevitably led to a significant increase in cybercrimes, which have taken on various forms. Some are traditional crimes that have simply migrated to virtual environments, while others are newly emerging offenses born from technological and digital advancements. In response to these developments, countries and institutions have been compelled to establish cybersecurity systems aimed at protecting their data and digital infrastructures.

Similarly, Algeria, like all nations of the world, strives to keep pace with digital progress by modernizing its security systems. The goal is to safeguard individuals, institutions, public administrations, and national digital infrastructures. This effort involves updating legal frameworks to address newly emerging crimes and creating specialized institutions capable of effectively tackling cybersecurity challenges.

1. Cybercrime:

1.1 The Nature of Cybercrime:

Over the past decade, patterns of crime have evolved remarkably, expanding their targets beyond physical harm and financial loss to include data and information. This emerging category of crime is often referred to as “white-collar crime” in certain circles, as the modern criminal can now commit offenses without resorting to physical violence, bloodshed, or even leaving their seat. For this reason, some describe such offenses as “soft crimes.”

With just a few keystrokes, a cybercriminal can unleash consequences that may be catastrophic for individuals, institutions, and even entire economies.

What makes this type of crime particularly alarming is its borderless nature — it is not confined to any specific geographic area, but rather transcends countries and continents alike. Hence, cybercrime has become a global issue that affects all nations without exception. (Samira, 2010, p.276)

1.2 Definition of Cybercrime:

Cybercrime has been given various names — some refer to it as computer crime, internet crime, or technological crime. With the diversity of these terms comes a variety of definitions. Some scholars focus on the technical aspect, while others emphasize the legal dimension.

One definition describes cybercrime as a harmful act in which the perpetrator — who is typically knowledgeable in computer technologies — uses a computer system or data network to gain access to data or programs with the intent to copy, alter, delete, falsify, damage, freeze, seize, distribute, or unlawfully publish them (Kamel, 2000).

It is also defined as “crimes committed against individuals or groups with a criminal motive to intentionally harm the victim’s reputation, or to cause physical or psychological harm, directly or indirectly, through modern communication networks such as the internet (social media platforms, chat rooms, email, etc.) and mobile phones (SMS, MMS).” This definition includes any criminal act carried out through computers or networks — such as hacking or unauthorized access — as well as traditional crimes that have been adapted to the online environment.

Dr. Abdel Fattah Mourad defines cybercrime as “acts that violate law and morality, committed via computer systems through the internet. These acts require specialized knowledge of computer technologies and information systems, whether for committing or investigating them. The term also refers to any illicit activity originating in one or more components of the internet, such as websites, chat rooms, or email. For this reason, it is often called a ‘cybercrime’ because it occurs within the virtual world.” Some also refer to it as high-tech crime or white-collar crime (Israel Jibreel, 2016).

Moreover, the misuse of information and communication technologies (ICTs) by offenders is interchangeably referred to as internet crime, computer misuse, computer-related crime, high-technology crime, or electronic crime.

The Association of Chief Police Officers (ACPO) defines it as “the use of computers or internet technologies to commit or facilitate the commission of a crime.” On the other hand, the Australian Institute of Criminology (AIC) defines cybercrime more broadly as “a general term for offenses committed using electronic data storage devices or communication technologies.” (Brown, 2015, p.57).

From a legal perspective, Algerian law refers to cybercrimes as offenses related to information and communication technologies. According to Article 2 of Law No. 09-04 of August 5, 2009, these are crimes involving attacks on automated data processing systems, as specified in the Penal Code, as well as any other crime committed or facilitated through an information system or electronic communication network (Law No. 09-04, 2009, p.5).

In broader terms, cybercrime can be defined as any form of deliberate and unlawful behavior committed through the use of computers connected to the internet, targeting the system itself, its contents, or its operations — with the intent to harm the victim, gain profit, or achieve other objectives — by individuals possessing extensive knowledge of information technology and its intricacies.

1.3 Categories of Cybercrime:

Legal scholars have not reached a unified standard for classifying cybercrimes, largely due to their complexity, diversity, and rapid evolution. Some classify them based on the means used to commit the crime, others by the motive of the offender, or by the target of the attack. On this basis, cybercrimes can generally be classified as follows: (Saghir, 2013, pp.43–58)

1.3.1 Crimes Against Property:

With the shift from traditional commercial transactions to electronic commerce, and the accompanying evolution of digital payment and transfer systems, online financial interactions have become increasingly vulnerable to various forms of crime. This includes online fraud, identity theft, unauthorized access to bank accounts, and manipulation of digital financial data.

1.3.2 Crimes Against Individuals:

As the internet continues to expand, personal information about individuals has become widely accessible and shared across digital platforms. This exposure has made such data a target for cybercriminals, leading to privacy violations, defamation, and digital harassment that can severely harm a person's reputation and well-being.

1.3.3 Crimes Against State Security:

Among the most serious forms of cybercrime are those that threaten national security, including:

Terrorist Activities:

Many extremist groups have exploited the communicative nature of the internet to spread their ideologies and recruit followers. In some cases, these activities extend to direct threats against the security and stability of targeted states.

Organized Crime:

Transnational criminal organizations have taken advantage of digital communication and internet technologies to plan, coordinate, and execute illegal operations with efficiency and discretion, transcending geographical boundaries.

Crimes Against Intellectual Security:

This category includes efforts to undermine the cultural and ideological foundations of societies. The internet offers vast opportunities to influence beliefs, values, and traditions, which can lead to ideological destabilization and social unrest.

Cyber Espionage:

The internet has made espionage activities significantly easier. Cybercriminals and state actors alike engage in spying on individuals, governments, and institutions, whether domestic or international. In the information age, cyber espionage typically targets three main domains: military, political, and economic intelligence.

In a broader classification, the manifestations of **cybercrime** can be outlined as follows:

1. **Data sabotage and misuse:**

This includes damaging or manipulating databases and digital libraries, corrupting records, or distorting official information.

2. **Information theft:**

Refers to stealing or selling valuable information such as research papers, technological, industrial, or military studies — or destroying such data.

3. **Data falsification:**

Involves unauthorized access to educational systems or databases to alter or manipulate information, such as changing students' grades.

4. **Information forgery:**

Entails creating or modifying data to produce false records, such as issuing counterfeit certificates that were never officially granted.

5. **Privacy violation:**

Includes publishing or leaking personal information, hacking into private accounts, or exposing individuals' personal histories without consent.

6. **Eavesdropping:**

Involves infiltrating databases or intercepting telephone communications to steal conversations or audio data.

7. **Espionage:**

Refers to intercepting information or monitoring individuals' activities for intelligence or malicious purposes.

8. **Defamation:**

The deliberate use of private or sensitive information — especially data linked to misconduct or crime — to damage a person's reputation or assassinate their character.

9. **Academic theft:**

Involves stealing intellectual works such as books, academic research, or scientific studies, particularly those of experimental or applied nature.

10. **Patent theft:**

The stealing or unauthorized use of **scientific or technical inventions**, often to sell or exploit them for personal gain.

11. **Unauthorized network access:**

Gaining illegal entry into networks with the intent to misuse them, sabotage data, spy, or obtain illegal benefits.

12. Software piracy:

Involves illegally copying, using, or reselling software without authorization.

13. Data and information piracy:

The interception or hijacking of data for profit, particularly credit card numbers, account details, login credentials, and passwords.

14. Child exploitation:

The distribution of child pornography or “child sex tourism” content — particularly targeting minors and females — as well as simulated sexual material online.

15. Number theft and trafficking:

Involves stealing and trading confidential numbers, such as secret phone codes or credit card numbers, and using them for illicit international calls or transactions.

16. Sexual harassment:

Refers to unwanted advances or harassment — by men or women — through emails, messages, or online chats.

17. Email bombing (malware attacks):

Sending viruses or malicious files via email to destroy data or disrupt systems.

18. Disclosure of secrets:

Obtaining and publishing highly confidential information over the internet without authorization.

19. Financial fraud using cards:

The illegal use of shopping, financial, or phone cards to conduct unauthorized transactions or purchases.

20. Stalking, harassment, and extortion:

The act of persistently pursuing or blackmailing individuals — often to force a personal relationship — using emails or digital messages.

21. Cyberterrorism:

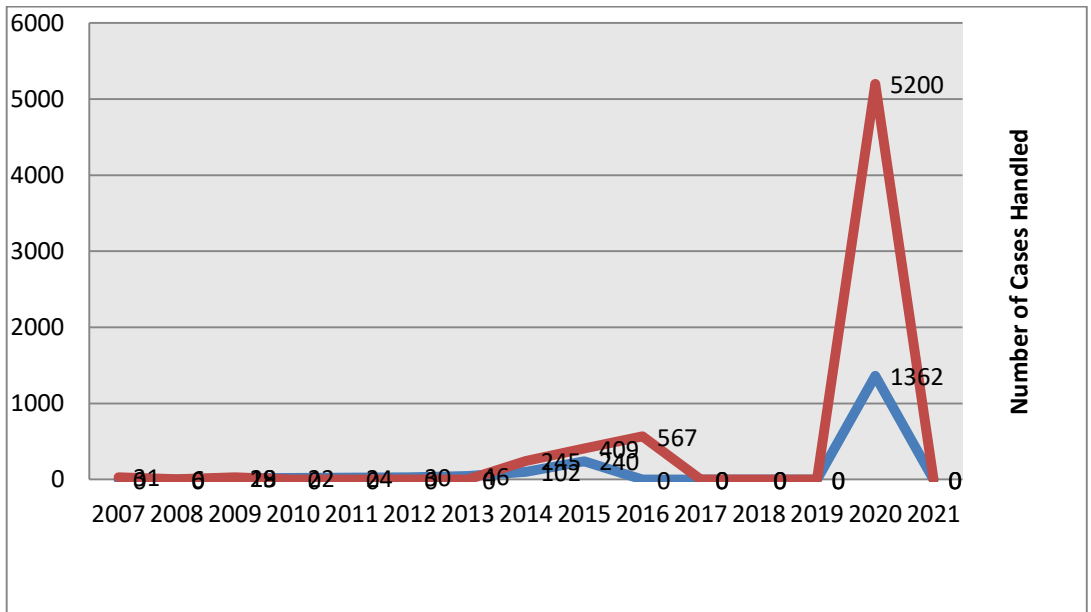
Encompasses all the above elements within a dynamic technological environment. Changes in digital tools and networks have altered the **methods, weapons, and objectives** of terrorist activities, giving rise to what is now known as **cyberterrorism**. (*Israel Jibreel, 2016*)

1.4 The Reality of Cybercrime in Algeria:

Algeria's experience with cybercrime began before 2008, albeit on a relatively limited scale. Early forms of cybercrime were mostly confined to illegal disk copying and similar acts that rarely required security intervention. However, with Algeria's entry into the era of high-speed internet through ADSL connections—and the steady annual increase in subscribers, which reached 26.35 million users on social media platforms by 2021, according to the latest DataReportal statistics—this digital transformation inevitably brought with it a set of challenges and negative consequences.

The following graph illustrates the evolution of recorded cybercrime rates in Algeria over time, highlighting their progression in relation to the chronological sequence.

Figure 01: Cybercrime Cases Handled by Security Authorities Over the Past 15 Years



Sources: (Hamlaoui & Al-Muqaddam Ezzedine, 2015); (Bachouch, 2021)

2. Cybersecurity

2.1 Definition of Cybersecurity:

According to Martti Lehto and Pekka Neittaanmäki, cybersecurity is defined as “a set of measures taken to defend against computer hacker attacks

and their consequences, including the implementation of necessary countermeasures.”

This view is supported by one of the most prominent experts in the field, Edward Amoroso, who defines cybersecurity as “the means by which the risk of attacks on software, computer systems, or networks can be reduced. These means include tools for countering hacking, detecting and stopping viruses, providing encrypted communications, and more.”

The International Telecommunication Union (ITU), in its report “Trends in Telecommunication Reform 2010–2011”, offered a definition that has since become a reference point for both academic and professional circles. It describes cybersecurity as “a collection of tools, policies, security safeguards, guidelines, risk management approaches, training, best practices, and technologies that can be used to protect the cyber environment and the assets of organizations and users.”

Based on these perspectives, a comprehensive definition can be proposed: Cybersecurity (or information security) encompasses all laws, tools, frameworks, security mechanisms, risk management methods, and technical practices related to information and communication technologies (ICTs) aimed at protecting the interests of both states and individuals. Ultimately, its core objective is to ensure the ability to resist deliberate cyber threats—such as hacker attacks—or unintentional threats stemming from human error, allowing systems to recover and mitigate the damage caused by the disruption or misuse of ICTs. (Jamal, 2019, p.1265)

2.2 Cybersecurity in Algeria:

Algeria, like many other nations, has placed cybersecurity among its top national priorities, updating its security policies and adopting new mechanisms to address emerging cyber threats. These efforts have gone hand in hand with the development of digital infrastructure and the modernization of ICT systems.

However, as cybersecurity measures intensify, so do concerns over potential risks to individual freedoms resulting from expanded monitoring systems. Today, cybersecurity represents a fundamental pillar of Algeria’s

modern security doctrine, requiring the involvement of national defense institutions, security agencies, and legislative authorities alike.

The Algerian legal framework has evolved to confront these new forms of crime, and recent statistics reveal a steady increase in cybercrime across the country. Consequently, Algerian authorities are compelled to adopt strong preventive security measures to reduce the risks and impact of such offenses. (Idris, 2019, p.112)

2.3 Cybersecurity Challenges in Algeria:

Both the National Gendarmerie and the National Security Directorate face numerous obstacles in their efforts to ensure effective cybersecurity. The most significant challenges include:

- **The growing number of internet users (over 10 million subscribers in Algeria):**

As internet use expands, the associated risks also rise. Identifying the perpetrators of cybercrimes becomes increasingly difficult due to the enormous and ever-growing user base, making investigation and digital tracking more complex.

- **Technological advancement and the rise of wireless internet (Wi-Fi/3G/4G):**

With these technologies, cybercriminals no longer need to sit behind a wired computer to carry out attacks. This evolution demands that security agencies enhance their technological capabilities and stay prepared with advanced tools to confront emerging threats.

- **The widespread use of social media platforms:**

The number of social media users in Algeria exceeds seven million, a phenomenon that has contributed to a noticeable rise in various types of cyber offenses such as defamation, sexual harassment, and the exploitation of minors. This situation calls for the development of well-structured national strategies to ensure cybersecurity within social media environments.

- **The Spread of High-Speed Internet Technologies (ADSL / VSAT / SDSL):**

Advanced technology contributes to the rapid execution of cybercrimes, placing specialized security agencies under the challenge of launching prompt investigations and tracking down offenders. This demands the use of sophisticated equipment and modern, high-performance software tools.

•Concealment During the Use of Internet Services (Proxy):

This represents one of the most significant challenges faced by investigative authorities. It requires collaboration among multiple entities and the adoption of advanced tools capable of detecting details, decrypting codes, and continuously updating and developing information infrastructure, along with designing highly advanced software systems.

•Lack of Coordination Among Countries and Governments:

It is well known that cybercrime transcends borders and continents. Offenders can infiltrate computer systems in one country, manipulate or breach data in another, and even store electronic evidence on servers located in a third country. This enables cybercriminals to conceal their identities and move materials through channels distributed across different regions. As criminals can electronically migrate from one network to another and access databases across various continents, several jurisdictions, courts, and legal systems become simultaneously involved — creating a serious challenge. Therefore, the effective combat of cybercrime requires increased, swift, and well-coordinated international cooperation at the highest levels.

•Technological Developments in the Field of Internet and Communications:

Such progress compels specialized security bodies to keep pace — both by acquiring and mastering advanced technologies and by leveraging them effectively. However, this often strains limited budgets, making it necessary to provide sufficient financial, material, and human resources to ensure robust cybersecurity capabilities.

•Raising Awareness of the Concept of Cybersecurity Among Internet Users:

It is essential to conduct awareness campaigns among internet users to help them adopt basic safety measures, learn about encryption mechanisms, and take appropriate precautions when using social media platforms. Users should also be encouraged to embrace a culture of timely reporting so that relevant authorities can act swiftly and identify offenders before further harm occurs.

•Enforcing Laws Strictly and Effectively:

One of the key factors contributing to the spread of cybercrime is impunity and delays in law enforcement, which allow criminals to repeat their offenses. Therefore, it is crucial to ensure the strict application of laws and to adapt legal provisions to the evolving nature of cyber threats. Additionally, the establishment of specialized cybercrime courts has become increasingly necessary due to the widespread and complex nature of these offenses.

(Samir, 2017, p.275)

3. Security Institutions Dedicated to Combating Cybercrime

The quantitative scope of cybercrime in Algeria remains unclear due to the lack of research and studies capable of revealing concrete data and indicators about the financial and institutional losses caused by this type of crime. Nevertheless, Algeria is by no means immune to the dangers of cybercrime, given its integration within the global digital space—particularly in the context of financial computing systems and government institutions, whose websites have been targeted and compromised by cyberattacks.

3.1 The Center for the Prevention of Cybercrime of the National Gendarmerie (CPLCIC)

Established in 2008, this center is the only specialized body in Algeria dedicated to addressing cybercrime. Its primary mission is to ensure the

security of the information systems of public safety institutions. Headquartered in Bir Mourad Raïs, it also serves as a documentation and analytical hub, responsible for examining data related to cyber offenses, identifying perpetrators—whether individuals or organized groups—and safeguarding sensitive digital infrastructures, particularly those belonging to official institutions and banks. (Kheira, 2010, p. 78)

The center collaborates closely with other security agencies to combat cybercrime by developing advanced methods for handling such offenses and proposing legal frameworks for the management of digital information. It coordinates with the Ministry of Justice and with criminology institutes to enhance the overall understanding of crime and, more specifically, cybercrime. Algeria has also sought to benefit from international expertise to strengthen its cyber defense mechanisms through several key strategies:

Prevention: This includes public awareness campaigns in cooperation with the Ministry of National Solidarity and Family, as well as organizing conferences, seminars, international forums, and media programs aimed at educating the public.

Combat: Algerian citizens are encouraged to use social media responsibly and to report suspicious or harmful online activities. Such civic engagement assists the Gendarmerie in identifying, investigating, and apprehending offenders more efficiently.

3.2 The National Institute of Forensic Evidence and Criminology of the National Gendarmerie (INCC)

The INCC is a public administrative institution under the direct supervision of the Minister of National Defense, tasked with performing expert analyses and examinations in the context of preliminary investigations and judicial inquiries. It also provides scientific support during complex investigations.

Located in Bouchaoui, the Institute was established by Presidential Decree No. 133/04 dated June 26, 2004, and became operational on January 1, 2009. The interim period (2004–2009) was devoted to training personnel and acquiring advanced scientific and technical equipment.

The INCC fulfills numerous functions, including responding to requests from judicial authorities, criminal investigation officers, and other competent institutions, particularly when handling complex cases. It also organizes advanced training programs in forensic and criminal sciences.

To effectively carry out its mission, the INCC comprises multiple specialized departments—such as Fingerprint Analysis, Environmental Studies, and most importantly, the Information Technology Division, which focuses on monitoring, tracing, and analyzing cases of hacking and cyber intrusions, as well as identifying stolen data and dismantling malicious software. (Adel, 2014, p. 64)

3.3 The Central Service for Combating Cybercrime under the Directorate of National Security (SCLC)

In response to growing cybersecurity concerns and the proliferation of digital threats, Algeria's National Security Directorate established the Central Service for Combating Cybercrime (SCLC). Initially formed as a small specialized unit within the Criminal Police Directorate, this entity evolved into a full-fledged national division dedicated to fighting cybercrime.

The foundation of this specialized structure dates back to 2011, when the General Directorate of National Security recognized the need for a focused institutional response to emerging cyber threats. By January 2015, the Central Service for the Fight Against Crimes Related to Information and Communication Technologies was officially added to the organizational framework of the Criminal Police Directorate by decree of the Director General of National Security. (Idriss, 2019, p. 114)

3.4 The National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies

This authority was established under Presidential Decree No. 261-15 as an independent administrative body under the supervision of the Minister of Justice. It operates under the guidance and oversight of a steering committee chaired by the Minister of Justice, comprising primarily government

members concerned with the issue, heads of security services, and two judges from the Supreme Court appointed by the High Council of the Judiciary.

The Authority is tasked with proposing elements of a national strategy for the prevention and combatting of crimes related to information and communication technologies, as well as coordinating and activating prevention operations. It also assists judicial and law enforcement authorities in the fight against such crimes by collecting and providing information, conducting forensic analyses, and ensuring preventive monitoring of electronic communications to detect crimes associated with terrorism, sabotage, or threats to state security.

The establishment of this body was previously outlined in Article 13 of Law No. 09/04 of August 2009, which defines specific measures for the prevention and combatting of ICT-related crimes. The law states: “A national authority shall be established; its organization and operation shall be determined by regulation.” Article 14 of the same law further clarifies its missions as follows: (Osama, Yassine & Issam, 2013, p.4)

3.4.1 Prevention of ICT-Related Crimes:

Preventive measures include raising awareness among ICT users about the dangers of cybercrimes they might fall victim to while browsing or using these technologies. Common examples include: espionage on communications and emails, tampering with customer accounts, and hacking into the systems of major corporations, institutions, or government agencies.

3.4.2 Combating ICT-Related Crimes:

-According to Article 14 of Law No. 09/04, the Authority’s combat operations include two main areas:

-Assisting judicial and law enforcement authorities in their investigations of ICT-related crimes, including data collection and conducting forensic analyses (Article 14, paragraph b).

-Exchanging information with foreign counterparts to gather useful intelligence for identifying and combating perpetrators of ICT-related crimes.

-The project also proposes the creation of a specialized national body responsible for coordinating and activating prevention efforts, assisting the judiciary and police in investigations, and exchanging information with

similar foreign institutions to effectively combat this complex and dangerous form of criminal activity.

3.5 The Cyber Defense and Systems Security Monitoring Department

Given the sensitivity of the national defense sector, the Cyber Defense and Systems Security Monitoring Department was established on November 6, 2015, within the Directorate of Employment and Preparation of the Staff of the People's National Army. Its mission is to protect the nation's vital systems and infrastructure from all forms of cybercrime. The department's operational framework focuses on several key aspects (Jamal, 2019, p.1289):

- Directing, implementing, and supervising activities in this field strictly within the functional and organizational framework.
- Developing and strengthening the legal framework to prevent misuse of technology and ensure the protection of information systems.
- Promoting technical and scientific training to build expertise and skills capable of establishing cyber defense systems across all military operations, thereby reducing criminal risks.
- Instilling a culture of responsible use of information and communication technologies through awareness campaigns targeting all personnel, regardless of rank or position.
- Continuously investing in scientific research to improve defense mechanisms in response to technological advancements.
- Promoting international cooperation with foreign military institutions experienced in cyber defense to exchange expertise and benefit from their knowledge in this field.
- Moreover, several ministries—such as those of Post and Telecommunications, Finance, Higher Education, and Interior—have issued directives and guidelines to their executive departments detailing the practical mechanisms necessary to prevent operational errors. These include:
 - Prohibiting unauthorized access to information systems connected to the internet, unless approved by a legally competent authority, and forbidding the use or exchange of personal accounts or passwords.

- Adhering to established standards for encrypted data transmission—both internal and external—to ensure information security.
- Following internationally recognized scientific and professional protocols when using ICTs for personal or professional purposes, to avoid system vulnerabilities and ensure equitable access to technological services.

In conclusion, while Algeria has made significant efforts to strengthen its cyber defense and develop institutions dedicated to the prevention and combatting of ICT-related crimes, these administrative measures remain insufficient. Achieving effective cybersecurity requires sustained commitment, continuous improvement, and long-term strategic coordination among all relevant actors.

3.6 The National Criminal Division for Combating Crimes Related to Information and Communication Technologies

Article 211 bis 22 establishes, within the court of the Algiers Judicial Council, a National Criminal Division specialized in the prosecution and investigation of crimes related to information and communication technologies (ICT), as well as associated offenses. This division also holds jurisdiction to adjudicate such crimes when they constitute misdemeanors. Under this law, crimes related to information and communication technologies refer to any offense committed through, or facilitated by, the use of an information system, an electronic communications network, or any other tool or mechanism linked to ICT.

Article 211 bis 23 states that the Public Prosecutor of the National Criminal Division for Combating ICT-Related Crimes, along with the Investigating Judge and the President of the Division, exercise their powers throughout the entire national territory.

Article 211 bis 24 provides that, without prejudice to paragraph 2 of Article 211 bis 22 above, the Public Prosecutor, Investigating Judge, and President of this Division hold exclusive authority to prosecute, investigate, and adjudicate the following ICT-related crimes and their associated offenses:

- Crimes that threaten the security of the State or national defense;

- Crimes involving the dissemination or promotion of false information among the public that could endanger public security, peace, or societal stability;
- Crimes involving the spread of malicious or destabilizing information that disrupts public order or security, particularly those with an organized or cross-border nature;
- Crimes targeting automated data processing systems belonging to public administrations or institutions;
- Crimes of human trafficking, organ trafficking, or migrant smuggling;
- Crimes of discrimination and hate speech.
- (Official Gazette of the Algerian Republic, 2021, pp. 8–9)

Conclusion

Algeria is making significant efforts to strengthen its cybersecurity framework by keeping pace with rapid digital transformations. Through international and regional agreements, it contributes to aligning and coordinating both global and national strategies to contain cyber threats at all levels. The country continues to modernize and create specialized branches and institutions under the authority of security services, the Ministry of Defense, and the judicial system, all dedicated to cybersecurity.

However, despite these commendable efforts, cybercrime remains a borderless and rapidly evolving threat, deeply intertwined with various digital domains and transactions. This reality places nations in a defensive position and significantly heightens the challenges of cybersecurity.

References

1. Maâchi, Samira. (April 2010). *The Nature of Cybercrime*. Legal Forum Journal, 07, pp. 275–285.
2. Al-Salek, Farid Kamel. (2000). *Cybercrime*. In *Symposium on Development and the Information Society* (pp. 1–9). Syria: Syrian Informatics Society Conference, Aleppo.
3. Rachad, Marai & Israel, Jibril. (August 9, 2016). *Cybercrimes: Objectives – Causes – Methods and Solutions*. Retrieved from the Arab Democratic Center: <https://democraticac.de/?p=35426>
4. Brown, C. (2015, January–June). *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*. *International Journal of Cyber Criminology*, 9(1), pp. 55–119. doi:10.5281
5. Law No. 09-04 (dated August 5, 2009). *Law on the Specific Rules for the Prevention and Combating of Crimes Related to Information and Communication Technologies*. Algeria: Official Gazette, No. 47.
6. Youssef, Saghir. (2013). *Crimes Committed via the Internet*. Master's Thesis in Law. Tizi Ouzou: Faculty of Law and Political Science, Mouloud Mammeri University.
7. Hamlaoui, Abdelrahman (National Security), & Lieutenant-Colonel Azzedine (National Gendarmerie). (2015). *The Legal Framework for the Prevention and Combating of Cybercrime: The Role of the General Directorate of National Security*. National Symposium: *Cybercrime Between Prevention and Control*. Mohamed Khider University of Biskra.
8. Bashoush, Nawara. (November 23, 2021). *Cybercrime... Terrifying Numbers*. Retrieved February 19, 2022, from *Echorouk Online*: shorturl.at/hqrR8
9. Bouzadia, Djamel. (April 2019). *Algeria's Strategy for Combating Cybercrime: Challenges and Future Prospects*. *Journal of Legal and Political Sciences*, 10(1), pp. 1262–1293.
10. Atia, Idris. (2019). *The Role of Cybersecurity within Algeria's National Security Framework*. *Misdakiya Journal*, No. 1, pp. 100–121.
11. Bara, Samir. (July 2017). *Cybersecurity in Algeria: Policies and Institutions*. *Algerian Journal of Human Security*, 4, pp. 255–280.
12. Rouabhi, Khira. (2010). *Internet Culture: A Field Study on Network Usage in the City of Tiaret*. Oran: University of Oran, Faculty of Humanities and Islamic Civilization.

13. Aloui, Hind. (2008). *Measuring Access to Information and Communication Technology in the Education Sector of Eastern Algeria*. Doctoral Dissertation. Constantine: Mentouri University, Faculty of Humanities.
14. Ghazal, Adel. (March 2014). *E-Government Projects from Strategy to Implementation: The Algerian E-Government 2013 Project as a Model*. *Libraries and Information Journal*, p. 34.
15. Ben Seddik Tayeb Osama, Fatni Yassine, & Ben Yahia Filali Issam. (2013). *E-Government: Toward a Knowledge Society*. Institute for Research and Consulting, p. 9.
16. *Official Gazette of the People's Democratic Republic of Algeria*. (August 26, 2021). *Ordinance No. 21-11 of Muharram 16, 1443 (August 25, 2021), Supplementing Ordinance No. 66-155 of Safar 18, 1386 (June 8, 1966), Containing the Code of Criminal Procedure*. No. 65, pp. 7–9.