

Algeria's cybersecurity strategy:
Defensive Techniques and Preventive Measures to Counter Cyber
Threats

Sehailia Samah¹

¹Echahid Cheikh Larbi Tebessi University Tebessa, samah.sehailia@univ-tebessa.dz

Received: 25/01/2025

Accepted: 27/03/2025

Published: 15/04/2025

Abstract:

Algeria's cybersecurity policy is an essential part of the national strategy to preserve national security, protect digital infrastructure, and ensure the safety of sensitive information and data from increasing cyber threats in cyberspace. Through its strategy, Algeria is seeking to take a set of defensive and preventive measures and mechanisms to build national capabilities in the field of cybersecurity, including specialized agencies and bodies to monitor cybersecurity, the legal framework to ensure the security of the information system permanently and continuously, as well as strengthening international cooperation and raising public awareness of the importance of cybersecurity in Algeria.

The study found that strengthening cybersecurity in Algeria requires the development of a legal and regulatory framework that guarantees strict penalties against cybercrimes, which encourages compliance with laws and enhances data protection and digital infrastructure protection, and requires effective and comprehensive strategies to address cyber threats, in addition to strengthening international cooperation and exchanging expertise more effectively to ensure the stability of the digital system in Algeria

Keywords: Strategy, cybersecurity, Algeria, cyber threats, digital space.

1. INTRODUCTION

Cyber threats are one of the biggest threats to the national security of countries at present, as they directly affect their political, economic, and social stability. These threats range from cyber-attacks targeting critical infrastructure to attempts to hack government and personal data.

In an era of increasing reliance on technology and the technological revolution, cybersecurity has become an urgent necessity to protect systems, networks, programs, and data connected to the Internet from digital attacks. This includes a set of technologies, policies, and practices that aim to ensure the protection and security of a country's cyber infrastructure and address cyber threats.

In this context, Algeria is seeking to combat cyber threats by strengthening its cybersecurity through the development of several legislations and a legal mechanism, which is considered one of the most important strategies that Algeria undertakes to protect its national security and national interests in cyberspace.

This topic derives its importance from the fact that cybersecurity is considered a new dimension of the new security research agenda in political science and international relations, and an essential part of national security, as it aims to protect national interests from threats that may arise in cyberspace. The importance of this topic is also evident in the urgent need to secure cyberspace, especially in light of the rapid digital transformations that Algeria is witnessing.

This study aims to identify the nature of the cyber threats facing Algerian national security, in addition to analyzing the Algerian defense and preventive strategy to protect its cyberspace and address these threats in light of the increasing technological challenges.

Research Question:

Based on the above, this study attempts to address the following the research question:

What are the most important defensive and preventive strategies to combat cyber threats and enhance cybersecurity in Algeria?

Sub-questions arise from this question, including the following:

- What is cybersecurity, and what are its strategic dimensions?
- What are the types of cyber threats?
- How do cyber threats affect national security?
- What are the mechanisms adopted by Algeria to confront cyber threats?

In order to answer this question, the following axes will be adopted:

- **First:** A conceptual framework for the study
- **Second:** The impact of cyber threats on national security
- **Third:** Defense techniques to confront cyber threats in Algeria
- **Fourth:** Preventive mechanisms against cyber threats in Algeria

Research methodology: Due to the nature of the topic and to answer the research question, we will rely on the descriptive and analytical method that suits the nature of the study by highlighting the concept of cybersecurity and cyber threats and identifying their nature that poses a threat to Algerian national security, as well as analyzing the strategic dimensions of the Algerian security system.

First: A conceptual framework for the study

1. Cybersecurity:

Definition of Cybersecurity:

Richard A. Kemmerer defines cybersecurity as: “Defensive means that will detect and thwart attempts by hackers,” while Edward Amorso defined it as: “Means that will reduce the risk of attack on software, computers, or networks and include those means and tools used to confront hacking, detect viruses, and stop them.”¹

The US Department of Defense (Pentagon) also provided a precise definition of the term cybersecurity, considering it all organizational measures necessary to ensure the protection of information in all its physical and electronic forms from various crimes, attacks, sabotage, espionage and accidents²

Cybersecurity is defined as:” A set of technical and technological means and processes that are used to protect networks, devices, software and data from unauthorized attacks or intrusion. Information technology security or

information protection” and is also defined as:” The activity that provides protection that ensures the protection of human and financial resources associated with communication technologies and limits the damage in the event of cyber-attacks or threats and restores the situation to what it was as soon as possible One of the most important goals achieved by cybersecurity is to maintain the security and stability of society Maintaining the integrity of the work of the state's electronic sectors from any penetration Saving important electronic data and information Protecting the information network in a scientific and technical manner Encrypting electronic transactions so that no hacker can access them, and encryption is one of the most important protection methods”, so cybersecurity in all its technical details³

It can be said that cybersecurity is a set of mechanisms, procedures and means that aim to protect software and computers from various attacks, breaches and cyber threats that may threaten the national security of countries.

Cybersecurity is a set of practices and techniques that aim to protect systems, networks, and data from digital attacks. This includes protecting sensitive information from unauthorized access, ensuring data integrity, and maintaining the confidentiality of information. Cybersecurity also includes protecting critical technological infrastructure.

Strategic dimensions of cybersecurity:

- **The military dimension**

The military dimension and the need to strengthen the electronic security system by linking military units to each other through the virtual world, which facilitates the exchange of information, which reflects positively on achieving military objectives and protecting the defensive and even offensive capabilities of the state and technology, for which the electronic units are working by relying on high technicians with high training in informatics, thus linking the military force to technological development is very important, but the most important is the protection mechanisms and digital support to secure this development.⁴

• **The political dimension:**

The political sphere was also not spared from cyber threats and attacks, which reached the extent of cyber wars, the cyber arms race and the exchange of piracy in sensitive files and issues. The reliance on cyberspace has revolutionized the concepts of political science, cyber powers and cyber deterrence, as well as the impact of espionage between countries that have become more dependent on piracy. Hacking is the most important state for espionage and generally these countries access information through digital gaps that governments and companies want to protect in addition to the hacking process, actors try to influence world opinion by publishing false news and in some cases actors try to influence world opinion by spreading fake news, and in some cases, government hacks occur in parallel with propaganda campaigns.⁵

• **The economic dimension:**

The economic dimension and the trend towards the digital economy has become Algeria's bet, and major economic companies and security and military institutions are working to develop their scientific capabilities in order to avoid any penetration attempts, especially in light of Algeria's regional conflicts, and this is what makes Algeria focus and pay great attention to maintaining electronic and digital security and this crime often comes from countries that disagree with Algeria in its political orientation and at the level of the stock exchange and financial trades through the protection of the business number that Algeria has, making the latter closely linked to cyber security in the first degree and the economy after it, which is closely linked to security in the first degree and the economy after it. There is a clear link between the knowledge economy and the expansion of the use of ICTs, which allows to promote the economic development of many countries by benefiting from the utilization opportunities offered by international companies and large companies looking to manage the cost of their production in the best conditions.⁶

• **The social dimension:**

The social dimension and securing social media platforms from external risks Social media pages have contributed to creating an unusual

and unprecedented communication space, which made the shares of hackers rise by searching for them and using them to create programs against bodies and institutions and opening the door to virtual wars between human groups within the state, especially countries that carry contradictory ideologies, where the participation of all segments of society in these wars represents a threat to the public security of the state and an opportunity for these groups to gain access to different ideas and information.

Therefore, it is necessary to work to raise citizen awareness of these risks to achieve cybersecurity in its social dimension.⁷

• **The legal dimension:**

The legal dimension called for the need to legislate a law that protects individuals and society from cyber hacking, as well as keeping pace with the development of human society by protecting personal data and the right to create a blog and maintain intellectual property rights on the Internet, as well as the need to activate international cooperation to build legal frameworks and structures concerned with resolving international disputes at the level of cyberspace and monitoring and punishing violators of it.⁸

2. Cyber threats:

Definition of Cyber Threats:

Cyber threats refer to those attacks that are carried out using Internet mechanisms and networks and computers and aim to damage electronic devices and networks connected to the Internet and aim to undermine, demolish and bypass digital walls that perform a protective function as security barriers in front of cyber threats with the aim of stealing information and data, accessing them, sabotaging them or even changing their content, all with the aim of causing harm to the victim party, and all with the aim of inflicting damage to the victim.⁹

Cyber threats also refer to the possibility of a successful cyber-attack aimed at unauthorized access, damage, disruption, or theft of an IT asset, computer network, intellectual property, or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.¹⁰

Cyber threats typically arise when an individual or organization's data, computer system, network, or device is targeted by a cyber attacker who seeks to gain unauthorized access or exploit any vulnerabilities in the information system, compromising its confidentiality, integrity, or availability.¹¹

Cyber threats are a group of risks that target digital systems, networks, and information through the use of computing and communication technologies, and are represented by a variety of malicious activities aimed at compromising systems, stealing data, or damaging digital infrastructure. The threat includes 3 categories:¹²

- **The first category:** This is a set of threats to national security in the political, military, economic, social and vital fields of states, capital markets, banking sectors, nuclear facilities, health institutions and transportation sectors of all kinds by land, sea and air.

- **The second category:** This category concerns organizations. These threats aim to affect cyberspace, which has become a major component in the course of work of organizations, as they affect the way they work and threaten their continuity, by causing physical or functional damage to electronic devices, systems and structures, whether disrupting or penetrating them.

- **The third category:** It concerns the personal aspects of individuals such as theft, leakage and use of personal data without permission, theft of money, infringement of intellectual and industrial property, trademarks, fraud, spam, crimes against children, illegal content and other risks that are considered cyber-crimes that are directly related to people and their property, and the cyber threat is the attempt to inflict damage and harm, whether against people, organizations or countries through the use of various information and technological means in order to achieve certain goals that may be political, economic, military, ideological or religious.

Types of Cyber Threats:

There are a variety of types of cyber threats that pose a threat to computer systems and data:¹³

- Viruses and worms are malicious programs that replicate themselves and

spread within systems and networks and cause data corruption or disruption of systems

- Spyware is software used to collect personal or sensitive information without the consent of the owner of the device and send it to hackers or malicious parties.
- Physics programs are encryption programs that aim to encrypt files on the victim's device and demand a ransom in exchange for decrypting them.
- Network hacking Attacks aimed at penetrating computer networks to gain unauthorized access to data or systems Distributed denial of service attacks. Attacks aimed at increasing the traffic on web servers or networks enough to disrupt the service
- Exploiting security vulnerabilities in software or systems to gain unauthorized access to data or to carry out other attacks
- Cyber fraud using fake emails or websites to obtain personal or financial information from victims
- Illegal cryptocurrency mining, i.e. using computer resources without consent to illegally generate cryptocurrencies
- Targeted attacks targeting a specific organization or VIP in sophisticated and organized ways.

There are many forms of cyber threats of varying nature and sources around the world that are detrimental to the national interest, such as:

❖ **Cyber espionage:**

It is the illegal acquisition of confidential information with the aim of gaining an economic, strategic or military advantage, cyber espionage is espionage that relies on the use of technology. Electronic access to information and cyber espionage differ in terms of type, there is espionage by individuals, through wired networks or espionage through satellites.¹⁴

It refers to the use of computer and electronic technology to collect confidential or sensitive information in an illegal or unauthorized manner. Cyber espionage is usually conducted by a state or an interested party such as organized crime organizations or competitive companies with the aim of obtaining confidential, intelligence or commercial information The activities carried out in cyber espionage include the following:¹⁵

Algeria's cybersecurity strategy:
Defensive Techniques and Preventive Measures to Counter Cyber Threats

- Hacking networks and systems Exploiting network or system security vulnerabilities to gain access to confidential data
- Hacking email and social media accounts Using phishing or social engineering to gain access to sensitive information
- Eavesdropping on electronic communications Recording and monitoring conversations and electronic communications without the consent of the data subject
- Using spyware and remote-control programs Installing spyware on computers to steal information or control systems remotely
- Using targeted hacks: Attacks directed at specific targets such as government organizations or large corporations to steal their sensitive information
- The use of malware: the implementation of malicious software to steal information or spy on systems

Accordingly, cyber espionage refers to the use of digital technology to obtain confidential or sensitive information by infiltrating computer systems or networks. Hackers infiltrate cybersecurity systems to obtain commercial, political, military or personal information.

❖ **Cybercrime:**

Cybercrime is crimes committed against individuals. or groups of individuals with a criminal motive with the intent to damage the victim's reputation directly or indirectly using communication networks such as the Internet (e.g. chat rooms, email, mobile phone) and computer communications for personal purposes or financial gain or damage, including forms of identity-related crime, and acts related to computer contents, all occur within the broader meaning of the term cybercrime.¹⁶

Cybercrime is a range of criminal activities practiced online or using digital technology, and includes acts such as hacking, e-fraud, the use of malware, and identity theft. These crimes include unauthorized access to systems, deceiving individuals to obtain their personal or financial information, and damaging data.

❖ **Cyberterrorism:**

It is the use of digital technology and the Internet to carry out terrorist activities or promote terrorist goals. This includes the use of the Internet for recruitment, training, guidance and communication between terrorist groups, in addition to carrying out cyber-attacks against civilian, military or governmental targets:¹⁷

- Recruitment and promotion using the Internet and social media to recruit individuals to terrorist organizations, promote terrorist ideas and encourage violent acts
- Training and mentoring Providing technical support and intellectual guidance to potential perpetrators of online terrorist attacks
- Cyberattacks Using cyberattacks to disrupt the critical infrastructure of governmental or corporate organizations or the critical infrastructure of the state
- Cyber threats to use online threats to intimidate and affect public safety and security
- Promoting terrorist ideas to use the Internet to spread terrorist ideas and promote violent extremism and extremist ideologies.

Thus, cyber terrorism is the use of digital technology and electronic means to carry out terrorist acts aimed at creating chaos, terror, and terror, including attacks on information networks, government systems, critical infrastructure, or even individuals through the Internet.

❖ **Cyber warfare:**

The concept of cyber warfare is mainly based on hacking the websites of countries in the world or information systems, especially those related to strategic sectors such as defense, energy, and communications, with the aim of either spying on them, disrupting their services, or stealing their information.¹⁸

Cyber wars differ in terms of their nature because the conflict within cyberspace does not guarantee the expected and planned results, as they are wars that threaten and target public order and security directly through attempts to disrupt information systems related to the vital issues of the targeted state, as they are dynamic and permanent because they are hidden,

as states under them and their military leadership are either in a state of permanent attack or defense, and they are characterized by their operational nature by the blurred line between war and politics and between combatants and civilians, the absence of a hierarchy of commands, nor are they based on a national command aimed at gathering intelligence.¹⁹

Thus, cyber warfare refers to conflicts that occur in cyberspace, where technology and the Internet are used as a means of attack and defense. This war includes a range of activities such as network attacks, data theft, systems sabotage, and digital propaganda.

Second: The impact of cyber threats on Algeria's national security:

1. The relationship of cybersecurity to national security:

The emergence of cyberspace has made the defense capacity of any country insufficient to protect its national security, and its association with multiple concepts such as espionage, cyber terrorism and cyber warfare has made it a priority on its information block and away from the circle of cyber conflict that threatens its national information. The relationship between cybersecurity and national security increases its importance the more reliance on cyberspace in the transfer and preservation of any information content in military, security, economic, social and technical matters and making the vital infrastructure that is linked to national interests based on a single working environment, , in which any attack would cause imbalance and a serious threat to national security, in addition to the expansion of the circle of users of this space, which helps some actors to exploit loopholes, spread rumors, and call for provocative acts that would lead to the erosion of the state's sovereignty.²⁰

The concept of international conflict in cyberspace has been transformed through the impact of advanced digital technology remarkably on the uses of the concept of traditional force in various international conflicts, especially in the field of cyber wars, as many countries seek to enter the field of race and competition in the possession of cyber power through cyberspace and use it as a tool for international industries and achieve various gains and victories at the political or economic and military level using this advanced digital technology, and thus international actors

have moved from the level of classic wars and security threats to the level of wars and threats of a different kind, which are cyber wars and threats. Among the results are the following: ²¹

✓ The international cyber conflict is one of the aspects of the traditional conflict that threatens international security and the security of a single state, which can cause great losses to it and paralyze the information, communication and digital infrastructure of the target state by possessing those technological and cyber capabilities such as spyware and viruses.

✓ The new concept of national security, unlike the traditional concept, aims to preserve the safety of the state and individuals in light of these rapid and sophisticated technological and digital developments, and thus the mechanisms for dealing with them have differed, and security has become a reflection of the historical path that has known an upward development, which was reflected in the nature of the current international conflict with the new information wave witnessed by the world, which was affected by information technology and cyberspace, which changed the nature of traditional conflict and power and its exercise at the international level, thus bringing a number of changes within the security environment of the current international system.

✓ The current international conflict tends to compete in the arena of economic achievements, commercial successes, increasing exports, possessing diverse ideas and innovations, and conquering global markets, all through the acquisition of information, data and secrets by using the cyber power that some countries possess to penetrate those economic, technical, scientific and commercial secrets of other countries in order to achieve development and raise their economic growth rates.

✓ The emergence of new international terrorism that employs communication and information technology is considered one of the most serious new security threats that threaten the security of states and societies alike and is completely different from traditional terrorism through its characteristics, effects, nature, parties, the possibility of using cyber power as a direct threat and the excessive use of all advanced programs in cyberspace and their use in all its sensitive activities that threaten

international and global security, such as nuclear, biological and chemical terrorism.

2. The cybersecurity environment in Algeria:

During the period from January 1, **2023**, to December 31 of the same year, the Central Office for Combating Cybercrime recorded **5136** cases related to information and communication technology, involving **6146** individuals. In this regard, thanks to the vigilance and expertise of its engineers, the office was able to decipher several national and international cases. For example, specialists from the Central Office for Combating Cybercrime were able to detect and repel a serious cyberattack that affected the personal lives of individuals and institutions by targeting computers to steal personal data stored on them. As part of implementing the directives of the National Security High Command aimed at intensifying efforts among police services, the Central Office for Combating Cybercrime, in coordination with the operational services of the Algiers Security Department, provided technical support. This support directly contributed to the dismantling of an organized criminal network active in the field of drugs, where approximately 1 million hallucinogenic pills were seized. At the international level, and within the framework of combating all forms of violence against children, a specific case was addressed following the monitoring of electronic accounts whose owners publish pornographic videos and photos of children.²²

The Central Office for Combating Cybercrime has monitored several groups active on the Viber application, with members of

different nationalities producing, possessing and disseminating pornographic videos and images of children. The number of involved accounts was estimated at **79**, belonging to foreign countries, including **7** from within the national territory. After retrieving the necessary technical data, the countries in which the involved individuals reside were contacted to take appropriate measures in accordance with the laws of their countries through Interpol channels.²³

**The table represents a comparative result for the years
2022 and 2023**

Crimes	Number of registered cases		Number of people involved	
	2022	2023	2022	2023
Harming people online	1999	2046	1796	1905
Tampering with automated data processing systems	323	331	217	202
Fraud and online scams	1130	801	1958	1318
Child abuse online	113	56	124	78
Publishing illegal content online	1066	1083	1332	1427
Selling prohibited goods online	110	115	181	159
Other crimes	395	286	538	496
Total	5136	4718	6146	5567

Source: Ghania Hassani, *op. cit.*, p. 21

Algeria is ranked 19th in the world in the list of countries most targeted by cyber-attacks and hacking attempts against sensitive institutions, with the aim of espionage and information theft, as more than **70 million “cyber-attacks”** were recorded in **2024** and stopped by the Kaspersky anti-virus and anti-hacking cybersecurity program. The most widespread types of attacks in Algeria are through password recognition, exploitation of personal data, and remote monitoring, as during **2024**, **236 039 cyber-attacks** were recorded by the cybersecurity program by discovering the password of computers, **1895,689** attacks by exploiting personal information, and **1538 156** attacks by remote monitoring, by following the targeted person or entity and spying on them to try to hack their digital information.²⁴

Algeria is among the countries that have intensified efforts and

prioritized the provision of cybersecurity, and included it in the work map of many state institutions and structures, including ministries, directorates, banks, commercial and economic institutions, in order to protect the data and privacy of individuals, as well as the information of institutions, companies, networks and programs: Ministries, directorates, banks, commercial and economic institutions, in order to protect the data and privacy of individuals, as well as the information of institutions, companies, networks and programs, and to repel cyber-terrorism attacks and digital incidents that undermine them and their stability.

Algeria has started its bet with the field of digital security by establishing an institutional structure, manifested in the formation of cybercrime centers that specialize in digital detection, and Algerian security forces to follow up on this type of crimes related to cybersecurity, such as: The National Institute of Criminal Evidence and Criminology of the National Gendarmerie (INCC) of the National Gendarmerie General Command, as the first defense device to address such illegal digital violations, which are characterized by impersonation, possession of credit cards with unrealistic and fake names, fraud against individuals through fake emails, identity theft and the use of fake personal information, access to financial and banking information, hacking banks' information base and damaging websites, buying names, adopting fake accounts, and other types of cyber-attacks, and the Department of Defense.²⁵

Third: Defense technologies to confront cyber threats in Algeria:

Algeria's current challenges require building and establishing a strong digital infrastructure to integrate into the global environment in light of the challenges that accompany this service, and this can only be affected by the development of a comprehensive strategy for all sectors, the features of which are as follows:²⁶

1. In the field of security and national defense:

The Government Action Plan 2020 gave great importance to cyber defense by working to develop a strategy related to control and autonomy in the cyber space to confront the dominance of major powers in the digital space, from protecting the transfer of personal digital data and the security

of digital authorities through entire operating systems and Internet services to devices in order to achieve digital sovereignty.

2. In the field of capacity building:

The Algerian Space Agency is working to contribute to strengthening national sovereignty in the field of space technology and communications, as it oversaw the implementation of the national space program with the launch of six satellites, and Algeria has developed a national space strategy 2020-2040, one of the objectives of which is to secure institutional communications, bridge the digital divide and give the citizen the opportunity to be an active party in the global information society.

3. In the field of international cooperation:

Algeria participated in several international seminars and conferences in the field of cybersecurity policies, in addition to organizing several international events, including an international symposium on cybersecurity under the theme of public services and public security 27 - 28 March 2018. Among its recommendations was the establishment of a university to combat threats to develop Algerian technology to guarantee a secure national cyberspace. Algeria also hosted the seventh edition of the African Summit on Cybersecurity in the Age of Digital Transformation in Africa 10 June 2019, which addressed cyber security, technology, digital economy, electronic payment, private life, threats.

4. In the field of technical management:

Algeria established “CERT.Dz”, a computer emergency response center, which is an essential tool to protect sensitive information by detecting and dealing with emerging information risks such as viruses, spyware and vulnerabilities in operational systems, and providing solutions and measures to enable individuals and companies to anticipate cyber-attacks and avoid damage before they occur.

The cyber defense strategy of the People's National Army focuses on strengthening and updating the legal framework related to the use of information and communication technologies and the security of information and communication systems, and is mainly based on 07 axes:²⁷

➤ A functional and organizational aspect aimed at carrying out cyber

defense actions in a targeted manner within a functional and organizational chain dedicated to ensuring the homogeneity of actions.

- The legal aspect aims at updating and strengthening the legal framework to ensure the security of the information system on a permanent and continuous basis.
- The human resources aspect allows the provision of a highly qualified human resource in the field of operational and management activities in the field of cyber defense.
- Technical aspect, through which it works to raise the technical capabilities of protection and vigilance and ensure the ability to respond quickly to cyber attacks.
- The aspect of prevention and sensitization of the users of the army and other sectors to the dangers of the use of information and communication technologies.
- The aspect of cooperation in the field of cyber defense alongside the armies of friendly and partner countries in order to ensure the transfer, acquisition and development of expertise.
- The research and development aspect is a critical aspect of the cyber defense strategy through the ability to diagnose issues and find solutions to them.

Fourth: Preventive Mechanisms against Cyber Threats in Algeria:

1. Legal framework to combat cyber threats:

Algeria uses preventive mechanisms to confront cyber threats, which we mention below:²⁸

• The National Authority for the Protection of Personal Data:

Established by Law No. 18-07 on the protection of natural persons with regard to the processing of personal data, which entered into force on August 10, 2023, it is an independent body tasked with ensuring that the processing of personal data complies with the provisions of the law, while establishing technical and organizational measures to ensure the confidentiality and integrity of the processing and prevent the transfer of data to a foreign country.

• **National Information Systems Security System:**

The National System for Information Systems Security was established by Presidential Decree No. 20-05 and is placed at the Ministry of National Defense and is considered the state tool for the preparation of the national strategy in the field of security for information systems, consisting of the National Council for Information Systems Security and the Information Systems Security Agency.

• **National Reference for the Protection of Information Systems:**

A unified national guide for information technology security applied to public institutions and administrations based on the Prime Minister's Instruction No. 02 issued on July 3, 2016 was updated in 2020 in accordance with international standards such as the International Standard for Information Systems Security. The guide aims to raise the level of security of information systems and protect them from various cyber threats by setting appropriate security controls and providing the best-known global practices in terms of their security, as this reference is necessary for the adoption of the e-government approach.

• **National Agency for the Development of Digitization:**

Established by Presidential Decree No. 19-317 and placed directly under the Prime Minister, the National Agency for the Development of Digitization is in charge of designing the elements of the national strategy for the development of digitization and proposing them to the government in consultation with ministerial departments, institutions, the economic sector and civil society, and is in charge of ensuring the follow-up of the implementation of the national strategy for the development of digitization.

Algeria has introduced several legislations and laws to fight cyber threats and crimes in order to strengthen its cybersecurity, such as Law No. 09-04 dated May 09, 2009 on special rules for preventing and combating crimes related to information and communication technologies, as well as Law No. 10. 05 of 20 June 2005, which includes the electronic directory, in addition to the Code of Criminal Procedure and the Penal Code, especially Articles 303, 333, 394 and 396, which criminalize and impose penalties on anyone found guilty of illegally penetrating the information systems of

institutions or individuals.²⁹

In light of Law 09-04, the Algerian legislator enacted Law 09-04 on preventing and combating information and communication technologies (ICTs), which established a set of preventive and procedural measures to prevent and combat these crimes, the most important of which are:³⁰

- Preventive measures
 - Electronic surveillance
 - Utilizing service providers to prevent cybercrime.
- Procedural measures
 - Search and seizure of information systems
 - Extending the jurisdiction of Algerian courts in the case of extraterritorial cybercrimes committed by a foreigner and targeting Algerian state institutions, national defense, or strategic interests of the national economy
 - Mutual international judicial assistance to collect evidence related to the crime in its electronic form
 - The National Authority for the Prevention and Control of Crimes Related to Information and Communication Technologies is an independent administrative authority with legal personality and financial autonomy placed under the authority of the President of the Republic.

2. Authorities and bodies specialized in combating cyber threats:

The authorities specialized in investigating cyber-related crimes must possess the necessary means and techniques to solve the mysteries of the crimes, and this can be summarized in the following elements:³¹

- Developing and strengthening human capacities in charge of cybercrime investigations.
- Availability of the latest technological equipment in the field of automation and telecommunications.
- Having an extensive and continuously updated database.
- The ability to design and develop computer programs.

These elements have been the focus of the National Defense Establishment since independence, and through its continuous and ongoing efforts, it has been able to develop its capabilities and capacities at all levels. This can be clearly seen in the degree of professionalism enjoyed by

members of the National Gendarmerie and their use of modern means and techniques that help in the accomplishment of investigations and inquiries in the field of investigation.

- **National Gendarmerie Cyber crime Prevention Center :**

This center was established in 2008 and is the only agency specialized in this field in Algeria. Its main objective is to secure the information system in the service of public security and is considered a documentation center based in Bir Mourad Rais. This center works to analyze the data and data of committed information crimes and identify the perpetrators, whether individuals or groups, in order to secure and preserve information systems, especially those used in official institutions, banks and homes, and to assist other security agencies in performing their tasks. The National Gendarmerie Command, through the continuous and distinguished training of its members, international and national forums and exchange of experiences with other countries, has been able to provide qualified forces and therefore a category of computer engineers and legal experts in order to properly understand and address cybercrime. In the same context, the center was able to address many electronic and digital crimes as well as those related to social media and crimes related to the hacking of official websites of public and private institutions, whose criminals targeted automated data processing systems.³²

- **National Institute of Forensic Evidence and Criminology:**

This agency consists of a department specialized in several different fields, all of which guarantee expertise, training, education and all technical assistance. The Department of Automatic and Electronic Media is in charge of processing, analyzing and presenting all digital evidence that helps the justice system while providing assistance to specialists. It also consists of several equipment, including a repair and repair station for devices, media networks and graphic equipment and contains seven halls, guidance books, charged systems platoon, data analysis platoon, phone platoon, data acquisition, a distributor hall and storage halls.³³

•The Central Service for Combating Cybercrime of the National Security:

Established in 2011, which dealt with many cybercrimes, especially those related to social media pages, and then was attached to the Judicial Police Directorate in 2015 in order to investigate more crimes that threaten national security, such as the following cases: Threats, crimes against public order, attacks on the private life of citizens, terrorism, cybercrime, cases of inciting minors to debauchery and prostitution, crimes against information systems and hackers, insulting a statutory body and state symbols, fraud, and sexual harassment against minors.³⁴

•The National Authority for the Prevention and Combating of ICT-related Crimes:

It was established by the Algerian legislator in 2009: Article 14 of Law 04.09, dated August 5, 2009, defines the tasks of the Commission as follows:³⁵

- Activate and coordinate operations to prevent and combat crimes related to information and communication technologies
- Assist judicial authorities and judicial police services in their investigations of ICT-related crimes
- Exchanging information with their counterparts abroad in order to collect all data useful in identifying the perpetrators of ICT-related crimes
- Electronic updating of sensitive and confidential information and data to preserve the safety of the state and individuals.

CONCLUSION

Finally, we conclude that cyber threats are a major challenge to the national security of countries in the digital age. Addressing these threats requires comprehensive strategies that include developing national capabilities, enhancing international cooperation, and raising public awareness of the importance of cybersecurity. It is also clear from this study that the challenges faced by Algeria in this field require effective and comprehensive strategies to address cyber threats, as it needs to strengthen the digital infrastructure and develop human cadres specialized in cybersecurity.

In the light of this study, we can conclude the following points:

- Cybersecurity is one of the key elements that contribute to strengthening the national security of the country, as it aims to protect information and digital systems from cyber threats and attacks.
- Cyber threats refer to any type of risks or attacks that target electronic systems and networks with the aim of unauthorized access to data, destruction of information, or disruption of services. These threats include a wide range of malicious activities
- Cyber-attacks can threaten national security, as the country's critical infrastructure can be targeted, necessitating the need to strengthen cybersecurity measures to protect information and systems from these risks.
- Algeria's policy of maintaining its cybersecurity is a vital matter that aims to protect sensitive information and data from cyber threats, and the Algerian government has paid great attention to strengthening cyber capabilities, through a set of strategies, technical and legal mechanisms, and preventive measures to address cyber threats
- Algeria has introduced several legislations and laws to combat cyber threats and crimes, in order to strengthen its cybersecurity and enhance international cooperation in the field.
- This policy includes developing technological and security infrastructure and enhancing cooperation with other countries in the field of cybersecurity. Specialized bodies such as the National Cybersecurity Center, which aims to monitor threats and provide technical support to government and private institutions, the National Institute of Forensic Evidence and Criminology, the National Authority for the Prevention and Control of ICT-Related Crimes, and the Central Service for Combating Cybercrime of the National Security.

In order to strengthen cybersecurity, we can monitor a set of recommendations to address cyber threats in Algeria:

- Spread the culture of cybersecurity to raise awareness among citizens about the importance of cybersecurity
- Develop a comprehensive national cybersecurity strategy that includes clear action plans, defining the objectives and resources required to

confront cyber threats

- Promote cooperation in the field of cybersecurity by utilizing international experiences to gain the necessary skills and exchange information to address cyber threats
- Conclude regional and international agreements to combat cybercrime
- Apply artificial intelligence techniques to analyze data and detect abnormal patterns, helping to identify cyber threats faster and more accurately
- Modernizing laws related to cybersecurity to ensure a strong legal framework that supports protection efforts and enhances the effectiveness of legal actions against cybercrime.

Bibliography List :

¹ Lamia Tala, "Cyber threats and islands: their impact on the national security of states and strategies to combat them", **Maalem Journal of Legal and Political Studies**, Vol. 4, No. 2, 2020, p. 60

² Fares Mohammed Al-Amarat, **Cybersecurity Concept and Challenges**, Amman: Gulf House for Publishing and Distribution, 2022, p. 16

³ Chouirab Jillali, Mourad Fayza, "The concept of cyber warfare and cyber security", **Journal of Rights and Freedoms**, Vol. 11, No. 1, 2023, pp. 165-166

⁴ Samir Galaa Al-Drous, "National Cybersecurity: A reading of the most important security and technical strategies to confront cybercrime in Algeria", **Riwaq Journal of Social and Humanitarian Studies**, Vol. 8, No. 2022, pp. 255-256

⁵ Chraiet Najma, "Cybersecurity in the Algerian Defense Policy and Doctrine: Opportunities and Limitations", **Algerian Journal of Politics and Security**, Vol. 2, No. 2, December 2023, pp. 78-80

⁶ Samir Kalaat Al-Drous, **op. cit.**, pp. 256-257

⁷ *ibid.*, p. 256

⁸ Chraiet Najma, **op. cit.**, p. 79

⁹ Abdelghani Chergui, "Cyber Threats, the Question of Sovereignty and the Re-reading of Westphalian Sovereignty", **Journal of World Politics**, Vol. 7, No. 2, 2023, p. 275

¹⁰ **What is a Cyber Threat**, accessed on 25/12/2024, at 12: 16, at the link: <https://www.upguard.com/blog/cyber-threat>

¹¹ **Cybersecurity threat**, accessed on 24/12/2024, at 18: 34, at the link: https://www.hpe.com/emea_middle_east/en/what-is/cybersecurity-threats.html

¹² Assia El Omrani, "International Cooperation in the Face of Cyber Algeria: Algeria as a Model", **Algerian Journal of Political Science and International Relations**, Vol. 3, No. 2, December 2010, pp. 59-60.

¹³ Manal Al-Balkasi, **Securing Cyber Threats Under the Digital Microscope**, Al-Abikan Library, 2024, pp. 59-58

¹⁴ Lehelli Abdelkader, "Cyber Security in the Algerian National Defense System", **social science journal** ,vol.14,n°1, 2024,p107

¹⁵ Manal Al-Balkasi, **op. cit.** pp. 67-66

¹⁶ Lehelli Abdelkader ,**Op cit.**p107

¹⁷ Manal Al-Balkasi, **op. cit.** p. 101

¹⁸ Dalila Al-Aoufi, "Cyber warfare in the age of artificial intelligence and its bets on international security", **Al-Hikma Journal for Philosophical Studies**, Vol. 9, No. 2, 2021, p. 782

¹⁹ Rabai Houssin , Samar Mahmoud, "Cyber Warfare: Risks and Strategies for Achieving Internal and International Cybersecurity", **Algerian Journal of Human Security**, Vol. 7, No. 2, 2022, p. 177

²⁰ Farah Yahia Al-Zaatara, **Cyber Threats to US National Security**, Al-Arabi Publishing and Distribution, 2023, p. 100

²¹ Fares Mohammed Al-Amarat, **Cybersecurity: Concept and Challenges of the Age**, Amman; Dar Al-Khaleej Publishing and Distribution, 2022, pp. 52-54.

²² Ghania Hassani, "SCLC...The Digital Nerve to Combat Cybercrimes", **Police Magazine**, No. 158, May 2024, p.p. 20-21

²³ Ibidem

- ²⁴ Algeria was targeted with 70 million cyber-attacks in 10 months, accessed on 12/01/2025, at 20: 22, at the link: <https://www.el-massa.com/dz>
- ²⁵ The future of cybersecurity in Algeria Prospects and Challenges , accessed on 11/01/2025, at 16: 10, at the link: <https://dounia.dz>
- ²⁶ Bouriah Salma, " Algerian public policies in the field of cybersecurity: reality and challenges", **Policy and Law Notebooks**, Vol. 15, No. 1, 2023, pp. 285, 286.
- ²⁷ Rabai Houssin and Samar Mahmoud, **op. cit.**, pp. 188-187.
- ²⁸ Badrin Sid Ali, "Algeria's strategy to confront cyber threats", **Police Magazine**, No. 156, October 2023, p. 50
- ²⁹ Djamel Bouazdia, "The Algerian strategy in the face of cybercrime, challenges and prospects", **Journal of Legal and Political Sciences**, Vol. 10, No. 1, April 2019, p. 1278
- ³⁰ Mehdi Redha, "Cybercrimes and mechanisms to combat them in Algerian legislation", Vol. 6, No. 2, **Elise Journal for Research and Studies**, 2021, pp. 118-120
- ³¹ Bara Samir, "Cybersecurity in Algeria: Policies and Institutions", **Algerian Journal of Cyber Security**, Issue 4, July 2017, p.p 270- 269
- ³² Dandan Djamel Eddine, "The security strategy of the Algerian state in the fight against cybercrime", **The Voice of Law**, Vol. 7, No. 2, November 2020, p.p. 986- 987
- ³³ Youcef Boughrara, "Cybersecurity: Algerian Strategy for Security and Defense in Cyberspace", **Journal of African and Nile Basin Studies**, Vol. 1, No. 3, September 2018, p. 111.
- ³⁴ Samir Galaa Al-Drous, **op. cit.**, p. 260.
- ³⁵ Aicha Kada Ben Abdallah, "the realities and stakes of cyber security and defense in Algeria", **Journal of police and legal science**, Vol 14, 2023. P20.