The Sankalpa: International Journal of Management Decisions
ISSN: 2454-7425

Volume 12, Issue 1 (January - June 2026)

Mechanisms for Achieving Algerian National Security Through Cybersecurity

Miloudi Mohamed[1*], Merad Ahmed[2]
[1]Lecturer Class A, Amar Telidji University of Laghouat, Algeria. m.miloudi@lagh-univ.dz
[2]Lecturer Class B, Amar Telidji University of Laghouat, Algeria. ah.merad@lagh-univ.dz

Received: 24/10/2025 Accepted: 03/04/2026 Published: 03/06/2026

*Corresponding author

Abstract
This study aims to emphasise the importance of cyber national security and Algeria's strategy for achieving it. National security is indeed a central benchmark for measuring the effectiveness of any political system. However, national security faces a variety of threats. Technological developments have brought new threats and negative impacts affecting individuals and states alike, such as hacking into the internet to obtain sensitive information about a country and spy on it, or using such access to spread and promote hostile ideas. This constitutes a threat to national security.
Algeria, like other states, has adopted comprehensive mechanisms and strategies with international and technological dimensions to safeguard its national security in these circumstances.
Keywords: Cybersecurity; Algeria's cyber national security; national security strategy; security threats.

Introduction

National security is of vital importance to states due to the threats they face, particularly in light of globalisation, the information and communications revolution, and cyber warfare. These developments have introduced new threats and had a negative impact on national security. These threats include breaching internet networks to obtain sensitive information about a country and spy on it, or using such information to disseminate and promote hostile ideas. Such activities constitute a threat to national security.
For this reason, Algeria, like other states, has adopted comprehensive international and technological mechanisms and strategies to achieve its national security, primarily through cybersecurity. Cybersecurity is a strategic instrument relied upon by states and a crucial component in warfare. Indeed, it has become one of the most important pillars of national security. However, achieving cybersecurity is a significant challenge fraught with threats and risks, particularly given the rapid pace of technological development. It is therefore necessary to keep abreast of these developments in order to provide the required protection, whether preventive or remedial.
Additionally, dominance in cyberspace is becoming increasingly important for carrying out effective attacks across land, sea and air, while also enabling states to prevent cyberattacks that do not recognise geographical boundaries.

Study problem/research question

The study focuses on the following question:
How does cybersecurity contribute to Algerian national security?
The importance of this study stems from the importance of the topic itself, especially given that cybersecurity and national security are currently major concerns, particularly in light of ongoing developments and threats affecting both individuals and states. The study also aims to:

- examine the nature of cyber threats and the most important strategies that Algeria has developed to confront them.
- provide solutions and proposals to strengthen cybersecurity.

-Chapter One: Conceptual Framework

Section One: The Concept of Cybersecurity

1. The cyber domain (cyberspace):

The term originates from the Greek Kybernetes, meaning "steering/command of a ship," or "the governor," or "the one who steers." In ancient Greece it was used to mean "ruler of the country." The Latin equivalent refers to "the governor." In this context, it refers to the world of networks and information beyond the computer screen with which the user interacts.

The term has been defined as follows: 'The scientific study of the means by which information is transmitted and control is exercised over machines, the brain and the nervous system'. It also denotes a system for organising and making available vast quantities of data stored in computers.

In the context of cybernetics, it refers to the science of control and communication, i.e. the general theory of interconnected processes, whether they are scientific, technical, psychological or social. From an administrative perspective, cybernetics is the scientific planning and prior organisation of administrative matters, the mathematical and logical analysis of administrative data, and the selection of optimal solutions to achieve a defined objective[1].

Conceptually, cybernetics expresses how information can be controlled, exploited and developed in a dynamic environment. It includes matters related to communications and systems theory. A modern organisation or company can be considered a system and a living organism, similar to a biological one. It is composed of electronics and people who are organised and operate together to achieve its goals. Therefore, a cybernetic company is one in which oversight and communication are shared between human beings and electronics.

The term was first introduced in this context by the thinker Norbert Wiener, who used it as the title of his 1948 book. Wiener defined it as: 'the science of control in living organisms and machines, and the study of communication mechanisms in each of them'. Accordingly, cybernetics involves replacing human beings with electronic devices for mental processes related to calculation, review, control and direction[2].

2. Information security

Information security refers to the set of procedures and preventive measures used to protect information and ensure its confidentiality. Protecting data and information from theft, tampering or unlawful intrusion has become a matter of increasing concern. This requires studying all technical, material, human and legal fields that contain information protection measures and ways to limit attempts at violation or destruction[3].

It is also defined as: 'protecting and providing information to users when they need it', taking into account the following factors:

A. Trust: the extent to which citizens or business institutions trust that the use of e-government systems will not harm them. Trust also refers to confidence in the government as an electronic administrator and in the process itself.

B. Security: ensuring that information is not exposed to theft or alteration. Today, states and institutions are increasingly aware of the importance of securing users' information.

C. Availability: ensuring access to information when needed.

D. Confidentiality: protecting information from being accessed by others, emphasising the importance of privacy. Therefore, confidentiality is particularly important when handling users' information and protecting it from unauthorised access[4].

3. Definition of cybersecurity

Cybersecurity is defined as the security of networks, information systems, data and internet-connected devices. It is therefore the field concerned with the procedures, measures and protective standards that must be adopted or complied with to address threats, prevent intrusions or reduce their impact[5]. The U.S. Department of Defense (the Pentagon) provided the following precise definition: All necessary administrative measures to protect information in all its physical and electronic forms from crimes, attacks, sabotage, espionage and incidents. Richard A. Kemmerer defined it as 'defensive means that detect and frustrate attackers' attempts', while Amorso Edward described it as 'means that reduce the risk of attacks against software, computer systems or networks. These include methods and tools used to counter intrusions, detect viruses and stop them'[6].

Thus, cybersecurity can be defined as a set of mechanisms, procedures and tools aimed at protecting and securing software, information and computer systems against attacks, intrusions and cyber threats that may endanger national security.

4. Types of cybercrime

There are several types of cybercrime, including:[7]

1) Crimes against data and information systems

These include offences involving unauthorised access to information systems, as well as offences involving the exposure and interception of data, and acts that hinder its operation.

2) Crimes involving money: These include fraud, deception or forgery using information technology; embezzlement or theft of funds using information technology; and theft of bank cards and electronic money.

3) Crimes involving the sexual exploitation of minors: These refer to acts involving the sexual exploitation of minors.

4) Crimes against intellectual property, such as copying digital works or pirating software, selling or displaying counterfeit works, or putting them into circulation, and infringing copyright or related rights.

5) Crimes affecting public safety and state security, such as disseminating false or hate/incitement-based (racist) information, threatening individuals, inciting crimes or terrorism, and disrupting government operations or committing espionage involving confidential state information.

6) Crimes involving the encryption of information: These include the marketing, distribution, export or import of prohibited encryption tools[8].

The second requirement: The Concept of National Security

The concept of national security can be traced back to the mid-seventeenth century and the conclusion of the Treaty of Westphalia in 1646. This treaty helped lay the foundations for the nation-state system. The term 'national interest' was frequently employed by states when engaging in war, forming alliances, or undertaking other activities related to foreign policy, to justify their actions on the grounds of defending their national interests.

From an analytical perspective, this concept did not become central to the human sciences until after the Second World War. This academic interest formed part of a broader focus on a phenomenon older than national security itself: the concept of 'national interest'. In fact, some have argued that national security may have evolved within the broader framework of national interest. For example, Wilfrids

attempted to combine the concepts of 'national interest' and 'national security' into a single term: National Security Interest[9].

The term 'national security' was first formally used after the Second World War in 1947, when the US administration established an official body known as the US National Security Council. This body was responsible for investigating all matters and events that affected the United States and threatened its security. Since then, the US National Security Adviser has become a key figure in shaping US strategy and security policy. Nevertheless, some U.S. leadership figures still use the term 'national interest'[10].

1. Definition of national security

Linguistically, the term 'national security' consists of two words: 'security', which denotes reassurance (i.e. the opposite of fear), and 'national', which refers to the nation-state. A state cannot exist without sovereignty, which highlights the close connection between national security and sovereignty such that they cannot be separated.

According to the Encyclopaedia Britannica, national security means protecting the state — the nation against the threat of coercion by a foreign power, repelling aggression, preserving the state's entity and ensuring its independence[11]. In short, the purpose of national security is to defend the state's sovereignty.

At a societal level, national security is defined as the absence of fear, the disappearance of threats and the predominance of psychological reassurance. It is characterised by three features, both material and psychological:

-The absence of fear of the unknown;

-The disappearance of threats from the 'other';

The predominance of reassurance is the outcome of the previous two features[12].

At the national level, it is defined as: 'the state's ability to defend itself against those who threaten it, whether through external attack or internal sabotage, and to defend the integrity of its borders and its existence.[13]'

In this context, Al-Kilani considers national security to be what the state does to protect itself from external and internal dangers that could lead to foreign control as a result of external pressures or internal collapse[14].

Along the same lines came Robert McNamara's book The Essence of Security, published in the 1960s. In it, he emphasises that security encompasses more than just the military, linking development to security. This formed the basis of a developmental concept of security. He states: 'Security is not just equipment, although it includes equipment.' Security is not just traditional military activity, although it involves that too. Security is development, and without development, security cannot exist. Developing countries that grow cannot simply remain secure.'

Based on this definition of national security, it can be considered in its modern sense as being characterised by comprehensiveness. It has moved beyond matters related to borders, stockpiling weapons and military training to include economic and social issues. In this way, national security becomes a societal issue that encompasses social welfare and all related matters.

Accordingly, national security should be a priority in strategic thinking at military and political levels for several reasons. Firstly, it acts as a driver of foreign policy and constitutes one of its most important foundations. It is also closely linked to the main threats and ambitions within the remit of economic and social development. Furthermore, it aligns with the political system's supreme interests, as defined by its philosophy[15].

2. Features of national security

National security is characterised by three main features:[16]

1. Change (dynamism): it is a dynamic reality that evolves in response to changing circumstances. It is linked to domestic, regional and international conditions and factors.

2. Relativity: National security is a relative, not an absolute, concept. It arises from states' continuous efforts to increase their power, achieve superiority, and establish hegemony. Consequently, international relations are characterised by uncertainty and distrust — an issue that realists refer to as the 'security dilemma'.

3. A composite and integrated concept: National security is an integrated, indivisible notion. It encompasses achieving security in both its internal and external dimensions[17].

The second topic: Security threats and measures to ensure cybersecurity

The first requirement: Security threats

In cyberspace, security risks can be classified into two types according to their objectives:

Threats targeting states: These threaten national security and endanger critical infrastructure such as financial markets, banking, the healthcare sector, transport and nuclear facilities[18].

1. Identifying Threat Sources to Security

This is carried out at three levels:

A. Decision-making level: This includes the highest security levels and official institutions (defence, foreign affairs and intelligence) responsible for preserving and maintaining national security. Concrete work steps are required to detect threats to national security, including identifying, prioritising and defining national objectives, in order to formulate an appropriate political and security strategy. These variables must be continuously monitored to uncover threats and determine the most effective method for dealing with them.

B. Elite level: This includes opinion leaders in security-related fields, as well as experts and researchers. This level aligns with the previous one in that it encompasses specialised professionals and requires their views and warnings to be taken into account.

C. Public (mass) level: This is the weakest link, largely due to the extent to which security awareness is spread among citizens. Additionally, a higher level of cultural awareness can increase the public's ability to recognise security threats, such as a strong sense of belonging to the homeland[19].

2. Sources of threats

This is addressed on two levels:

A. Main sources of threats: These are dangers that threaten the state as a whole and affect people's lives. Examples include threats to water resources (e.g. the Nile for Egypt and the Tigris and Euphrates for Iraq and Syria), attacks on oil resources (e.g. in Libya, Iraq, Iran and Venezuela), and other similar threats.

B. Secondary threats: These threats have only a limited and secondary impact. They can be dealt with gradually or deferred, provided they remain secondary and do not evolve into main threats to the state[20].

3. Factors Undermining Security and Indicators for Measuring Them

A. Internal sources of threats

Internal threats are local and domestic dangers that undermine a state's national security. They can significantly impact societal cohesion, for example through sectarian tensions or unrest (e.g. Sunni-

Shiite conflict in the Gulf, Muslim-Copt conflict in Egypt, etc.). Such threats may escalate into armed conflict, as seen in the Houthi conflict in Yemen and the Kurdish conflict in Turkey.
Furthermore, such threats can spread from one state to affect multiple states in a region, as is the case with Kurdish populations in Turkey, Syria and Iraq. They can also arise from power struggles, opening the door for external powers to intervene to secure their own interests, as occurred in Iraq and Syria, thereby undermining the state's political stability and threatening its national security.
Indicators for measuring internal threat components
These can be summarised as follows:
- Weak political loyalty and reduced national belonging;
- Ambiguity and lack of clarity regarding national objectives;
- Opposition to the political system and weakness in civil society participation;
- undermining the prestige and effectiveness of the authorities, alongside the increased influence of pressure groups.

B. Sources of external threats

External threats are dangers that originate outside a state and undermine its security. They often involve the intervention of external powers or splinter, separatist or opposition groups supported or hosted by foreign states. Geographically, these threats are frequently linked to neighbouring countries (e.g. Kurdish groups in Iraq, the Houthis in Yemen and ISIS).
At their most extreme, these threats manifest as armed attacks on a state's territory and external interests. Sometimes, governments may exaggerate these threats by invoking conspiracy theories to justify repressive measures and authoritarian control. They may also invent external sources of threat, similar to how some states use external threats to obtain foreign assistance, build national consensus and address internal crises. In such cases, these external threat sources undermine the state's ability to formulate its foreign policy, thereby entrenching political dependency, which is one of the gravest and most dangerous threats to national security. Consequently, the state loses the capacity to pursue an independent foreign policy.
Indicators for measuring elements of external threats can be summarised as follows:
- severing diplomatic relations with neighbouring states;
- imposing political sanctions on the state or issuing condemnation resolutions by international organisations and bodies;
- Losing membership status or being suspended/removed from regional and international organisations[21].

Section Two: Protection of Personal Information

In order to protect personal information in the digital environment, the following is required:
A. Providing technical protection tools (the technical dimension): This involves reducing or preventing the collection of personal information without the user's knowledge. It also includes techniques that enable users to interact with the digital environment in a way that is suitably discreet for their intended use. Additionally, protective software against viruses, intrusion detection systems and technical tracking and monitoring programmes must be used to identify who acted, when and from where[22]. This would lay the groundwork for subsequent legal accountability. It also involves using artificial intelligence in cybersecurity to improve institutions' ability to detect digital intrusions and manage information system risks[23].

B. Providing an appropriate legal framework for regulation and protection (the legal dimension):

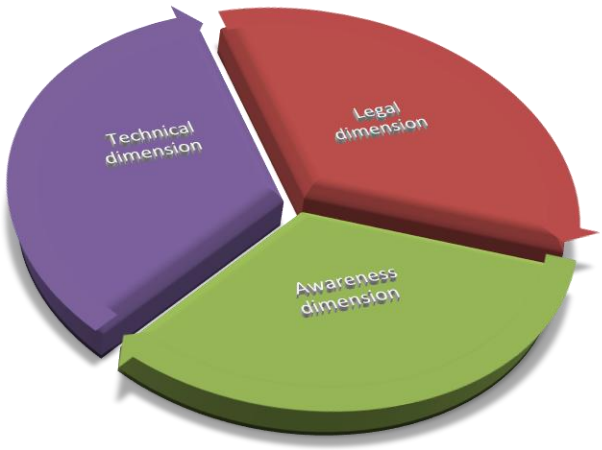
This involves enacting suitable legislation to protect information and personal data. Many existing laws would need to be revisited, such as those related to administrative or criminal law, to ensure they cover electronic crimes, including electronic sabotage or theft, attacks against electronic signatures and information forgery crimes, as well as to protect individuals' privacy. In order to create an appropriate digital environment, a set of legal instruments is required, including:

- a law to protect information and data
- a law to regulate telecommunications services and investment in them, alongside market liberalisation and fair competition[24]
- laws related to intellectual property to ensure innovation and creativity
- a law to protect access to information, electronic identity and electronic signatures
- a law to combat internet crimes and protect property[25]

C. Raising awareness of the necessary performance to protect privacy and of how to deal with the digital environment (the awareness dimension):

This can be achieved by disseminating a suitable administrative and organisational strategy among institutions and users. The aim is to establish a culture of engagement with the digital environment, enhance awareness of risks and prevent their occurrence[26]. Additionally, the government should launch a public awareness campaign on the security of the country's cyberspace, targeting all levels of society and explaining the security risks and how to avoid them.

The following figure illustrates the scope of cybersecurity[27].



Section Two: Means and Procedures to Ensure Cybersecurity

A variety of methods and processes can be used to ensure cybersecurity, including:

1. Organisational and structural strategy: Specialised cyber-security formations must be established within the State's security agencies. Their tasks include setting cyber defence and cyber-attack policies and ensuring that all government administrations implement the prescribed security prevention measures.
2. Developing external security agreements: This involves developing and updating bilateral and multilateral security agreements with other countries to include cybersecurity issues and potential areas of cooperation in this field.

3. A strategy of encouragement and deterrence: Encouragement is achieved by encouraging citizens to report cyber-attacks without revealing the informants. This can be achieved by setting up a dedicated hotline. Conversely, the state must impose deterrent penalties on perpetrators of cybercrimes, which requires the enactment of deterrent legislation in this area[28].
4. Encryption: This involves embedding information in an incomprehensible, confidential code — i.e. replacing it with symbols — and then decrypting this code using the encryption key to restore the message to its original form once it has reached the secure recipient[29].
5. Unified electronic identity: This involves identifying citizens through a national number, as occurred in Algeria with the introduction of biometric passports and identity cards. The purpose is to establish a unified electronic identity, thereby enabling secure access to electronic services[30].
6. Digital certificates: A digital certificate is an essential tool for verifying the identity of parties exchanging information. It is an electronic document issued by an internationally recognised independent entity known as an Accreditation/Certification Authority. This body proves that the holder of the electronic message or transaction is the person specified in the certificate. Thus, a digital certificate enables its holder to establish their electronic identity and confirm the validity of all the information contained within it[31]. A digital certificate includes a set of electronic data and information. The Algerian Authority for the Regulation of Post and Telecommunications (P&T) defines an electronic certificate as a form of electronic identification card on the internet that establishes a zone of trust between two entities that require authentication to communicate and exchange confidential information remotely. It also specifies the name of the entity and attests that it possesses the public key listed in the certificate. All electronic certificates are issued by a trusted third party or certification authority.
There are four types of electronic certificate: the electronic signature certificate; the web distributor certificate; the private virtual network certificate; and the signature certificate (code/signature of a symbol).
Electronic authentication can be used in various fields, including e-government, e-commerce, and small and medium-sized enterprises (SMEs)[32].
7. Electronic signature: An electronic signature is a method of protection used in electronic transactions. It is a specific electronic method designed to link a particular person to defined information or allow them to access a specific information repository[33]. It also facilitates the documentation and signing of transactions without the need for travel or physical presence, thereby saving effort, time and costs associated with completing an administrative contract. Under Algerian law, an electronic signature is defined as electronic data that are attached to, or logically associated with, other electronic data for the purpose of authentication[34].
8. Antivirus systems and processing (Antivirus): Antivirus software detects and removes computer viruses, worms and Trojan horses, as well as tracking and tracing files, whether transmitted via email or removable storage media[35].
9. Firewall: A firewall is software designed to protect a company's information and prevent intrusion and destruction. It does this by creating a barrier between the institution's internal network and the internet, inspecting and filtering all inbound and outbound traffic to prevent unauthorised access. This helps to avoid the risk of viruses and malicious programmes. It is also necessary to have services that record the electronic trace of the service requester in order to identify the actor, place and time. Furthermore, passwords must be complex and changed automatically over time[36].

Third Section: Algerian state policies for achieving national and cyber security

First requirement: The Cyber Defence Strategy in Algeria

Specialists emphasise that Algeria's high cybercrime rate is closely related to the number of internet users. A report compiling data from multiple specialised websites and statistics[37] on internet use worldwide indicates that Algeria has over 60 million internet users out of a population of approximately 47 million. This figure includes both fixed and mobile subscriptions: fixed internet subscriptions totalled 7.61 million, while mobile internet subscriptions reached 54.05 million[38]. The figures suggest that users often hold more than one mobile line, as shown in the table.

Of these users, 27 million use social networking platforms, corresponding to 57.7% in 2025[39]. These figures imply that social media platforms have become fertile ground for all forms of extremism and a 'trap' for organisations.

The following table illustrates demographic growth and the number of internet users in Algeria from 2000 to 2025.

Year	2025	2024	2020	2017	2016	2014	2012	2010	2008	2005	2000
Population Number of	47.985.397	46.814.308	44,616,624	41.689.299	41,263,711	38,813,722	37,367,226	34,586,184	33,769,669	33,033,546	31,795,500
Internet Users	60.560.337	54.550.359	36.967.783	34.628.551	28.553.025	10.110.938	5,230,000	4,700,000	3,500,000	1,920,000	50,000
Percentage of Internet	%126.2	%116.52	%82.85	%83.06	%69.19	%26.04	%14	%13.6	%10.36	%5.8	%0.15

Prepared by the researcher based on consultations.

Kaspersky Cybersecurity reported that Algeria faced more than 70 million cyberattacks in 2024. During the same period, more than 13 million phishing attempts were blocked; these attacks targeted banks, public institutions and individual users via fraudulent emails and fake links[40]. Cyberattacks in Algeria are reported to be increasing by 15% annually. For instance, Algeria dealt with 2,400 cases involving malicious email attachments in 2023, a figure that rose to 2,700 in the first months of 2024[41]. In 2025, the authorities announced the dismantling of a phishing network involved in approximately 140,000 cyberattacks, primarily targeting banking accounts and local digital platforms, highlighting the scale of the threat.

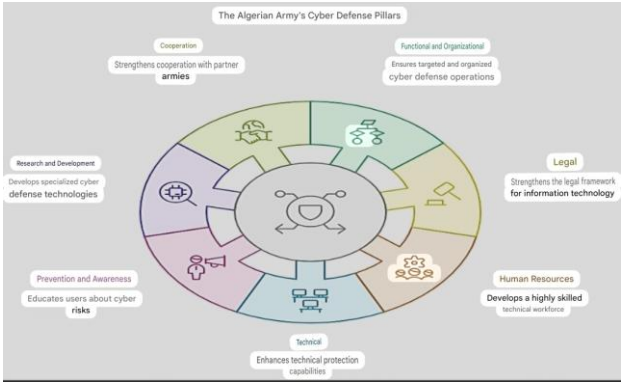
However, these figures do not fully reflect the actual situation because they only cover cases that have been processed following a complaint. Furthermore, digital development and the intensive use of social media networks are among the factors behind this upward trend in cybercrime.

Given the nature of cybercrime and its distinctive features — such as the absence of geographic barriers and the difficulty of detecting the user's identity — these circumstances necessitate the strengthening of cybersecurity using the most advanced technical tools in order to confront the dangers it poses. Therefore, on 6 November 2015, the High Command of the National People's Army established a unit entitled "Cyber Defence and Monitoring of Systems Security" at the level of the Staff of Use and Preparation (within the Army's commands). The aim of this unit is to secure and protect the country's vital systems and facilities against threats related to cyberterrorism and electronic espionage of Algerian state secrets.

The purpose of this unit is to protect the state from all cyber defence threats. It covers all aspects related to this system, becoming comprehensive and effective in securing and protecting Algeria's vital and sensitive systems and facilities. The unit's mission includes planning, implementing and monitoring activities that aim to ensure the effectiveness of the comprehensive cyber defence policy against threats targeting information systems, communications systems and the army's weapons systems. To this end, the National People's Army Command has developed an integrated and effective cyber defence strategy to protect the state's vital systems and facilities.

The Algerian Army's cyber defence strategy is based on seven pillars, namely:

1. Functional and organisational axis: This is implemented within a unified functional and organisational structure to ensure that cyber defence activities remain coherent and effective across army operations.
2. Legal axis: This focuses on updating and strengthening the legal framework governing the use of information and communication technologies, with a particular focus on securing information systems.
3. Human resources axis: The aim is to ensure high technical readiness and the availability of highly competent personnel in the field of cyber defence. This is a core objective for successfully integrating this area into the Army's operational and administrative activities.
4. Technical axis: This continually strengthens and adapts technical capabilities for the protection, detection and response to cyberattacks, while maintaining constant vigilance regarding the methods and tools used by attackers.
5. Prevention and awareness: This involves raising awareness among National People's Army users of the risks and threats arising from the use of information technologies, in both professional and personal contexts.
6. Research and Development Axis: This involves the use of specialised technical tools by the Research and Development structures of the National People's Army, particularly those intended to protect against cyber threats. These tools are considered a decisive element in the cyber defence strategy.
7. Cooperation axis: This aims to enhance cyber defence cooperation with the armed forces of partner countries in order to benefit from their advanced expertise and technological capabilities[42].



The National Defence institution has devoted significant attention to strengthening its capabilities through continuous efforts at all levels. This is evident in the professionalism of the National Gendarmerie and its use of modern tools and techniques to assist with investigations and inquiries. For instance, it has adopted advanced incident re-enactment programmes providing accurate and detailed reconstructions to facilitate the formulation of predictions and interpretations to help

investigators prepare their reports. Additionally, the institution has procured the latest equipment and software to protect information infrastructure against digital threats and has provided its personnel with the highest level of training. This is evident in its achievements, such as its personnel working to prevent the leakage of Baccalaureate examinations and developing and deploying digital applications, among other information-related accomplishments[43].

In this context, on 20 January 2020, a presidential decree establishing a national system for the security of information systems was published in the Official Gazette. The decree explicitly stipulates the preparation of a national strategy in this field, including digital investigations in the event of cyberattacks targeting state structures and institutions. Supervised by the Ministry of National Defence, this national system is overseen by the National Council for the Security of Information Systems (Conseil national de la sécurité des systèmes d'information). Its tasks include:

- studying and preparing the national strategy for the security of information systems;
- establishing an agency responsible for the security of information systems and tasked with coordinating and implementing the national strategy in this area, as determined by the Council.

The issuance of this presidential decree highlights the significant importance that Algeria places on cybersecurity and its forward-looking vision of profound changes that could impact other sectors. It also demonstrates the country's commitment to safeguarding its vital institutions and facilities.

Furthermore, in 2016, Algeria introduced a unified national framework for the security of automated information systems with the aim of:

- extending protection and security arrangements for information systems across state structures and institutions;
- raising awareness among internet users of the risks and threats resulting from their use;
- promoting the safe and proper use of the internet and information technology.

Alongside these measures, the Army is working to counter cyber threats based on the premise that securing and protecting the information systems used by civilian and military institutions is now directly related to protecting national sovereignty.

Second requirement: Laws related to cybersecurity in Algeria

Algeria has adopted a bill to combat cybercrime, which includes mechanisms for monitoring the internet and countering 'virtual offences' (cybercrime). The procedures applied include:

- imposing new conditions and licensing requirements on internet operators and providers;
- requiring these companies to preserve electronic communications (records of correspondence);
- obliging internet cafés to install surveillance cameras;

Launching search and inspection campaigns carried out by security authorities and imposing penalties on offenders.

In terms of Algerian legislation, a division was introduced within the Penal Code, resulting in the issuance of Law No. 04-15, which contains the Penal Code. The seventh chapter (bis) was allocated to offences involving interference with automated systems for processing data. Subsequently, in 2006, the legislator introduced an amendment under Law No. 06-23, dated 20 December 2006. Then, in 2009, Law No. 09-04 was issued, establishing specific rules for preventing and combating crimes connected to information and communication technologies.

Third requirement: Specialised Cybersecurity Authorities in Algeria

There are several bodies specialising in cybersecurity, including the following:

1. The National Authority for the Prevention of Crimes Related to Information and Communication Technology (ICT)

This authority was established by Law No. 09-04 to prevent and suppress crimes related to information and communication technology[44]. Its responsibilities include activating international judicial and security cooperation, as well as managing, coordinating and carrying out preventive operational activities. The Authority also provides technical assistance to judicial and security authorities and may be tasked with performing judicial expert assessments in cases of attacks against an information system that threaten state institutions, national defence or the strategic interests of the national economy[45].

2. Specialised Criminal Judicial Authorities:[46]

These were established under Law No. 04-14 dated 10/11/2004, amending and supplementing the Code of Criminal Procedure. They have jurisdiction over crimes affecting automated data processing systems, in accordance with Articles 329–37–40 of the Code of Criminal Procedure. They also have an expanded territorial jurisdiction pursuant to Executive Decree No. 06-348 dated 01/05/2006. Accordingly, they hear cases involving information and communication technology offences committed abroad, even if the perpetrator is foreign, provided such offences target state institutions or national defence, as set out in Article 15 of Law No. 09-04.

3. The National Institute of Forensic Evidence and Criminalistics

The Institute provides technical assistance, including an Automated and Electronic Media Unit which is responsible for processing, analysing and presenting digital evidence to assist the administration of justice. The Institute also offers technical support to investigators during on-site examinations. Additionally, the Institute addresses evolving forms of cybercrime and software viruses at the national network level, which will present a challenge in the medium to long term. Furthermore, the General Directorate of National Security is responsible for preventive measures, delivering awareness lessons at various educational levels. The Directorate also participates in national conferences, seminars and other activities intended to inform citizens about the seriousness of cybercrime. Furthermore, given the international dimension that such crimes often have, Algeria is an active member of the International Criminal Police Organisation (INTERPOL). This enables the exchange of international information and facilitates judicial procedures related to the surrender of offenders, including the execution of international judicial requests and the dissemination of arrest warrants for individuals wanted internationally[47].

In addition, the following bodies and institutions are involved:

- The National Council for Security of Information Systems (CNSSI), which is responsible for setting public policies and coordinating between ministries and operates under the Ministry of National Defence. The Information Systems Security Agency (ASSI), which identifies cybersecurity vulnerabilities and provides technical guidance. The Algerian Computer Emergency Response Team (DZ-CERT), which responds rapidly to cybersecurity incidents. DZ-CERT was established by Presidential Decree No. 25-321, issued on 30 December 2025, which defined Algeria's national cybersecurity strategy for the period 2025–2029. This was complemented by Decree No. 26-07, issued on 7 January 2026, which concerns the legislative framework for cybersecurity within public institutions. This decree requires the establishment of internal cybersecurity units within public institutions, including a cybersecurity defence function.

Conclusion:

Algeria needs to invest further in cybersecurity. This investment could focus on two areas: first, localising cybersecurity technologies and developing the related cyber infrastructure, and second, improving skills and expertise to build national capabilities in designing, managing, analysing and

developing cyber systems. Additionally, the incorporation of 'cyberspace' as a field of study within educational curricula should be seriously considered, in coordination with the Ministry of National Defence and the National Cyber Administration. Scientific research and innovation must also be encouraged.

Furthermore, awareness must be raised among employees across all state institutions, their professional standards must be strengthened, and the infrastructure needed to enter the global software industry must be established, while enabling domestic products to compete with imported ones. To achieve this, the government must incentivise investment and cooperation between civilian and military sectors, ensuring that each benefits from the other without compromising the principles of confidentiality and privacy.

Civil society institutions also play an important role in addressing the unsafe use of information technology. This can be achieved through scientific activities and by promoting a culture of safe internet use and modern digital applications. Finally, artificial intelligence should not be overlooked as it is one of the most important tools for enhancing states' security capabilities.

List of sources and references:

- Basim al-Tousi, Political Perception of Sources of Threat to Arab National Security: A Jordanian Viewpoint, *Al-Mustaqbal al-arabi, Issue 231, 1998.
- Abdel Karim Darwich and Leila Takla, Principles of Public Administration, Egypt: Al-Maktaba Al-Inglouziyya Al-Misriyya, 1976.
- Abdelmonaim al-Mushat, 'Towards an Arabic Formulation of the Theory of National Security', Al-Mustaqbal al-Arabi, Issue 54.
- Ala Abd al-Razzaq al-Salimi, E-Government Administration, Jordan: Dar Wail Publishing, 2008.
- Al-Badr website on Cybernetics (or 'Goal-Oriented Self-Guidance through Mechanizing Thought'), http://www.albadr.org/www/doc/sitevisitors/3.doc.
- Doug (Doge) Gerrals, The Complete Guide for the Smart Ones: Investing through the Internet, trans. Tib Tub for Arabisation and Translation Services, Egypt: Dar al-Farouq Publishing and Distribution, 2001.
- Mohamed Maysar Fatih, 'The Strategy of U.S. National Security after the Events of 11 September 2001', Tikrit University Journal for Legal and Political Sciences, Vol. 5, Issue 17, 2013.
- Noura bint Mohammed al-Obayd, 'Digital Certificates... What Are They and Why Are They Important in Our Digital Lives?', Laha Online website, 12 September 2012.
- sabah Mahmoud Mohamed, Islamic Security—Studies in Geopolitical Challenges, sanaa: al-Jami'ah Institution for Studies and Publishing and Distribution, 1994.
- sedam al-Khaymayza, 'E-Government: The Path towards Administrative Reform', Jordan: Alam al-Kitab al-Hadith for Publishing and Distribution, 2013.
- The Regulatory Authority for Posts and Electronic Communications (or Posts, Landline and Wireless Communications), 'Electronic Authentication/Certification': Transmitted from the website of the Regulatory Authority, available at: The Regulatory Authority for Posts and Electronic Communications' Internet Market Observatory, June 2025: https://www.arpce.dz/ar/doc/int

- World Bank: Population growth in Algeria: Worldometer, Algeria population: https://www.worldometers.info/ar/algeria/
- Alaa al-Salimi, Othman al-Kilani and Hilal al-Bayati, Fundamentals of Management Information Systems, Amman.
- Atlas Magazine, 'Cybercrime on the rise in Algeria', 28/11/2024: https://www.atlas-mag.net/en/articles/cybercrime-rise-algeria-0
- Bara, S. (2017). 'Cyber Security' in Algeria: Policies and Institutions', Algerian Journal of Human Security, Issue 4, July 2017.
- Boukbacha Mohamed, 'Cyber Security and Defence': A Top Priority', The Army Journal, Issue 651, October 2017.
- Edward Amoroso, Cyber Security, Silicon Press, 2007.
- ESCWA Guidelines for Cyber Legislation (a project coordinating cyber legislation to promote a knowledge society in the Arab region), Beirut: ESCWA Publications, 2012, pp. 109–110 (available at: https://www.unescwa.org/sites/www.unescwa.org/files/page_attachments/directives-full.pdf).
- Fadila Aqali, 'Electronic Crime and the Procedures for Confronting It through Algerian Legislation', paper presented at the International Conference on Cybercrime, Jil Research Center, Tripoli, Lebanon, 2017.
- Fatih al-Nour Rahmoun, 'Lectures on Strategy and International Security', delivered to Master's students in Political Science at the University of M'sila, 2017–18.
- Hayla Abd al-Hamid al-Hafiz, 'Challenges Facing Cyber Security', Journal of Humanities and Natural Sciences, Islamic University of Lebanon, Vol. 6, Issue 7, 2025.
- Imad Abi Shannab, 'E-Government Projects between Theory and Practice', Egypt: Arab Administrative Development Organisation, 2010.
- Internet World Stats, 'Algerian Internet Usage and Population Growth': http://bit.ly/2lR3OIo
- Karrar Ali Mahtouf, 'The Development of the Concept of National Security after the Cold War', Wasit Journal of Human Sciences, Vol. 11, Issue 32, 2016.
- Lynor Martin, 'Turkish National Security in the Middle East', trans. Khalil Ali Mourad, Regional Affairs Series, Issue 3, Regional Studies Centre, University of Mosul, 2005.
- Ministry of Posts, Landline and Wireless Communications, 'Numbers and Indicators 2025': https://www.mpt.gov.dz/%d8%a3%d8%b1%d9%82%d8%a7%d9%85%d9%88%d9%85%d8%a4%d8%b4%d8%b1%d8%a7%d8%aa
- Mohamed Dhaher Watar, Administrative Strategy, 2nd ed., Beirut: Muassasat al-Risala, 1980.
- Mohamed Hasan Omar, Administration and Technology: Partners in Confronting the Challenges of the Internet Age, Jordan: al-Fallāḥ Library for Publishing and Distribution, 1997.
- Mouna al-Ashqar Jabour, Cybernetics: The Obsession of the Era, Beirut: Arab League University, Arab Center for Legal and Judicial Research, 2016.
- Naim Ibrahim al-Zahir, 'The Path to E-Government: A Comprehensive Vision*, Jordan: Alam al-Kitab al-Hadith for Publishing and Distribution, 2014.
- Ousama al-Khouly et al., The Arabs and the Information Revolution, Lebanon: Center for Arab Unity Studies, 2005.

- Oussama Ahmad al-Manaisa and Jalal Mohamed al-Zouabi, the previously cited reference.
- People's Democratic Republic of Algeria, Presidential Decree No. 04-183, establishing the National Institute of Forensic Evidence and Criminalistics for the National Gendarmerie and determining its basic statute (dated 26 June 2004), Official Gazette, Issue 41 (issued 27 June 2004).
- People's Democratic Republic of Algeria, Law No. 09-04 dated 5 August 2009 containing special provisions for preventing and combatting crimes related to information and communication technologies, Official Gazette, Issue 47, 16 August 2009.
- Saghir, Y. (2013). Crime Committed via the Internet. Master's Thesis in Political Science. Mouloud Mammeri University of Tizi Ouzou.
- Samira Njoya, 'Algeria adopts 2025–2029 national cybersecurity strategy', Wearetech. africa, 05/03/2026.
- Souleiman Abd Allah al-Harbi, 'The Concept of Security: Its Levels, Forms and Threats (A Theoretical Study of Concepts and Frameworks)', Arab Journal of Political Science, Issue 19, 2008.
- The same definition can be found in Law No. 15-04, dated 1 February 2015 and published in the Official Gazette (Issue 6, p. 7), which specifies the general rules relating to electronic signatures and certifications. It can also be found in Law No. 26-02, dated 17 February 2026 and published in the Official Gazette (Issue 14, p. 7, Article 2), which specifies the general rules relating to trust services for electronic transactions and electronic identification.
- Translated/adapted from the book E-Government between Theory and Practice by Oussama Ahmad al-Mana'isa and Jalal Mohamed al-Zouabi, Jordan: Dar al-Thaqafa Publishing and Distribution, 2013.

Footnotes:

[1]-Mohamed Dhaher Watar, Administrative Strategy, 2nd ed., Beirut: Muassasat al-Risala, 1980, p. 737.
- Abdel Karim Darwich and Leila Takla, Principles of Public Administration, Egypt: Al-Maktaba Al-Inglouziyya Al-Misriyya, 1976, pp. 255–257.
Mohamed Hasan Omar, Administration and Technology: Partners in Confronting the Challenges of the Internet Age, Jordan: al-Fallāḥ Library for Publishing and Distribution, 1997, pp. 47–48.
-And the Wikipedia website: Cybernetics: http://ar.wikipedia.org/wiki/%D8%B3%D9%8A%D8%A8%D8%B1%D9%86%D9%8A%D8%B7%D9%8A%D9%82%D8%A7

[2]- For further details, see also: Ousama al-Khouly et al., The Arabs and the Information Revolution, Lebanon: Center for Arab Unity Studies, 2005, pp. 13–16.
Abdul Karim Darwish and Laila Takla, Principles of Public Administration, Egypt: Anglo-Egyptian Library, 1976, pp. 255-257.
- Muhammad Hassan Omar, Management and Technology: Partners in Facing the Challenges of the Internet Age, Jordan: Al-Falah Library for Publishing and Distribution, 1997, pp. 47-48.
- And the Wikipedia Cybernetics website.
http://ar.wikipedia.org/wiki/%D8%B3%D9%8A%D8%A8%D8%B1%D9%86%D9%8A%D8%B7%D9%8A%D9%82%D8%A7
- Al-Badr website on Cybernetics or purposeful self-leadership through the automation of thought

[3]- Alaa Al-Salmi, Othman Al-Kilani, and Hilal Al-Bayati, Fundamentals of Management Information Systems, Amman: Dar Al-Manahij for Publishing and Distribution, 2006, p. 21.

[4]- Ammar Ahmed Abu Shanab, E-Government: A Tool for Democracy and Community Development, Egypt: Publications of the Arab Organization for Administrative Development, League of Arab States, 2012, pp. 166-170.

[5]- Mouna al-Ashqar Jabour, Cybernetics: The Obsession of the Era, Beirut: Arab League University, Arab Center for Legal and Judicial Research, 2016, p. 25.

[6]- Edward Amoroso, Cyber Security, Silicon Press, 2007, p. 1.
[7]- ESCWA Guidelines for Cyber Legislation (a project coordinating cyber legislation to promote a knowledge society in the Arab region), Beirut: ESCWA Publications, 2012, pp. 109–110 (available at: https://www.unescwa.org/sites/www.unescwa.org/files/page_attachments/directives-full.pdf).
[8]- Same reference as above, p. 110.
[9]- Abdelmonaim al-Mushat, 'Towards an Arabic Formulation of the Theory of National Security', Al-Mustaqbal al-Arabi, Issue 54, p. 10.
[10]- Basim al-Tousi, Political Perception of Sources of Threat to Arab National Security: A Jordanian Viewpoint, *Al-Mustaqbal al-arabi, Issue 231, 1998, p. 86.
[11]- sabah Mahmoud Mohamed, Islamic Security—Studies in Geopolitical Challenges, sanaa: al-Jami'ah Institution for Studies and Publishing and Distribution, 1994, p. 8.
[12]- Mohamed Maysar Fatih, 'The Strategy of U.S. National Security after the Events of 11 September 2001', Tikrit University Journal for Legal and Political Sciences, Vol. 5, Issue 17, 2013, p. 265.
[13]- Lynor Martin, 'Turkish National Security in the Middle East', trans. Khalil Ali Mourad, Regional Affairs Series, Issue 3, Regional Studies Centre, University of Mosul, 2005, p. 5.
[14]- Naim Ibrahim al-Zahir, 'The Path to E-Government: A Comprehensive Vision*, Jordan: Alam al-Kitab al-Hadith for Publishing and Distribution, 2014, p. 81.
[15]- Karrar Ali Mahtouf, 'The Development of the Concept of National Security after the Cold War', Wasit Journal of Human Sciences, Vol. 11, Issue 32, 2016, pp. 431–432.
[16]- Souleiman Abd Allah al-Harbi, 'The Concept of Security: Its Levels, Forms and Threats (A Theoretical Study of Concepts and Frameworks)', Arab Journal of Political Science, Issue 19, 2008, p. 10.
[17]- Fatih al-Nour Rahmoun, 'Lectures on Strategy and International Security', delivered to Master's students in Political Science at the University of M'sila, 2017–18, p. 5.
[18]- Imad Abi Shannab, 'E-Government Projects between Theory and Practice', Egypt: Arab Administrative Development Organisation, 2010, pp. 178–181.
[19]- Naim Ibrahim al-Zahir, The Previously Cited Reference, pp. 94–95.
[20]- Same reference, p. 95.
[21]- Same reference, pp. 96–97.
[22]- Oussama Ahmad al-Manaisa and Jalal Mohamed al-Zouabi, the previously cited reference, p. 194.
[23]- Hayla Abd al-Hamid al-Hafiz, 'Challenges Facing Cyber Security', Journal of Humanities and Natural Sciences, Islamic University of Lebanon, Vol. 6, Issue 7, 2025, p. 730.
[24]- Same reference as above, p. 80.
[25]- Tarek al-Majdhoub, the previously cited reference, p. 925.
[26]- Ala Abd al-Razzaq al-Salimi, E-Government Administration, Jordan: Dar Wail Publishing, 2008, pp. 305–309.
[27]- Compiled by the researcher according to the review.
[28]- sedam al-Khaymayza, 'E-Government: The Path towards Administrative Reform', Jordan: Alam al-Kitab al-Hadith for Publishing and Distribution, 2013, p. 121.
[29]- Doug (Doge) Gerrals, The Complete Guide for the Smart Ones: Investing through the Internet, trans. Tib Tub for Arabisation and Translation Services, Egypt: Dar al-Farouq Publishing and Distribution, 2001, p. 279.
[30]- Sedam al-Khaymayza, The Previously Cited Reference, pp. 122–123.
[31]- Noura bint Mohammed al-Obayd, 'Digital Certificates... What Are They and Why Are They Important in Our Digital Lives?', Laha Online website, 12 September 2012; available at: http://www.lahaonline.com/articles/view/41544.htm
[32]- The Regulatory Authority for Posts and Electronic Communications (or Posts, Landline and Wireless Communications), 'Electronic Authentication/Certification': Transmitted from the website of the Regulatory Authority, available at: http://www.arpt.dz/ar/gd/ce/.
[33]- Translated/adapted from the book E-Government between Theory and Practice by Oussama Ahmad al-Mana'isa and Jalal Mohamed al-Zouabi, Jordan: Dar al-Thaqafa Publishing and Distribution, 2013, pp. 180–181.
[34]- The same definition can be found in Law No. 15-04, dated 1 February 2015 and published in the Official Gazette (Issue 6, p. 7), which specifies the general rules relating to electronic signatures and certifications. It can also be found in Law No. 26-02, dated 17 February 2026 and published in the Official Gazette (Issue 14, p. 7, Article 2), which specifies the general rules relating to trust services for electronic transactions and electronic identification.
[35]- Amar Ahmad Abo Shannab (previously cited reference, p. 184).
[36]- Sedam al-Khaymayza, previously cited, p. 124.
[37]- Several statistics were relied upon, including:
- National Office of Statistics
Internet World Stats, 'Algerian Internet Usage and Population Growth': http://bit.ly/2lR3OIo

The Regulatory Authority for Posts and Electronic Communications' Internet Market Observatory, June 2025: https://www.arpce.dz/ar/doc/int
Worldometer, Algeria population: https://www.worldometers.info/ar/algeria/
World Bank: Population growth in Algeria: https://data.albankaldawli.org/indicator/SP.POP.GROW?locations=DZ

[38]- Ministry of Posts, Landline and Wireless Communications, 'Numbers and Indicators 2025': https://www.mpt.gov.dz/%d8%a3%d8%b1%d9%82%d8%a7%d9%85%d9%88%d9%85%d8%a4%d8%b4%d8%b1%d8%a7%d8%aa

[39]- Datareportal, Digital 2026: Algeria: https://datareportal.com/reports/digital-2026-algeria?rq=algeria

[40]- Samira Njoya, 'Algeria adopts 2025–2029 national cybersecurity strategy', Wearetech.africa, 05/03/2026. https://www.wearetech.africa/en/fils-uk/news/tech/algeria-adopts-2025-2029-national-cybersecurity-strategy

[41]- Atlas Magazine, 'Cybercrime on the rise in Algeria', 28/11/2024: https://www.atlas-mag.net/en/articles/cybercrime-rise-algeria-0

[42]- Boukbacha Mohamed, 'Cyber Security and Defence': A Top Priority', The Army Journal, Issue 651, October 2017, p. 35.

[43]- Bara, S. (2017). 'Cyber Security' in Algeria: Policies and Institutions', Algerian Journal of Human Security, Issue 4, July 2017, p. 435.

[44]- People's Democratic Republic of Algeria, Law No. 09-04 dated 5 August 2009 containing special provisions for preventing and combatting crimes related to information and communication technologies, Official Gazette, Issue 47, 16 August 2009.

[45]- Saghir, Y. (2013). Crime Committed via the Internet. Master's Thesis in Political Science. Mouloud Mammeri University of Tizi Ouzou.

[46]- People's Democratic Republic of Algeria, Presidential Decree No. 04-183, establishing the National Institute of Forensic Evidence and Criminalistics for the National Gendarmerie and determining its basic statute (dated 26 June 2004), Official Gazette, Issue 41 (issued 27 June 2004).

[47]- Fadila Aqali, 'Electronic Crime and the Procedures for Confronting It through Algerian Legislation', paper presented at the International Conference on Cybercrime, Jil Research Center, Tripoli, Lebanon, 2017, p. 115.