Erriwak: Journal of Social and Human Studies | ISSN: 2437 - 0363 EISSN: 2602-6767 | Volume: 12 / N°: 01 (2026), p 65-85

Cyber security as a Pillar of Digital Sovereignty: A Legal Analysis of Algeria's National Strategy for Information Systems Security 2025–2029

Bouchria Fatima,

Department of Law, Ahmed Zabana University, Relizane, fatima.bouchria@univ-relizane.dz

Received: 16/03/2026 Accepted: 18/04/2026 Published: 05/06/2026

Abstract:

The rapid development of information and communication technologies has led to the emergence of new security challenges related to the protection of information systems and digital data. In light of the digital transformation experienced by states, cyber security has become one of the fundamental pillars for safeguarding the strategic interests of the state and ensuring the continuity and sustainability of public services. In this context, Algeria has recently adopted the National Strategy for Information Systems Security for the period 2025–2029, with the aim of strengthening the security of the national cyberspace and building an integrated system for protecting digital infrastructure through the establishment of legal frameworks and clarifying their role in reinforcing the state's digital sovereignty.

Keywords: Cyber security; Digital Sovereignty; Information Systems; National Strategy; Digital Infrastructure.

* **Bouchria Fatima**

1. INTRODUCTION

Over the past decades, the world has witnessed profound transformations as a result of the rapid development of information and communication technologies. This evolution has led to the emergence of a digital space that has become a new arena for conducting economic and even political activities. This transformation has also contributed to the transfer of many state functions into the digital environment, whether through e-government, digital public services, or the information systems upon which institutions rely to manage their various activities. Although this transition offers significant opportunities to enhance efficiency and transparency, it has simultaneously generated new legal and security challenges, mainly related to the protection of information systems and digital data from various cyber threats.

In this context, the concept of security is no longer limited to its traditional dimensions associated with protecting borders or ensuring internal stability. It now also encompasses the protection of cyberspace, which has become one of the essential components of national security for states. Cyber-attacks targeting information systems can lead to the disruption of public services or affect critical infrastructure, making the security of information systems both a strategic and a legal issue. These developments have prompted many countries to adopt national cyber security strategies aimed at protecting digital space and strengthening the capacity of institutions to address the risks associated with it. (Khalf, 2021 ,p.21)

From this perspective, the concept of cyber security has emerged as a comprehensive framework that encompasses a set of technical, organizational, and legal measures aimed at protecting networks, information systems, and data from intrusion, sabotage, or unauthorized use. This concept is not limited to the technical dimension alone; it also extends to include the legal and institutional aspects that regulate the responsibilities of various actors involved in the protection of digital space. Therefore, cyber security today has become one of the fields where law and technology clearly intersect, as effective protection

of information systems requires the development of legal rules capable of keeping pace with rapid technological developments. (Yahia, 2023,p. 86)

With the increasing reliance on digital technology across various vital sectors, the concept of digital sovereignty has also emerged. It refers to the ability of a state to control the data and digital infrastructure located within its territory and to ensure the independence of its technological decision-making. This concept has gained growing importance in light of the increasing challenges related to the protection of states' strategic data, particularly with the expanding influence of major technology companies and their control over a large part of the global digital infrastructure. In this context, achieving digital sovereignty has become one of the main objectives of public policies related to digital transformation, given its close connection with the protection of national security and the strategic interests of the state. (Arpagian, 2022,p. 21)

In Algeria, with the acceleration of the digitalization process affecting various administrative and economic sectors, the need has emerged to establish a strategic framework aimed at strengthening the security of information systems and ensuring their protection against cyber risks. In this context, the National Strategy for Information Systems Security for the period 2025–2029 was adopted as a reference document that defines the state's general orientations in the field of protecting cyberspace and enhancing its capacity to address digital threats. This strategy seeks to build an integrated cyber security system based on strengthening institutional governance, developing mechanisms for prevention and response to cyber incidents, and supporting national capacities in protecting sensitive digital infrastructure. (National Strategy for Information Systems Security 2025–2029, Information Systems Security Agency, 2025, p.5)

However, the adoption of this new strategy raises several legal questions regarding its ability to establish an effective framework for protecting information systems and

strengthening the state's digital sovereignty, particularly in light of the continuous evolution and transnational nature of cyber threats. It also raises the issue of the relationship between the strategic dimension of cyber security and the legislative framework governing cybercrime and data protection. This necessitates analyzing the legal dimensions of this strategy and assessing the extent of its contribution to strengthening digital security in Algeria. Accordingly, this study raises an important research question: To what extent does the National Strategy for Information Systems Security (2025–2029) contribute to strengthening the legal framework for protecting the digital sovereignty of the Algerian state?

2. The Regulatory and Institutional Framework for Information Systems Security Governance within the National Strategy 2025–2029

The rapid development of information and communication technologies has led to the emergence of new challenges affecting the security of states' information systems. Cyberspace has become a vital domain where economic, security, and sovereign interests intersect.

In response, Algeria has moved toward developing a comprehensive legal, legislative, and regulatory framework for the governance of information systems security. This has been reflected in the enactment of several legal texts and the establishment of specialized institutional bodies. In addition, the National Cyber security Strategy 2025–2029 has been adopted as a guiding framework aimed at strengthening the state's digital sovereignty and enhancing its capabilities in the field of information systems security.

2.1. Legal Foundations for Organizing Information Systems Security in Algeria

One of the key objectives outlined by the National Strategy for Information Systems Security is to ensure national cyber resilience by strengthening preventive, detection, and incident response capabilities to support Algeria's digital transformation (National Strategy for Information Systems Security 2025–2029, Information Systems Security Agency, 2025, p.4), while also safeguarding national digital sovereignty. Achieving this, of course, requires a

robust legal arsenal that guarantees and enforces these objectives.

Amendments to the Algerian Penal Code have introduced a range of offenses related to attacks on information systems or their exploitation in committing crimes. This reflects the orientation of Algeria's criminal policy toward enhancing legal protection of cyberspace and keeping pace with rapidly evolving technological transformations. (Bousquia, 2022 ,p. 312)

2.1.1. Law No. 09-04 on Special Rules for the Prevention and Combating of Crimes Related to Information and Communication Technology

Law No. 09-04, dated August 5, 2009, which establishes special rules for the prevention and combating of crimes related to information and communication technology, is one of the most important legal texts forming the legislative foundation for combating cybercrime in Algeria. Through this law, the legislator set out a series of legal provisions aimed at criminalizing acts that compromise the integrity of information systems, such as unauthorized access to an information system, disrupting its operation, or damaging stored digital data.

The law also grants judicial and security authorities specific powers for investigating and collecting digital evidence, thereby strengthening the investigation of information-related crimes. (Bougfa, 2021, p. 85)

This law also established a set of preventive and procedural measures, the most important of which include electronic monitoring, collaboration with service providers to prevent cybercrimes, as well as the inspection, seizure, and recording of information systems to protect public order and support necessary investigations and inquiries. (law 09-04**,** Article 07)

Furthermore, the law expanded the jurisdiction of Algerian courts to cover crimes related to information and communication technology committed outside the national territory, in cases where they are perpetrated by foreigners and target Algerian state

institutions, national defense, or strategic economic interests. It also opened the door for international judicial cooperation in this field.

Additionally, Law No. 09-04 established the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technology. (Mehdi, 2021, p. 120)

2.1.2. Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data

Algeria strengthened its legislative framework for information systems security with Law No. 18-07, dated June 10, 2018, concerning the protection of natural persons in the processing of personal data. This law aims to safeguard individuals' privacy in the digital environment and to regulate the collection and processing of personal data. It establishes several fundamental principles, including the legality of processing and data security, and created an independent national authority responsible for monitoring compliance by organizations and institutions with legal rules on personal data protection. (Loukal, 2019, p . 1316)

The key points of this law can be summarized as follows:

-Establishment of a national authority for the protection of personal data.

-Imposition of a set of obligations on the entity responsible for the automated processing of personal data.

-Qualification of supervisory officers to conduct investigations and inspections of offenses related to personal data under the supervision of the Public Prosecutor.

-Any individual whose rights under this law are violated may request from the judicial authority any protective measures to prevent further infringement or to obtain compensation. (Mehdi, 2021, p. 122)

2.1.3. Presidential Decree 20-05 on Establishing a National System for Information Systems Security

To strengthen and protect information systems, Presidential Decree No. 20-05, dated 20 Jumada al-Awwal 1441 AH (corresponding to January 20, 2020), was issued to establish a national system for information systems security. This decree is among the most important regulatory texts adopted by Algeria in the field of digital space protection. It was introduced in the context of rapid digital transformations and the increasing threats related to cybercrime and cyber-attacks, which may target public institutions and agencies. (Sonia Makri,Walid Ben Laamer, 2025,p. 132)

The decree aims to create a national institutional framework responsible for organizing and coordinating efforts to protect the state's information systems. This is achieved through the establishment of a national system tasked with developing the general policy for information security and monitoring its implementation at the national level. This approach reflects the authorities' recognition of the importance of transitioning from a purely punitive approach to cybercrime to a comprehensive institutional approach based on prevention and coordination among all relevant entities responsible for protecting cyberspace.

In this context, the decree establishes a national system for information systems security comprising a set of bodies responsible for guiding the national policy in this field and coordinating its implementation. This system is tasked with developing strategic directions for the protection of information systems and monitoring their execution across the state's critical sectors. This organization reflects a move toward establishing national cyber security governance based on coordination between specialized security and technical institutions. (Kheira Abdessadok, Amal Boulghab, 2021, pp. 374–376)

The significance of Presidential Decree No. 20-05 lies in its role as the regulatory

framework underpinning the National Cyber security Strategy, defining the institutional structures responsible for developing national policies in information security and coordinating their implementation. The decree aims to strengthen the state's capabilities in protecting digital infrastructure and to develop mechanisms for preventing cyber risks. (Sonia Makri,Walid Ben Laamer, 2025, p. 134)

Furthermore, the importance of Decree 20-05 is highlighted by its direct alignment with the axes of the National Strategy for Cyber Systems Security 2025–2029, particularly in enhancing digital trust and securing electronic transactions. The strategy emphasizes the need to develop a legal and regulatory framework that ensures the security of digital services and fosters confidence in the digital economy, which is clearly reflected in the provisions of the aforementioned presidential decree.

This law also intersects with another axis of the strategy, namely the protection of digital infrastructure and the enhancement of information systems security. It requires entities responsible for electronic certification services to adopt strict security standards to safeguard the information systems used in managing electronic certificates, thereby helping to reduce the risks associated with cyber-attacks targeting sensitive digital infrastructure.

Additionally, Decree 20-05 contributes to supporting the digital transformation of public administration and strengthening e-governance, which is one of the core objectives of the National Strategy for Information Systems Security. The strategy aims to develop digital services while ensuring their security simultaneously. ((ITU), 2022, p.41)

Despite the importance of these legal texts in organizing the field of cyber security, other related laws, such as Law No. 15-04 on Electronic Certification and Signatures and Law No. 18-05 on E-Commerce, as well as amendments to the Algerian Penal Code and Code of Criminal Procedure, play a role in this domain. However, some scholars argue that the Algerian regulatory framework remains incomplete, as cyber security rules are spread across multiple laws. This fragmentation may affect the effectiveness of their application, especially

in light of rapid technological advancements and the emergence of new types of cybercrime. (Baali, 2020, p. 214)

2.2. The Institutional Framework Responsible for Implementing the National Strategy 2025–2029

The success of the National Cyber security Strategy does not depend solely on establishing a legislative framework to regulate the protection of cyberspace, but also on the presence of an institutional structure capable of implementing this general policy and ensuring coordination among all relevant entities. In this context, Algeria adopted, within the National Strategy for Information Systems Security 2025–2029, a multi-level institutional approach based on the distribution of responsibilities between strategic bodies tasked with guiding national cyber security policy and technical and operational bodies responsible for its practical implementation.

2.2.1. Strategic Bodies Responsible for Guiding the National Policy for Information Systems Security

Presidential Decree No. 20-05 established a set of bodies tasked with defining strategic directions for the protection of information systems, within the framework of the National System for Information Systems Security. This organizational structure aims to ensure coordination among various institutions involved in cyber security and to enhance the effectiveness of responses to digital threats. (Sonia Makri,Walid Ben Laamer,2025, p.131)

Among the most important of these bodies is the National Authority for Information Systems Security, which plays a central role in guiding national information security policy. It is responsible for proposing national strategies for the protection of information systems, monitoring their implementation, and coordinating across different sectors and institutions involved in safeguarding cyberspace. (National Strategy for Information Systems Security 2025–2029, Information Systems Security Agency, 2025, p.2)

This authority also establishes general guidelines for information systems security and oversees the compliance of national institutions with the adopted standards, reflecting the emphasis on coordination among digital actors. (Kheira Abdessadok, Amal Boulghab, 2021, p. 375)

Additionally, the National Strategy for Information Systems Security 2025–2029, under the aforementioned Decree 20-05, provides for the establishment of the National Council and the National Agency for Information Systems Security. (National Strategy for Information Systems Security 2025–2029, Information Systems Security Agency, 2025, p.2)

The National Council for Information Systems Security represents the highest advisory and strategic body within Algeria's national information security system. It was established as a senior authority aimed at guiding national policy and ensuring coordination among the various institutions responsible for protecting the state's information systems. Its main role is to set the general strategic directions for information security, propose national policies for the protection of critical digital infrastructure, assess cyber risks at the national level, and provide recommendations to senior authorities on best practices to safeguard the state's digital space. (Sonia Makri,Walid Ben Laamer, 2025, p. 132)

The council's work is based on the principle of multi-level cyber governance, coordinating between ministries and national bodies to ensure integration and strategic oversight. Its importance is highlighted within the National Strategy for Information Systems Security 2025–2029, as it serves as the supreme pillar through which national policies are determined and all efforts are directed toward achieving optimal digital protection. (Kheira Abdessadok, Amal Boulghab, 2021, pp. 374–375)

2.2.2. Technical and Operational Bodies Responsible for Implementing the National Strategy 2025–2029

Presidential Decree 20-05 also established a set of technical bodies tasked with implementing practical measures for the protection of information systems. This

organizational structure aims to enhance the state's technical capabilities in preventing cyber-attacks and responding to information system incidents.

The mission of these bodies includes monitoring the security of information systems within public institutions, providing technical support for cyber risk prevention and mitigation, and playing a key role in developing mechanisms for detecting cyber-attacks and strengthening incident response capabilities to protect the state's sensitive digital systems.

In this context, these technical bodies serve as the executive instruments that operationalize the directions set forth in the National Strategy for Information Systems Security 2025–2029. They contribute to implementing policies related to the protection of digital infrastructure across all vital sectors of the state.

Among the most important of these operational technical bodies is the National Agency for Information Systems Security, which acts as the primary executive authority within the national information security system. It was established to implement the policies and plans set by the National Council for Information Systems Security and to ensure the protection of digital infrastructure. This aligns with the objectives of the National Strategy for Information Systems Security 2025–2029, operating under the supervision of the Ministry of National Defense to safeguard the state's information space and enforce the nationally adopted policies in this domain.

In this context, the Agency plays essential roles that complement the strategic and primary functions of the National Council for Information Systems Security, focusing directly on the following:

-Implementing national technical policies for the protection of information systems in government administrations and institutions based on general strategic guidelines. (Sonia Makri,Walid Ben Laamer, 2025, pp. 134–136)

-Coordinating cyber incident response mechanisms and managing breaches targeting the

state's sensitive systems, ensuring rapid intervention and recovery. (Hizam, 2020, pp. 179)

-Supporting ministries and technical institutions in applying information security requirements, preparing analytical risk assessments, and monitoring the implementation of cyber security programs. (Sonia Makri,Walid Ben Laamer, 2025, p. 137)

Through these functions, the agency works in coordination with other bodies within the national system, assuming the practical and technical aspects of implementing the National Strategy for Information Systems Security 2025–2029. This makes it a cornerstone for ensuring information security and for the effective practice of digital protection in Algeria. (Hizam, 2020, pp. 177–179)

3. Mechanisms for Protecting Cyberspace and Enhancing Digital Resilience under the National Strategy

Implementing the National Strategy for Information Systems Security does not only require defining general directions, but also necessitates adopting a set of technical and regulatory measures that allow its activation on the ground. This is especially important regarding the protection of digital infrastructure, strengthening capabilities to detect cyber-attacks, and developing risk management mechanisms related to the use of information systems. In this context, the national strategy also emphasizes the need to enhance coordination among various actors in the field of cyber security, both at the national and international levels.

3.1. Technical and Regulatory Measures to Activate the National Strategy for Information Systems Security

Implementing the National Strategy for Information Systems Security requires adopting a set of technical and regulatory measures aimed at strengthening the protection of the national cyber information space. These measures fall within a comprehensive approach based on preventing cyber risks, early detection of threats, developing national capacities in this field, and ensuring national and international cooperation to achieve the objectives of

the national strategy.

3.1.1. Protection of Digital Infrastructure and Sensitive Information Systems

Protecting digital infrastructure is one of the most important priorities pursued by the National Strategy for Information Systems Security, given the critical role that information systems play in managing various economic and administrative sectors in the state. This infrastructure includes a range of systems and networks relied upon by government institutions and vital sectors such as telecommunications, energy, and the financial sector. (Boudraa, 2019**,** p. 48)

In this context, the national strategy seeks to enhance the protection of national information systems by relying on technical measures aimed at securing government networks and sensitive databases. It also emphasizes the need to develop information security standards within government institutions to ensure the integrity of their digital systems and to reduce the risks of cyber-attacks that threaten the state's digital infrastructure. (Sonia Makri,Walid Ben Laamer, 2025, p. 133)

Securing the state's digital infrastructure requires adopting advanced mechanisms for monitoring and analyzing potential cyber threats. This enables the identification of vulnerabilities within digital information systems and the implementation of appropriate preventive measures, aligning with the directions set forth by the National Strategy for Information Systems Security. (Khodir, 2022 , p. 90)

3.1.2. Developing Early Detection Mechanisms and Response to Cyber Incidents

The National Strategy for Information Systems Security emphasizes the importance of developing mechanisms for the early detection of cyber-attacks and responding to them, as the speed of detecting and addressing these threats is a fundamental factor in mitigating their impact. Accordingly, the state seeks to adopt advanced systems for monitoring information networks and analyzing digital data to identify suspicious activities that may

indicate the occurrence of cyber-attacks.

In this context, cyber-attack detection mechanisms rely on a set of advanced technologies that allow for analyzing data traffic within information networks and identifying abnormal patterns that may signal digital threats. These systems also contribute to enhancing the national capacity to respond to cyber incidents by enabling competent authorities to implement appropriate technical measures to counter cyber-attacks in a timely manner. (Hizam, 2020, pp. 178–179)

These measures fall within the general directions of the National Strategy for Information Systems Security, which aims to raise the national readiness to face cyber risks. This is achieved through the development of early monitoring systems and the enhancement of digital incident response mechanisms, ensuring the protection of information systems and the continuity of their operation. (National Strategy for Information Systems Security 2025–2029, Information Systems Security Agency, 2025, p. 07)

3.1.3. Developing National Capacities to Confront Cyber Threats

Developing human and technical capacities is one of the fundamental pillars of the National Strategy for Information Systems Security. Addressing cyber threats requires specialized competencies capable of handling the technical challenges related to protecting information systems. Accordingly, the strategy emphasizes the importance of investing in human resource training and developing national expertise in the field of cyber security.

In this context, the state works to support specialized training programs in the field of information systems security and to encourage scientific research in the domain. It also seeks to strengthen cooperation between academic institutions and government bodies to develop the technical solutions necessary for protecting the national cyberspace. These efforts contribute to enhancing the country's autonomy in information security and reducing dependence on foreign technologies. (Khodir, 2022, p. 93)

The National Strategy for Information Systems Security also emphasizes the development of educational and training programs in higher education institutions to enhance professional capacities in technical fields related to cyber security. Several measures have been implemented in this regard in Algeria, including:

-Integrating cyber security disciplines into PhD and Master's programs in the Faculties of Law and Political Science, as well as in Media and Communication Sciences at several Algerian universities, including the University of Algiers 1 and the University of Constantine. (Boudraa, 2019, pp. 78–79)

-Establishing specialized vocational training programs in cyber security at professional training centers, such as the Center for Information and Communication Technology Training in Algiers, aimed at training national technicians on the latest digital protection tools. (Khodir, 2022, p. 94)

-Organizing specialized training courses and workshops in cooperation with international institutions, such as workshops organized by the Organization for Security and Co-operation in Europe (OSCE) on raising awareness of cyber threats for public sector employees. ((OSCE), 2023, pp.12-13)

-Supporting specialized diplomas in information security within departments of electrical engineering and computer technology, which strengthens a solid technical foundation that the state can rely on to implement the strategy.

-Encouraging peer-reviewed scientific publications in information security by funding Algerian researchers' participation in international conferences such as the CYBER SECURITY SYMPOSIUM, organized by academic institutions in collaboration with international technical entities, contributing to knowledge transfer and updating digital expertise. (Karim, pp. 47–48)

-Launching directed scientific research units in cyber security within accredited university

laboratories, such as the Information Systems Laboratories at the Faculty of Technical Sciences at the University of Oran, which conduct research on analyzing cyber threats and designing advanced technical solutions.

This link between the objectives of the national strategy and the axes of human and technical capacity development demonstrates that the Algerian state does not view building competencies merely as an organizational choice, but as a strategic investment essential for achieving long-term national cyber security. Every training or qualification program is directly aligned with the objectives and operational directions set forth in the strategy.

3.2. National and International Cooperation in the Field of Information Systems Security

Addressing cyber threats now requires a collective approach based on cooperation among various national and international actors, due to the cross-border nature of cybercrimes and cyber-attacks. The National Strategy for Information Systems Security has emphasized strengthening coordination mechanisms and highlighted the necessity of developing international partnerships for information exchange and technical expertise sharing. (Kara, 2021**,** p. 215)

3.2.1. National Cooperation among Institutions and Bodies Concerned with Information Systems Security

Algeria has sought to establish an institutional framework that ensures coordination among various entities responsible for protecting information systems. This was achieved by setting up a national cyber security system based on cooperation between regulatory bodies and specialized technical authorities, foremost among them the National Agency for Information Systems Security, which plays a pivotal role in this field by monitoring the implementation of information security standards within government institutions and providing them with technical support. (Boudraa, 2019, p. 134)

This coordination also includes a number of government sectors that rely heavily on information systems to perform their functions, such as the finance, telecommunications, and energy sectors. Protecting these sectors requires developing joint mechanisms for exchanging information on cyber threats and handling security incidents in a coordinated manner. (Cheikh, p. 88)

In this context, efforts are underway to develop a national system for exchanging information on digital threats among various government bodies. This enables the early detection of cyber-attacks and the coordination of responses. This mechanism contributes to enhancing protection levels within sensitive institutions, particularly those linked to the state's critical infrastructure, such as energy, telecommunications, and banking systems. (HARBI, 2021, p.210)

Similarly, major economic institutions-considered vital sectors, particularly in banking, energy, and telecommunications-are encouraged to establish specialized information security units responsible for monitoring information systems and detecting intrusion attempts. Cooperation between these institutions and the relevant government bodies is also strengthened through training programs and workshops aimed at raising awareness of cyber risks and developing employees' skills in this field. (JAHANKHANI, 2019 , p142)

Practically, this cooperation enhances institutions' capacity to confront digital threats by enabling the exchange of technical expertise and coordination of protective measures. This, in turn, improves the effectiveness of the national response to cyber attacks (Bouguerra, 2023, p. 173) and supports the implementation of the objectives of the National Strategy for Information Systems Security.

3.2.2. International Cooperation in the Field of Information Systems Security

The National Strategy for Information Systems Security 2025–2029 emphasizes the importance of developing international partnerships and exchanging technical expertise

with countries and international organizations to strengthen the state's capacity to prevent and respond effectively to cyber attacks (Cheikh, p. 92). Among the specialized international organizations that Algeria engages with in this field is the International Telecommunication Union, which provides support programs for countries in building technical capacities and developing national cyber security strategies. Algeria also participates in a number of international digital initiatives aimed at enhancing cyberspace security and information exchange. (HARBI, 2021,p. 214)

Algeria also collaborates in law enforcement, coordination, and investigation with international bodies specializing in combating cybercrime (Boudraa, 2019, p. 188). Furthermore, the country seeks to strengthen international judicial cooperation in this field through the exchange of legal assistance between states, which accelerates cybercrime investigations and facilitates the sharing of digital evidence. (JAHANKHANI, 2019, p167)

4. CONCLUSION

It is evident from the study of the National Strategy for Information Systems Security 2025–2029 that Algeria seeks to establish a comprehensive national framework aimed at enhancing the protection of the national digital space and addressing the increasing cyber threats. This approach has been manifested through the adoption of a set of legal, regulatory, and institutional mechanisms, alongside the establishment of specialized bodies and the development of national policies designed to secure information systems and strengthen their resilience against various digital risks.

The study also highlighted that the successful implementation of this strategy depends not only on the existence of legal and regulatory texts but also requires effective coordination among the different bodies and institutions involved in information security. Moreover, it necessitates the development of human and technical capacities capable of keeping pace with the rapid advancements in digital technology. In this context, national cooperation between government institutions and critical sectors forms a fundamental pillar

for ensuring the effectiveness of the adopted security policies, particularly given these sectors' increasing reliance on information systems to manage their activities.

On the other hand, international cooperation emerges as a complementary element to national efforts in the field of cyber security, given the cross-border nature of cyber threats and cybercrime. Consequently, Algeria seeks to develop partnerships with specialized international organizations and exchange technical expertise with various countries. Despite the efforts made in this domain, strengthening cyber security in Algeria requires the continued development of the legal and regulatory framework concerning the protection of information systems, as well as support for scientific research and specialized training in this field. Additionally, it is necessary to enhance the culture of information security within public and private institutions, ensuring the achievement of the objectives set by the National Strategy for Information Systems Security.

5. Bibliography List:

(ITU), I. T. (2022). National Cybersecurite Strategy Guide. Geneva: International Telecommunication Union (ITU).

(OSCE), O. f.-o. (2023). Cyber Awareness in North Africa, Training Report on Cybersecurity Capacity Building. Vienna, Austria.

09-04, L. N. (s.d.). pp. Article 07,.

National Strategy for Information Systems Security 2025–2029, Information Systems Security Agency. (2025). Algeria: Ministry of National Defense.

Arpagian, -N. (2022). La cybersécurité. Paris: presses de France.

Baali, M. E. (2020). Administrative Law and the Legal Regulation of Modern Technologies. Algeria: Dar Al-Ouloum Publishing.

Boudraa, M. E.-A. (2019). Criminal Protection of Information Systems in Algerian Legislation, . PhD Dissertation in Criminal Law, p. 48.

Bougfa, A. (2021). Cybercrime in Algerian Legislation. Algeria: Dar Houma Publishing House.

Bouguerra, A. (2023). The Role of National Policies in Strengthening Cybersecurity. Al-Bahith Journal for Legal and Political Studies(8), p. 173.

Bousquia, A. (2022). Concise Guide to Special Criminal Law (Vol. Part Two). Algeria: Dar Houma Publishing House.

Cheikh, A. B. (s.d.). Cybersecurity and Contemporary Legal Challenges. (U. o. 1, Éd.) Journal of Law and Political Science(14), p. 88.

HARBI, N. (2021). Cybersecurity governance and national strategies. Journal of cyber policy, 6(2).

Hizam, F. (2020). Protection of Digital Systems between Technical Mechanisms and Protection Agencies: A Reading of the Provisions of Presidential Decree No. 20-05. Journal of Law and Human Sciences, 123(3), pp. 172-179.

JAHANKHANI, H. (2019). Cyber security and information warfar. (S. o. computing, Éd.) p. 142.

Kara, A. (2021). Criminal Policy for Combating Cybercrime in Algerian Legislation. (M. K. Faculty of Law, Éd.) Journal of Legal Studies, 7(2), p. 215.

Karim, K. (s.d.). The Role of University Laboratories in Developing Cybersecurity. Journal of Information Technologies and Digital Security, pp. 47-48.

Khalf, A. (2021). Criminal Protection of Information Systems. Algeria: Dar Houma Publishing House.

Kheira Abdessadok, Amal Boulghab. (2021). The Legal Framework of Information Security. Journal of Research in Law and Political Science, same volume(2), pp. pp. 374–376.

Khodir, A. (2022). Information Security in Light of Contemporary Cyber Challenges. (U. o. Faculty of Law, Éd.) Journal of Legal Studies, 8(1), p. 90.

Loukal, M. (2019, Apri). International and National Legal Protection of Personal Data in the Digital Space in Light of the Data Protection Law 18-04. Journal of Legal and Political Sciences, 10(1), p. 1316.

Mehdi, R. (2021). Cybercrimes and the Mechanisms for Combating Them in Algerian Legislation. (Algeria, Éd.) Journal for Research and Studies, 6(2), p. 120.

Sonia Makri, Walid Ben Laamer. (2025). The National Information Systems Security Framework as an Institutional Mechanism for Combating Cybercrime in Accordance

with Presidential Decree No. 20-05. Journal of Research in Contracts and Business Law, 10(02), p. 132.

Yahia, M. B. (2023). Cybersecurity and the Challenges of Digital Sovereignty. (F. o. Science, Éd.) Journal of Legal Studies(2), 86.