*2026, Cilt 3, Sayı 4, 325-330*

OPEN ACCESS
***ISSN:*** 3062-262X

***Akademik Eğitim ve Sosyal Bilimler Dergisi (AJESS Journal)***

# *The Evolution of Algeria's National Cybersecurity Strategy: From Combating Cybercrime to Building Cyber Resilience and Digital Sovereignty*

Ali Mohammed (professor), University of Adrar Algeria. Ali.Mohammed@univ-adrar.edu.dz
DJAFOUR Islam, Associate Professor (Class A), Faculty of Law and Political Science, Mouloud Mammeri University of Tizi Ouzou, Algeria. islam.djafour@ummto.dz

**Article History**
Received: 27/02/2026; Accepted: 06/08/2026; Published: 08/09/2026

**Abstract:**
This study examines the trajectory of cybersecurity in Algeria from a perspective that goes beyond the traditional approach of limiting it to combating cybercrime, and instead considers it within the broader context of digital transformation and increasing dependence on networks. Greater digitalization simultaneously enhances institutional efficiency and increases exposure to cyber threats. Accordingly, the study focuses on the evolution of the concepts of cybersecurity and cybercrime, the Algerian legal and institutional framework, prevention, investigation, and response mechanisms, and the transformations introduced by the National Information Systems Security Strategy for 2025–2029. The study adopts a descriptive-analytical approach, complemented by an Algerian case study, drawing on national legislation, official documents, and relevant international standards. The findings show that Algeria has accumulated important elements of a national cybersecurity architecture, particularly in the legal, regulatory, and institutional domains. However, the transition toward sustainable cyber resilience remains dependent on strengthening technical capabilities, developing human capital, expanding research and innovation, consolidating a cybersecurity culture, and improving national and international cooperation. International indicators also suggest that Algeria's relative strength in the legal domain is accompanied by areas requiring further development, particularly technical and organizational capabilities, capacity building, and cooperation.

**Keywords**: cybersecurity; cyber resilience; cybercrime; digital sovereignty; information systems security; Algeria; digital governance.

**Introduction:**
Cyberspace has become an integral component of the infrastructure on which the modern state depends. Public administration, public services, the financial sector, telecommunications, health, energy, education, and supply chains all rely, to varying degrees, on interconnected information systems. Consequently, cyber disruption is no longer merely a technical problem; it can affect service continuity, public trust, economic performance, and national security (Attia, 2019; Zarouka, 2019).
These transformations coincide with the diversification of threat sources, including malware, phishing and fraud, identity and data theft, denial-of-service attacks, unlawful exploitation of vulnerabilities, influence campaigns, espionage, and attacks targeting critical infrastructure. Such threats evolve rapidly, some can be implemented at relatively low cost, and many transcend geographical borders. Consequently, approaches based solely on deterrence and punishment are insufficient (Ben Arabia, 2021; Bouzadia, 2019).
In Algeria, the issue is particularly important in light of the accelerating digital transformation. The state established a specific legal framework for preventing and combating crimes related to information and communication technologies through Law No. 09-04 of August 5, 2009. The institutional architecture concerned with cybersecurity has also developed. In March 2026, the Information Systems Security Agency of the Ministry of National Defence announced the publication of the National Information Systems Security Strategy for 2025–2029 as a comprehensive framework for national cyber resilience, protection

of digital infrastructure and data, continuity of essential public services, and strengthening trust in the digital environment (Ministère de la Défense Nationale – Algérie, 2026; Agence de Sécurité des Systèmes d'Information, 2026).

Against this background, the study addresses the following central question: To what extent has Algeria succeeded in moving from an approach centered on combating cybercrime toward a more comprehensive national approach based on prevention, risk management, resilience, and digital sovereignty?.

**Research Problem and Questions:**

The research problem lies in the tension between the expanding dependence on the digital environment and the increasing complexity of cyber threats. The central question gives rise to the following sub-questions:

- What is meant by cybersecurity and cybercrime, and what are the boundaries between the two concepts?
- How has the Algerian legal and institutional framework evolved to address digital threats?
- What are the principal prevention, detection, response, and investigation mechanisms adopted in Algeria?
- What does the National Information Systems Security Strategy for 2025–2029 add to the national cybersecurity architecture?
- What are the main challenges that continue to constrain the effectiveness of cybersecurity in Algeria?

**Research Hypothesis:**

The study proceeds from the hypothesis that the effectiveness of cybersecurity in Algeria is not determined solely by the existence of legal provisions and specialized institutions, but by the extent to which these elements are integrated with technical capabilities, governance, training, research and development, awareness, public–private cooperation, and international coordination.

**Methodology and Scope:**

The study adopts a descriptive-analytical approach because it permits the description of concepts, structures, and legislation and the analysis of the relationships among them. It also employs a case-study approach, treating Algeria as the unit of analysis. The material is based on the original research, with its concepts and formulation reconstructed and its section on the National Information Systems Security Strategy for 2025–2029 updated through the addition of recent institutional and international references. The study does not claim to statistically measure actual cyber incidents in Algeria, since such an undertaking would require detailed national databases and an independent measurement methodology.

**Section One: The Conceptual Framework of Cybersecurity and Cybercrime**

**1. Cybersecurity: From Technical Protection to Risk Management:**

Cybersecurity should not be reduced to antivirus software or firewalls. The contemporary concept is broader and encompasses policies, processes, human resources, and technologies intended to manage risks arising from the use of systems, networks, and data. The NIST Cybersecurity Framework (CSF) 2.0 emphasizes that cybersecurity should be managed as an enterprise risk and identifies six core functions: Govern, Identify, Protect, Detect, Respond, and Recover (National Institute of Standards and Technology [NIST], 2024; Rigopoulos et al., 2024).

Accordingly, cybersecurity is operationally defined in this study as an integrated system of governance and legal, regulatory, technical, and human measures aimed at reducing the risks posed by digital threats; protecting the confidentiality, integrity, and availability of information; ensuring the continuity of systems and services; and enabling the detection of, response to, and recovery from incidents.

This definition differs from narrow conceptions that equate cybersecurity with prevention. A mature cybersecurity system does not assume that every incident can be prevented; rather, it seeks to reduce the probability and impact of incidents, detect them rapidly, respond effectively, and restore essential functions (NIST, 2024).

**2. Dimensions of Cybersecurity:**

- Technical dimension: protecting networks, devices, applications, and data; managing vulnerabilities; authentication and encryption; and monitoring and responding to incidents.
- Organizational and governance dimension: allocating responsibilities, identifying risks, managing policies and standards, monitoring compliance, and measuring performance.
- Legal dimension: criminalizing unlawful acts; regulating investigation and electronic evidence; protecting data and privacy; and regulating digital transactions.
- Human dimension: developing specialized skills, providing continuous training, and raising awareness among employees and citizens, since human error represents an important pathway to risk exposure.
- Economic and strategic dimension: digital service disruption or data leakage can affect institutions, markets, trust, and digital autonomy.
- International dimension: because many attacks are cross-border, information sharing, mutual legal assistance, and police and technical cooperation form an integral part of cybersecurity.

**3. Cybercrime and Its Conceptual Approach:**

The literature uses several terms, including electronic crime, information crime, cybercrime, and computer and Internet crime. Methodologically, it is more precise to distinguish between crimes in which an information system is the direct target and crimes in which technology is used as a tool to commit a traditional or emerging criminal act (Chaib, 2022; Halder & Jaishankar, 2011).

Algerian Law No. 09-04 provides a functional framework for crimes related to information and communication technologies. It covers offenses affecting automated data-processing systems as well as other crimes committed or facilitated through an information system or electronic communications system (Law No. 09-04, 2009). This approach is significant because it does not restrict cybercrime to one category of conduct but links it to a technological means or information system.

Accordingly, the study operationally defines cybercrime as any conduct criminalized by law that targets an information system, data, a network, a person, or an institution through information and communication technologies, or that uses such technologies to facilitate the commission of a crime.

**4. Major Forms of Cybercrime:**

• Fraud, phishing, and theft of credentials.
• Unauthorized access to systems and databases.
• Distribution of malware and ransomware.
• Data and identity theft and violations of privacy.
• Extortion, defamation, cyberbullying, and threats through digital platforms.
• Attacks targeting websites, services, and infrastructure.
• Crimes involving unlawful content and child exploitation.
• Use of cyberspace to support organized crime, terrorist activities, or illicit financing.

5**. Characteristics of Cybercrime:**

Cybercrime is characterized by speed and scalability, the difficulty in some cases of linking conduct to an offender's identity, the absence of a conventional physical crime scene, and the possibility of distributing different stages of an offense across several countries. Electronic evidence is also susceptible to alteration or deletion, which requires precise rules for its collection, preservation, and analysis. Its cross-border nature makes international cooperation a practical necessity rather than a secondary option (Council of Europe, 2001; Halder & Jaishankar, 2011).

**Section Two: The Development of Cybersecurity in Algeria:**

**1. Legal and Legislative Framework:**

Law No. 09-04 of August 5, 2009, establishing special rules for the prevention of and fight against offenses connected with information and communication technologies, represents a cornerstone of Algeria's legal framework. It establishes specific rules concerning prevention, monitoring in legally defined circumstances, search, and seizure, thereby enabling judicial and investigative authorities to address the particular nature of electronic evidence (Law No. 09-04, 2009; Cheikh, 2020).

Algerian legislation has also developed toward regulating digital transactions and electronic signatures and certification, alongside provisions contained in the Penal Code and the Code of Criminal Procedure. This trajectory reflects a gradual shift from treating computer-related crime as an emerging phenomenon toward integrating it into the broader criminal justice system (Denden, 2020).

Nevertheless, legislative development must be accompanied by continuous updating of laws and procedures because the technologies used to commit crimes evolve more rapidly than the legislative cycle. The effectiveness of legal provisions is not measured by penalties alone, but also by the capacity of investigative and judicial authorities to obtain, analyze, and preserve the integrity of digital evidence.

**2. Institutional Architecture:**

Algeria's cybersecurity system includes multiple bodies whose roles intersect in prevention, investigation, and response. The original research addresses the national body responsible for preventing and combating crimes related to information and communication technologies, specialized services within the security and gendarmerie institutions, specialized judicial divisions, and awareness and international-cooperation functions. The development of a specialized national architecture for information-systems security further strengthens this trajectory. The Information Systems Security Agency of the Ministry of National Defence indicates that among its responsibilities is the preparation of components of the national strategy and the coordination of its implementation, reflecting a move toward more specialized and institutionalized governance (Agence de Sécurité des Systèmes d'Information, 2026).

**3. Prevention, Detection, and Response:**

Modern prevention is based on managing risks before an incident occurs rather than waiting for an incident and subsequently seeking the perpetrator. Prevention includes inventorying digital assets, classifying data, updating systems, managing privileges, training, maintaining backups, testing response plans, and monitoring unusual activity (NIST, 2024).

Detection relies on continuous monitoring of logs and events, analysis of indicators of compromise, and the use of security operations centers and analytical tools. Response involves containing the incident, investigating its source, reducing its impact, communicating with relevant authorities, restoring services, and analyzing lessons learned.

This cycle is particularly important for public institutions because protecting data alone is insufficient; continuity of essential services must also be ensured. This principle is consistent with the National Information Systems Security Strategy for 2025–2029, which emphasizes cyber resilience, protection of digital infrastructure, and continuity of essential public services (Ministère de la Défense Nationale – Algérie, 2026).

**4. Electronic Evidence and Investigation:**

Electronic evidence differs from traditional physical evidence in that it can be copied, modified, and transmitted across networks with relative ease. Cyber investigations therefore require procedures that preserve evidentiary integrity, document the manner in which evidence was obtained, establish its chain of custody, and prevent unauthorized alteration of data. Law No. 09-04 grants competent authorities powers relating to search, seizure, and restricting access to certain data under legally prescribed conditions (Law No. 09-04, 2009).

In practical terms, legislative development should be accompanied by investment in digital-forensics laboratories and the training of judges, judicial police officers, and specialists in digital forensic analysis.

**Section Three: The National Information Systems Security Strategy for 2025–2029**

The National Information Systems Security Strategy for 2025–2029 represents a qualitative stage in Algeria's cybersecurity trajectory. On March 3, 2026, the Ministry of National Defence announced that the first version of the strategy had been approved at the national level and that it constitutes a comprehensive framework for ensuring national cyber resilience, protecting the state's digital infrastructure and data, supporting digital transformation, protecting citizens, and strengthening trust in the digital environment (Ministère de la Défense Nationale – Algérie, 2026; Agence de Sécurité des Systèmes d'Information, 2026).

The strategy comprises four principal pillars: operational and technical capabilities; the legal, regulatory, and standards framework; training, research and development, improvement, and awareness; and national and international cooperation. This structure reflects a balanced conception of cybersecurity that does not treat technology as a substitute for law or human capacity, but rather integrates them within a single system.

**1. Operational and Technical Capabilities**

This pillar seeks to strengthen the protection of national systems and critical infrastructure and enhance capabilities for preventing, detecting, and responding to incidents. This priority is particularly important because public services and the economy increasingly depend on digital systems and because the attack surface expands as the number of connected devices and systems increases.

**2. Legal, Regulatory, and Standards Framework:**

This pillar seeks to provide an appropriate legal, regulatory, and standards framework for cyber resilience. It is not limited to criminalizing unlawful acts; it also requires clear security standards, defined responsibilities, risk management, and periodic policy review.

**3. Training, Research and Development, Improvement, and Awareness:**

The strategy places human resources at the center of national cybersecurity development. This is consistent with the fact that skills shortages can prevent institutions from benefiting from available technologies. Universities, research centers, and training institutions are therefore expected to produce expertise in network security, digital forensics, penetration testing, risk management, security governance, and artificial-intelligence security.

Training should also move beyond theoretical instruction toward practical exercises, simulation, and incident-response drills. This can build national expertise capable of handling incidents without excessive reliance on external expertise.

**4. National and International Cooperation:**

A state cannot build cybersecurity in isolation. Private institutions manage significant portions of digital infrastructure, universities produce knowledge, civil society contributes to awareness, and international partners provide channels for exchanging information and expertise. The cross-border nature of cybercrime also makes police, judicial, and technical cooperation essential.

The Budapest Convention on Cybercrime provides an international model for cooperation on criminalization, procedures, and electronic evidence, while its Second Additional Protocol focuses on strengthening international cooperation and disclosure of electronic evidence (Council of Europe, 2001).

**Section Four: Assessment of the State of Cybersecurity in Algeria:**

**1. Strengths:**

• Existence of a legal framework specifically addressing the prevention of and fight against crimes related to information and communication technologies.
• Development of specialized institutional structures for cybersecurity and combating digital crime.
• Existence of a multi-pillar National Information Systems Security Strategy for 2025–2029.
• Inclusion of training, research and development, and awareness within the national strategy.
• Openness to international cooperation and the exchange of information and expertise.
• Growing recognition that cybersecurity is connected to digital sovereignty and service continuity.

**2. Areas for Improvement:**

The International Telecommunication Union's 2024 Global Cybersecurity Index places Algeria in Tier 3, Establishing. The country profile indicates relative strength in legal measures while identifying technical measures, organizational measures, capacity development, and cooperation as areas with potential for further growth (International Telecommunication Union

[ITU], 2024). This provides an objective basis for the argument that the challenge is no longer limited to establishing legal rules, but increasingly concerns their transformation into sustainable operational capabilities.

Key areas for improvement include expanding specialized expertise; developing reporting and response mechanisms; increasing the readiness of small and medium-sized enterprises; improving supply-chain security; harmonizing standards; increasing research and development funding; and expanding awareness programs directed toward citizens and employees.

**3. The Role of the Private Sector, Universities, and Civil Society:**

Cybersecurity requires a partnership model that does not position the state against the private sector, but makes both components of a shared system. The private sector possesses technical expertise, resources, and innovative capacity, while the state has regulatory authority and responsibility for protecting vital interests. Universities contribute to skills development and applied research, while civil society helps disseminate a culture of digital safety.

It would therefore be useful to develop joint national programs, including applied research laboratories, national incident-response exercises, specialized cybersecurity incubators, vulnerability-reporting platforms, and joint training programs between universities and institutions.

**4. Future Challenges:**

• Rapid evolution of attacks and the tools used to conduct them, including automation and artificial intelligence.
• Expansion of the attack surface as a result of the Internet of Things, cloud services, and digital transformation.
• Shortages of specialized expertise and the need to retain talent nationally.
• Difficulty investigating cross-border crimes and obtaining electronic evidence from abroad.
• Risks arising from dependence on external suppliers and technologies within complex digital supply chains.
• Balancing cybersecurity requirements with privacy and fundamental rights.
• Moving from post-incident response toward proactive measurement of resilience and preparedness.

**Study Findings**

• Cybersecurity is broader than combating cybercrime because it integrates risk management, governance, technology, law, human resources, and resilience.
• Algeria possesses an important legal and institutional foundation, particularly since Law No. 09-04 and the development of specialized bodies.
• The National Information Systems Security Strategy for 2025–2029 represents a move toward a more integrated vision combining technical capabilities, the legal framework, training, research, and cooperation.
• ITU indicators reveal relative strength in the legal domain alongside a need to develop technical and organizational capabilities, capacity building, and cooperation (ITU, 2024).
• Human resources, training, and applied research remain decisive factors in translating the strategy into measurable outcomes.
• The cross-border nature of cybercrime requires the expansion of international judicial, police, and technical cooperation channels.
• Cybersecurity should become part of institutional risk management in every sector rather than the responsibility of a separate technical unit.

**Conclusion:**

Digital transformation has demonstrated that cybersecurity is no longer a marginal technical sector but has become a component of national security, economic development, and the quality of public services. In Algeria, the legislative and institutional trajectory indicates a gradual transition from addressing computer-related crimes toward building a broader cybersecurity system. This transition becomes clearer with the National Information Systems Security Strategy for 2025–2029, which places resilience, protection of digital infrastructure and data, and continuity of services within an integrated national framework.

Nevertheless, the success of the strategy depends not merely on its formulation but on implementation, measurement, and periodic evaluation. The true measure of success is the capacity of institutions to prevent incidents where possible, detect them rapidly, contain them, restore services, and learn from their consequences. Building cyber resilience in Algeria therefore requires long-term investment in people, technology, knowledge, and partnerships, alongside continued legislative development and international cooperation.

**Recommendations:**

• Establish measurable national performance indicators for monitoring implementation of the 2025–2029 strategy.
• Strengthen specialized training programs and create practical pathways jointly developed by universities and institutions.
• Develop security operations centers and incident-reporting and response mechanisms in critical sectors.
• Adopt unified policies for risk and vulnerability management, backup, and business continuity in public institutions.
• Support applied scientific research and specialized cybersecurity start-ups.
• Expand digital-awareness programs to employees, students, citizens, and small and medium-sized enterprises.
• Strengthen international cooperation in digital investigations and the exchange of threat indicators and expertise.
• Balance security requirements with the protection of privacy, data, and fundamental rights.

• Conduct periodic independent assessments of cybersecurity maturity in sensitive sectors and link assessment results to improvement plans.

**References:**

Agence de Sécurité des Systèmes d'Information, Ministère de la Défense Nationale – Algérie. (2026). *National Information Systems Security Strategy for 2025–2029*.
Ben Arabia, R. (2021). Strategic dimensions of cybercrime and its threats to national security. *Scientific Research Notebooks, 9*(1), 265–266.
Ben Azouz, H., & Manani, H. (2022). Cybersecurity and cybercrime in postmodern states: The United States of America as a model. *Al-Risala Journal of Media Studies, 6*(2), 581–582.
Bouzadia, J. (2019). The Algerian strategy for confronting cybercrime: Challenges and future prospects. *Journal of Legal and Political Sciences, 10*(1), 1277–1278.
Boughrara, Y. (2018). Cybersecurity: The Algerian strategy for security and defense in cyberspace. *Journal of African and Nile Basin Studies, 1*(3), 107–109.
Chaib, N. (2022). Strategic mechanism of combating cyber crime under the new environment of digital communication. *Law and Political Science Journal, 8*(2), 712.
Cheikh, A. S. (2020). Prevention of cybercrime under Law No. 09-04. *Ma'alim Journal of Legal and Political Studies, 4*(1), 198–199.
Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention), ETS No. 185*.
Denden, J. E. (2020). The Algerian state's security strategy in combating cybercrime. *Sawt Al-Qanun, 7*(2), 985.
Halder, D., & Jaishankar, K. (2011). Cybercrime and the victimization of women: Laws, rights, and regulations. *International Journal of E-Business Research, 7*(4), 15–25.
International Telecommunication Union. (2024). *Global Cybersecurity Index 2024*. ITU.
Khelia, W. (2021). The problematic nature of citizenship under the values of modern technology: Between citizens' freedom and cybersecurity. *Annals of the University of Algiers 1, 35*(1), 812.
Law No. 09-04 of August 5, 2009, establishing special rules for the prevention of and fight against offenses connected with information and communication technologies. *Official Gazette of the People's Democratic Republic of Algeria*, No. 47.
Ministère de la Défense Nationale – Algérie. (2026). *National Information Systems Security Strategy for 2025–2029*.
Muslim, N. I. (2021). Cybercrimes and their impact on cybersecurity. *Al-Qadisiyah Journal of Law and Political Science, 12*(1), 276–277.
National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). U.S. Department of Commerce.
Rigopoulos, K., Quinn, S., Pascoe, C., Marron, J., Mahn, A., & Topper, D. (2024). *NIST Cybersecurity Framework 2.0: Resource & Overview Guide* (NIST SP 1299). National Institute of Standards and Technology.
Zarouka, I. (2019). Cyberspace and the transformation of concepts of power and conflict. *Journal of Legal and Political Sciences, 10*(1), 1023–1024.
Attia, I. (2019). The position of cybersecurity within the Algerian national security system. *Masdaqiya, 1*(1), 115–116.
Methodological note on the update: The article was reformulated while preserving its subject matter and principal axes. Contemporary concepts, including cyber resilience and risk governance, were added, and the section concerning the National Information Systems Security Strategy for 2025–2029 was updated on the basis of official documents published in 2026.