



The Algerian Public Security Policy on Combating Cybercrime: Implemented Strategies, Evaluation Frameworks, and Approaches to Enhancing Effectiveness

Omar djilali *

University of laghouat (Algeria)

Omar djilali918@gmail.com

Received: 10/02 /2026

Accepted: 17/03 /2026

Published: 31/03 /2026

Abstract:

This study examines Algeria's security policy with a particular focus on cybersecurity as a fundamental component of national defense. It highlights the transition from a traditional state-centered security model toward a more comprehensive approach that prioritizes the protection of individuals and society. Through an analysis of legal reforms, institutional arrangements, and technological measures, the study assesses Algeria's capacity to address digital threats. The findings show the establishment of specialized bodies, supportive cybercrime and data protection legislation, and investments in human capital and digital infrastructure, including AI-based tools. However, the study emphasizes the need for enhanced innovation, research, and international cooperation to strengthen national cybersecurity resilience.

Keywords: Algerian Security Policy, Cybersecurity, Cyber Legislation, E-Governance.

Introduction :

Security policy has become a fundamental pillar in modern governance systems, making it a central focus, particularly amid escalating cyber challenges that threaten the stability of states and their critical functions. The rapid pace of

* Corresponding author



digital transformation and the increasing frequency of cyberattacks—often carried out by non-state actors—have necessitated a reassessment of the foundations and mechanisms of national protection.

This is particularly evident in the Algerian context, given its geostrategic position and growing reliance on digital infrastructure across strategic sectors, especially defense, energy, and finance, where risks are increasingly complex and require proactive and flexible solutions. In response, the state has adopted strategies based on prevention, modernization of technological systems, and the development of specialized human capital.

Consequently, cybersecurity has become a strategic line of defense against multi-dimensional, asymmetric threats. These efforts reflect a growing awareness of the importance of protecting national security and ensuring the sustainability of state stability in a changing digital environment.

Research Problem:

To what extent is Algeria's public policy capable of effectively addressing cybercrime, and what procedures and evaluations are employed to ensure the policy adapts to evolving digital threats?

Research Hypothesis:

Within this framework, the study assumes the hypothesis that the effectiveness of Algeria's public policy in combating cybercrime is determined by the integration of organizational and technical measures alongside continuous evaluation. This integration enhances the state's ability to prevent cybercrime and mitigate its impacts on national and societal security, highlighting the central role of institutional coherence in shaping a cohesive security policy capable of adapting to technological transformations, protecting critical infrastructure, achieving digital sovereignty objectives, and strengthening the state's resilience in the cyber domain.

Research Methodology:

This study employs three main methodologies:

1. Descriptive-analytical approach to examine legal texts, official documents, and national strategies while evaluating the role of relevant institutions.



2. Comparative approach to analyze similar international experiences in order to identify strengths and weaknesses within the national system and draw lessons for developing more effective policies and strategies.

3. Foresight approach to anticipate future directions in security policy and propose recommendations to enhance Algeria's cyber resilience.

THE FIRST TOPIC : The Concept of Public Security Policy: A Conceptual and Theoretical Approach

Public security policy constitutes an analytical and operational framework that bridges theory and practice in order to protect society from diverse risks and threats. It is grounded in the concept of security in its multiple dimensions, ranging from traditional state security to human and cyber security, while ensuring a balance between the interests of the state and the individual. This policy is also influenced by different theoretical approaches that explain how it is formulated and implemented through actors and institutions.

FIRST REQUIREMENT: The Concept of Security

The conceptual framework provides a foundation for understanding public security policy by defining the core concepts of security and public policy and their relationships with actors and institutions. It also clarifies the different dimensions of security and prepares the ground for studying strategies and practical applications.

Firstly: The Linguistic Concept of Security

From a linguistic perspective, security is defined as the opposite of fear and is associated with reassurance and stability. The triliteral Arabic root "amana" conveys both the sense and provision of safety for oneself and others. Ibn Manzur addresses this concept in *Lisan al-Arab*, noting that the verb implies self-security as well as the protection of others, particularly in safeguarding their trust and secrets.¹ This linguistic understanding is further reinforced by the Qur'anic verse: "Let them worship the Lord of this House, who has fed them against hunger and secured them from fear" (Qur'an, 106:3–4)², which clearly establishes the intrinsic

¹ Ibn Manzur, edited by Abdullah Ali Al-Kabir et al., *Lisan al-Arab*, Cairo: Dar Al-Ma'arif, 1979, pp. 140–141.

² The Holy Qur'an, Surat Quraysh, Verses 3–4



relationship between security and the elimination of fear. In political and security studies, scholarly literature generally conceptualizes security as a state of psychological and physical stability resulting from the absence of threats.

Secondly: The Terminological Definition of Security

Security represents one of the most debated and theoretically contested concepts, largely due to its complex and multidimensional nature. This ambiguity has led scholars to adopt operational or conceptual definitions to facilitate theoretical framework construction. Within international relations and strategic studies, several theoretical contributions have sought to conceptualize security. Barry Buzan, a leading figure of the Copenhagen School, significantly redefined security in the post–Cold War context, conceptualizing it as “freedom from threat” and linking it to the ability of states and societies to preserve their independent identity and functional cohesion against perceived hostile or destructive challenges.¹

Conversely, theoretical perspectives vary according to intellectual schools. The traditional realist approach equates security with state power, viewing it as the accumulation of military and material capabilities. Security, in this sense, is defined as the capacity to possess or exercise power through deterrence and control.² More broadly, security may be defined as a condition in which individuals, society, and the state are protected from internal and external threats, encompassing political, economic, social, cultural, environmental, military, and technological dimensions.

Third: The Concept of Public Policy

Public policy is a multidimensional concept shaped by diverse theoretical and methodological approaches, which has prevented consensus on a single definition. David Easton conceptualized public policy as an authoritative allocation of material and symbolic values within society through interactions between inputs, outputs, and feedback mechanisms.³ James Anderson viewed public policy as a purposive course of action designed to address a specific problem, developed by governmental bodies with potential involvement from non-

¹ Ben Antar, Abdelnour, *The Mediterranean Dimension of Algerian Security: Algeria, Europe, and NATO*, Algiers: Al- Maktaba Al-Asriya for Printing and Publishing, 2005, p. 13.

² Williams, Paul D., ed., *Security Studies: An Introduction*, London: Routledge, 2008, p. 9.

³ Easton, David, *A Systems Analysis of Political Life*, New York: Wiley, 1965, pp. 134–135.



official actors.¹ In Arab scholarship, Khairy Abdel Qawi defined it as a set of procedures aimed at identifying problems, formulating policy alternatives, and selecting binding solutions², while Ahmed Saifan described it as an integrated governmental orientation encompassing objectives, instruments, actors, and implementation mechanisms.³

Fourth: The Concept of Public Security Policy

Sebastian Roché defines public security policy as the set of legislative, regulatory, and operational arrangements through which security issues are managed by official and local actors, sometimes in partnership with civil society organizations or the private sector.⁴ This approach targets offenders, victims, and public opinion simultaneously and emphasizes the institutional framework and political dynamics shaping the definition of security phenomena within the political system. When crime is interpreted as an individual or social deviation, policies prioritize control and punishment; when viewed as a complex phenomenon, preventive and educational mechanisms are adopted. Human security constitutes a central dimension, linking security to individual dignity, fundamental rights, and comprehensive development. Contemporary studies also highlight the gap between policy formulation and field implementation, underscoring the need to adapt policies to local contexts and to involve multiple stakeholders to ensure sustainability and institutional coherence.⁵

Fifth: Definition of Cybersecurity

According to the U.S. Department of Defense, cybersecurity refers to the set of organizational measures aimed at protecting information in all its physical and digital forms from threats and crimes, including cyberattacks, sabotage, espionage, and technical incidents.⁶ The International Telecommunication Union

¹ Anderson, James E., *Public Policy Making*, translated by Amer Al-Kaisi, Amman: Dar Al-Masira, 1999, p. 15.

² Khairy, Abdel Qawi, *Public Policy Studies*, Kuwait: That Al-Salasil Printing, Publishing and Distribution, 1988, pp. 35–36.

³ Saifan, Ahmed, *Dictionary of Political, Constitutional and International Terms*, 1st ed., Beirut: Librairie du Liban Publishers, 2004, p. 213.

⁴ Roché, Sébastien, *Political Sociology of Insecurity*, Paris: Presses Universitaires de France, 1998, cited in Laurent Mucchielli, *Revue française de sociologie*, Vol. 40, No. 1 (1999), p. 151.

⁵ Bouriche, Riadh, “Approaches and Conceptions of Public Security Policies,” in *International Forum “Algiers and Security in the Mediterranean: Reality and Prospects”*, Mentouri University of Constantine, Faculty of Law and Political Science, 29–30 April 2008, p. 1

⁶ Mayar, Adel Fathi Abdelhamid, and Tuqa Hamed Moawad Abdelhamid, “The Role of Russian Political Leadership in Enhancing Cybersecurity (2012–2023),” *Arab Democratic Center for Economic*



(ITU), in its report on Trends in Telecommunication Reform, defines cybersecurity as a framework encompassing tools, policies, safeguards, and security principles designed to protect cyberspace by deterring or preventing attacks through strategies adapted to technical, human, organizational, and legal environments.¹ Operationally, cybersecurity may be defined as a system of technical and organizational measures intended to protect computers, software, networks, and data by preventing or mitigating unauthorized access through mechanisms such as encryption, access control, incident response planning, system continuity, and data recovery.²

SECOND REQUIREMENT: Theoretical Approaches in Security Policy Studies

Firstly :Systems Theory

Systems theory views public policy as a response of the political system to demands and pressures from its internal and external environment. Inputs (demands and support) are transformed into outputs (policies and decisions) through institutional mechanisms, while feedback reflects policy impacts on society. Although effective in structuring analysis, this approach offers limited insight into decision-making processes within the political “black box.”³

Secondly: Group Theory

This theory assumes that public policy results from competition and interaction among interest groups seeking to influence governmental institutions. Policies reflect shifting balances of power among these groups. Critics argue that this approach exaggerates group influence while underestimating institutional and bureaucratic roles.⁴

Third: Elite Theory

Elite theory posits that public policy reflects the preferences of a ruling minority rather than the will of the majority. According to Dye and Zeigler,

and Political Studies, article published on the Center’s website on 22 June 2023, available at: <https://democraticac.de/?p=>, accessed on 6 April 2025 at 15:30

¹ Mayar, Adel Fathi Abdelhamid, and Tuqa Hamed Moawad Abdelhamid. *ibid* .

² Mayar, Adel Fathi Abdelhamid, and Tuqa Hamed Moawad Abdelhamid. *Ibid*.

³ Anderson, James E. *ibid*, p. 31.

⁴ Al-Hussein, Ahmed Mustafa, *An Introduction to Public Policy Analysis*, 2nd ed., Amman: Scientific Center for Studies, 2002, p. 119.



policies primarily protect elite interests, with gradual reform ensuring system stability. Despite highlighting the hierarchical nature of policymaking, the theory is criticized for marginalizing popular participation.¹

Fourth: Institutional Theory

Institutional analysis emphasizes the role of formal governmental

institutions in shaping public policy. While early approaches focused on legal structures and procedures, contemporary perspectives integrate behavioral and political dynamics, recognizing institutions as both structural and interactive frameworks influencing policy outcomes.²

THE SECOND TOPIC : Actors in the Formulation of Public Security Policy in the Cyber Domain

The process of making public security policy in the cyber domain results from a complex interaction between official and non-official actors, whose roles and influence vary according to the political and institutional context. Official actors are responsible for legislation, implementation, and oversight, while non-official actors contribute by shaping decision-making through political and societal influence. This interaction ultimately determines the scope, effectiveness, and adaptability of cybersecurity policies in response to evolving threats.

FIRST REQUIREMENT: Official Actors

Official actors constitute the institutional framework governing the public security policy-making process, as they perform legislative, executive, and oversight functions that ensure the formulation and implementation of cybersecurity policies within constitutional legitimacy.

Firstly: The Executive Authority:

The executive authority constitutes a central component in the process of public policy formulation, as it is responsible for implementing legislation, maintaining public order, and managing national affairs. Its structure varies

¹ Bayoumi, Ali Mahmoud, *Elite States in Political Decision-Making*, 1st ed., Cairo: Dar Al-Kitab Al-Hadith, 2004, p. 14.

² Khalifa, Mahmoud, and Mohamed Jouda, "The Elite Approach in the Study of Comparative Political Systems," Arab Democratic Center, website article, available at: <https://democraticac.de/?p=550>, accessed on 5 April 2025



according to the nature of the political system: it is concentrated in the hands of the head of state in presidential systems, shared between the government and the head of state in parliamentary systems, and exercised by an elected body in representative systems. De Tansy notes that the executive authority consists of the head of state, members of the government, and the civil administrative apparatus. Its functions include proposing new public policies, supervising their implementation, making decisive decisions during crises, exercising appointment powers with political and strategic implications, and managing official political communication through speeches and conferences. The extent of its influence depends on the institutional balance among powers, with broader authority in developing states and more restrained roles in advanced democracies.

Secondly: The Legislative Authority:

The legislative authority is a core institution in the formulation and adoption of public policies. Its primary function lies in enacting laws, debating draft legislation proposed by the executive, and exercising oversight over governmental performance. Kenneth Bess, Nicholas Mays, and Gail Walt argue that the legislature embodies the principle of popular sovereignty as the highest decision-making body, fulfilling three main roles:¹ representing the popular will, legislating, and supervising the executive authority.

Additionally, the legislature contributes to balancing political interests, consulting civil society and the private sector, and ensuring policy continuity. De Tansy emphasizes that legislators' roles extend beyond lawmaking to include accountability and budgetary control, thereby reinforcing their position in the policymaking process.

Third: The Judicial Authority:

The judiciary represents a key institutional pillar influencing the public policy cycle by ensuring compliance with laws and resolving disputes arising from their interpretation. Its responsibilities include constitutional review of laws and regulations, legal interpretation, adjudication of disputes between individuals and the state, and the administration of justice. Institutional independence is a fundamental prerequisite for fulfilling these functions. In democratic systems, the judiciary plays a vital role in reviewing the legality and constitutionality of public policies, whereas this role is often diminished in developing countries due to

¹ Buse, Kent, Nicholas Mays, and Gill Walt, *Making Health Policy*, Maidenhead, Berkshire: Open University Press, 2005, p. 87.



executive dominance, weakening judicial influence in policymaking. Consequently, the judiciary's political role depends largely on the degree to which the separation of powers is upheld.¹

Fourth: The Administrative Apparatus:

The administrative apparatus is no longer confined to policy implementation but has become a key actor in shaping and guiding public policies due to its technical expertise and knowledge resources. Its role manifests through direct contributions—such as proposing or amending draft legislation based on specialized analysis—and indirect contributions, including policy interpretation during implementation and influencing policy trajectories through technical consultation.² Its influence is reinforced by its proximity to citizens, enabling the assessment of policy effectiveness; the growing complexity of societal issues requiring expert input; and its delegated authority to issue secondary legislation through executive regulations. Accordingly, the administrative apparatus serves as a fundamental actor in ensuring institutional continuity and adapting policies to technical and social changes.

SECOND REQUIREMENT: Non-Official Actors

Firstly: Political Parties

Political parties are considered social and political organizations that aim to articulate the interests of specific groups and seek to influence political power or gain access to it through elections or participation in elected bodies. Parties influence the policy-making process through several mechanisms, including:³ nominating candidates for public office, participating in political deliberations, organizing campaigns and demonstrations, building alliances and coalitions, mobilizing public opinion, and engaging in political competition with other parties. In this sense, political parties constitute an institutional channel for aggregating and expressing interests within the formal political framework.

Secondly: Pressure Groups

¹ Naji, Abdelnour, and Sahli, Mabrouk, *An Introduction to Public Policy Studies*, Annaba: Dar Al-Olum for Publishing and Distribution, 2014, p. 4.

² Al-Tayyib, Hassan Abshar, *The Modern State as an Institutional State*, Cairo: Dar Al-Fajr for Publishing and Distribution, 2000, p. 107.

³ Al-Hamdani, Qahtan Ahmed, *Introduction to Political Science*, Jordan: Dar Al-Thaqafa for Publishing and Distribution, 1st ed., 2012, p. 273.



Pressure groups are defined as associations with shared interests, often professional or economic in nature, that seek to influence the decision-making process in order to safeguard their interests. According to Marie-Jean-Marie Duncan, these groups exert influence through various means, such¹as using the media to influence parliamentarians, engaging in direct consultations with government authorities, issuing public threats on specific issues, building informal relationships with political elites, and shaping public opinion through advocacy campaigns or strikes. Consequently, pressure groups represent an effective instrument of influence on public policies, including security policies.

Third: Public Opinion

Public opinion represents a collective orientation resulting from the interaction of individual and group views within society and serves as an indicator of popular acceptance or rejection of public policies. It is not merely the sum of individual opinions, but rather a dynamic outcome of their interaction, which grants it significant influence over decision-makers, either through their direct responsiveness to societal demands or indirectly through intermediaries such as political parties and the media.

Fourth: Mass Media

Mass media constitute an influential non-official actor in the public policy-making process, given their capacity to set public agenda priorities and shape public opinion. They act as an intermediary between society and decision-makers by disseminating information, framing issues, and generating political pressure. Accordingly, the media represent an indirect yet decisive force in shaping the social and political environment within which security policies are formulated.

THE THIRD TOPIC : Algerian Public Policy in Confronting Cybercrime: Measures and Evaluation

Cybercrime represents a growing security challenge that compels Algeria to adopt a comprehensive public security policy capable of addressing the complexity of digital threats. Despite the multiplicity of actors and the diversity of institutional, legislative, technological, and human measures, significant gaps continue to undermine the effectiveness of this policy. This section examines the

¹ Duncan, Jean-Marie, Political Science, translated by Mohamed Arab Sassila, Beirut: University Foundation for Studies, Publishing and Distribution, 1997, pp. 346–355.



adopted measures and provides a critical evaluation of the Algerian cybersecurity policy by identifying its strengths and structural limitations.

FIRST REQUIREMENT: Measures Adopted by Algerian Public Policy in Confronting Cybercrime

The measures adopted by the Algerian public policy to combat cybercrime fall within a comprehensive approach aimed at securing the digital space through integrated institutional, legislative, technological, and human mechanisms. This section highlights how the state addresses cyber threats by structuring governance frameworks, enacting legal regulations, advancing technological capacities, and strengthening human and societal capabilities.

Firstly: Definition of Cybercrime

The concept of cybercrime has not been subject to a unified definition in legal and academic literature, as perspectives vary according to the analytical approaches adopted by scholars. While some focus on the criminal act itself, others emphasize the technological tools used in its commission.

In this context, cybercrime has been defined as: “Any illegal or unethical behavior committed through global information networks, posing a threat to finance, knowledge, trust, and reputation, and carried out entirely using modern technological means.”¹

Within Algerian legislation, the legislator has not adopted a single term to describe this phenomenon, but rather employed multiple designations across different legal texts. Law No. 15-04 refers to it as “offenses affecting automated data processing systems,”² while Law No. 04-09 uses the term “crimes related to information and communication technologies.”³ These terminologies reflect an implicit legislative approach that considers cybercrime to encompass all criminal acts targeting or committed through information systems or electronic communication means, whether directly or indirectly.

Secondly: Institutional Measures

¹ Goudri, Ali, and Amal Al-Aysh, “Cybercrime: Concept and Prevention Methods,” *Nomiers Economic Journal*, Vol. 3, No. 1, 2022, p. 194.

² Law No. 04-15 of 10 November 2004, amending and supplementing Law No. 66-156 containing the Penal Code, *Official Gazette of the People’s Democratic Republic of Algeria*, No. 71, 2004.

³ Law No. 09-04 of 5 August 2009 on special rules for the prevention and repression of crimes related to information and communication technologies, *Official Gazette*, No. 47, 16 August 2009.



The institutional dimension is characterized by the multiplicity of national structures involved in cybersecurity, whose responsibilities are distributed across strategic planning, supervision, implementation, and investigation. Key institutions include:

1- **The High Security Council:** An advisory body to the President of the Republic, established under the 1976 Constitution, responsible for defining overarching national security orientations, including major cyber threats.¹

2- **Ministry of National Defense:** Plays a leading role in shaping and implementing cybersecurity strategies and supervising central bodies in this field.

3- **National Council for Information Systems Security:** Established by Presidential Decree No. 20-05, chaired by the Minister of National Defense, responsible for approving national strategies, supervising the national agency, validating cooperation agreements, electronic certification, and information system classification.²

4- **National Agency for Information Systems Security (ANSSI):** A public administrative institution tasked with preparing strategies, investigating cyberattacks, coordinating preventive measures, developing legislation, training, and technological monitoring.³

5- **National Gendarmerie:** Hosts the Cybercrime Prevention Center (2008)⁴ and the National Institute of Criminal Evidence (2009)⁵, responsible for investigation, monitoring, and digital forensic analysis.

6- **General Directorate of National Security (DGSN):** Includes the Central Service for Combating Cybercrime (established in 2011).¹

¹ Constitution of 1976, Official Gazette of the People's Democratic Republic of Algeria, No. 5, 25 February 1976, Article 125, establishing the Supreme Security Council chaired by the President of the Republic.

² People's Democratic Republic of Algeria. Presidential Decree No. 20-05 of 22 January 2020 on the establishment of the National Council for the Security of Information Systems. Official Gazette, No. 04, 2020.

³ People's Democratic Republic of Algeria. Presidential Decree No. 20-05 of 22 January 2020, previous reference.

⁴ Mahni, Sofiane, "Establishing a Center for Combating Cybercrime in Algeria," El Fadjr Newspaper, 17 May 2008, accessed 4 June 2025, <https://www.djazairiess.com/alfadjr/71333>.

⁵ Presidential Decree No. 04-183 of June 2004 establishing the National Institute of Criminal Evidence and Criminology of the National Gendarmerie. Official Gazette, No. 41, 2004.



7- National Authority for the Prevention of Cybercrime (ONPLITIC): An independent administrative authority affiliated with the Ministry of Justice, tasked with cybercrime prevention, judicial support, and electronic surveillance in sensitive national security cases.²

Third: Legislative Measures

The legal framework constitutes the regulatory foundation of the national cybersecurity policy and has evolved gradually in response to technological transformations.

1-Initial phase: The legislator addressed certain issues within existing laws, such as Ordinance No. 05-03 on copyright, which classified computer software as protected literary works.³

2-Specific criminalization: Law No. 04-15 introduced amendments to the Penal Code concerning offenses against automated data processing systems⁴, followed by Law No. 06-23, which expanded the scope of criminalization to include unlawful access, data alteration, and illegal trafficking of information.⁵

3-Core framework: Law No. 09-04 on the prevention of cybercrime established a comprehensive definition of cyber offenses and set out preventive and procedural mechanisms, most notably:⁶

□ **Electronic surveillance:** subject to judicial authorization in cases related to terrorism and national security (Article 4).

¹ Chahid, Elias; Al-Hallaj, Arraba; and Defrou, Abdelnaim, "Evaluating the Experience of E-Government Implementation in Algeria," *Algerian Journal of Accounting and Financial Studies*, No. 3, 2016, p. 130.

² Presidential Decree No. 15-261 of 8 October 2015 on the establishment of the National Authority for the Prevention and Repression of Crimes Related to Information and Communication Technologies, *Official Gazette*, No. 53, 8 October 2015.

³ Ordinance No. 05-03 on Copyright and Related Rights, *Official Gazette of the People's Democratic Republic of Algeria*, No. 04, 2005.

⁴ Law No. 04-15 of 10 November 2004 amending and supplementing the Penal Code concerning attacks on automated data processing systems, *Official Gazette*, No. 75, 2004.

⁵ Law No. 06-23 of 20 December 2006 amending and supplementing Ordinance No. 66-156 (Penal Code), extending criminalization to include illegal access to or remaining in an information system and manipulation of electronic data, *Official Gazette*, No. 84, 2006.

⁶ Law No. 09-04 of 5 August 2009 on special rules for the prevention and repression of crimes related to information and communication technologies, *Official Gazette*, No. 46, 2009.



- **Cooperation with service providers:** obliging them to retain traffic data and block illegal content (Articles 11 and 12).
- **Search and seizure:** including remote searches and the use of experts (Articles 3 and 7).
- **Extended jurisdiction:** enabling the prosecution of offenses committed outside the national territory against state institutions.
- **International cooperation:** through mutual legal assistance in the collection of electronic evidence.

This legislative framework complements the Penal Code and the Code of Criminal Procedure, reflecting a dual orientation toward criminalization and prevention, while revealing practical implementation challenges related to rapid technological change and the need for continuous legal updates.

Fourth: Technical and Technological Measures

The technological dimension constitutes a core pillar of cybersecurity policy, intersecting strategic digital opportunities with complex cyber threats. Algeria seeks to enhance its digital infrastructure, particularly with the adoption of 5G technologies, which, while enabling high-speed communication and smart services, also increase attack surfaces and infrastructure vulnerabilities.

In response, Algeria pursues a national cybersecurity strategy based on digital sovereignty, resilient systems, governmental digitalization, and international cooperation, including Algerian–Russian partnerships supporting **EPE PROXYLAN SPA** under **CERIST**. This reflects recognition of technology as a competitive arena requiring sustained investment and capacity development.¹

Fifth: Human and Societal Measures

Human capital represents both the first line of defense and a potential vulnerability in cybersecurity. Algeria has intensified efforts to build national expertise and raise awareness. Notable initiatives include cybersecurity training for

¹ Ben Mera, Mustapha, “5G in Algeria: Between the Dream of Digital Transformation and the Nightmare of Cyber Threats,” El Ayem News, 6 May 2025, accessed 16 May 2025, <https://elayem.news/06-05-25-06949-5g-fy-aljzair-byn-hlm-althwl-alrqmy-wkabws-althdyd-alsybrany.html>



over 90 health-sector engineers in June 2024 and cooperation with Kaspersky in the banking sector in April 2025.¹

Efforts also focus on integrating cybersecurity into educational systems and awareness programs to promote safe practices, data protection, and resistance to social engineering. Thus, human capacity-building emerges as a strategic complement to technical and regulatory efforts.²

SECOND REQUIREMENT: Evaluation of Algerian Cybersecurity Public Policy

Firstly: Institutional dimension

Despite specialized bodies such as ONSC and CERT.dz, weak coordination, overlapping mandates, limited resources, and bureaucratic constraints hinder effectiveness. Unlike South Korea's centralized KISA model with measurable KPIs, Algeria suffers from institutional fragmentation.³

Secondly: Legislative dimension

Existing laws lag behind technological advances such as AI, IoT, and ransomware. In contrast, France adopts a dynamic legislative approach with CNIL ensuring compliance and enforcement.⁴

Third: Technological dimension

Heavy reliance on imported technologies, outdated systems, limited R&D, and weak adoption of advanced security solutions undermine digital sovereignty. Turkey's investment in national SOCs and domestic solutions highlights Algeria's technological lag.⁵

Fourth: Human dimension

¹ Algerian Ministry of Health, "Training Course on Health Data Security," post on the official Facebook page of the Ministry, June 2024, accessed 12 January 2025.

² Algerian Ministry of National Defense, "The Multidisciplinary Military Polytechnic School," accessed 4 June 2025, https://www.mdn.dz/site_em_anp/sommaire/formation/ar/emp-ar.php.

³ Korea Internet & Security Agency (KISA), Official Website, accessed 3 March 2025, <https://www.kisa.or.kr/EN>

⁴ Agence nationale de la sécurité des systèmes d'information (ANSSI), Activity Report 2019–2023, Paris: ANSSI, 2023, p.4.

⁵ Presidency of the Republic of Turkey, National Cyber Security Strategy and Action Plans 2016–2023, Ankara: Republic of Turkey, 2023.



A shortage of skilled professionals, limited training programs, weak awareness campaigns, and brain drain undermine resilience. South Korea's integrated capacity-building policy contrasts with Algeria's fragmented approach.¹

THE FOURTH TOPIC : Future Prospects of Cybersecurity Policy in Algeria

Firstly: Reactive Response Scenario

In this scenario, Algeria continues to address cyber threats in a reactive rather than proactive manner. Legislation and institutional structures are updated gradually in response to major incidents or international pressures, without developing a comprehensive long-term strategic vision. The focus remains on protecting critical infrastructure, while challenges such as skills gaps and technological dependence continue to exert negative effects.

Secondly: Strategic Enhancement Scenario

This scenario represents the adoption of a more integrated and effective national approach, whereby a national cybersecurity strategy is established with clear objectives and measurable performance indicators, accompanied by regular monitoring and evaluation. The role of the National Cybersecurity Authority is reinforced as a central coordinating body, alongside concrete efforts to bridge the skills gap and develop the legislative framework in alignment with digital transformations.

Third: Regional Leadership and Innovation Scenario

Under this approach, Algeria moves beyond defensive enhancement to aim for a regional leadership role in cybersecurity, whether at the Maghreb or African level. This scenario relies on a proactive policy based on local innovation, development of national solutions, and export of expertise. It involves substantial investments in research and development, human capacity building, and strengthening international partnerships.

Conclusion:

The study concludes that the state of cybersecurity in Algeria is characterized by a multiplicity of institutional actors and a relatively developed legislative

¹ Korea Internet & Security Agency (KISA), *ibid.*



framework. However, weak coordination and the absence of a unified leadership continue to limit overall effectiveness. The findings also indicate that technical and human challenges necessitate sustained investment in infrastructure and human resources, while linking cybersecurity closely to the digital transformation process. There is a clear need for a comprehensive national strategy that strengthens governance, addresses emerging threats, ensures digital sovereignty, and establishes a resilient cybersecurity ecosystem.

Addressing existing gaps in Algeria's cybersecurity landscape requires a set of solutions across four interrelated levels. At the institutional level, it is necessary to strengthen governance through the establishment of a central coordination mechanism, provision of adequate financial and human resources, and adoption of flexible organizational structures capable of adapting to emerging developments, thereby ensuring more effective responses to challenges. At the legislative level, there is a need for periodic review of laws, expansion of legal protection to cover personal data and emerging technologies, enhancement of enforcement capacities, and activation of international cooperation to combat cybercrime. At the technological level, priorities include updating and securing digital infrastructure, promoting the adoption of advanced security solutions, establishing national standards for securing 5G networks and the Internet of Things, alongside supporting research and development to reinforce digital sovereignty. At the human level, effective measures require the development of education and training programs, the implementation of comprehensive national awareness and capacity-building initiatives, and the encouragement of national talent and professional certifications, all of which contribute to building a sustainable and efficient cybersecurity ecosystem.

List of sources and references

First: Legal and Constitutional Texts

1. Constitution of 1976, Official Gazette of the People's Democratic Republic of Algeria, No. 5, 25 February 1976, Article 125.
2. Law No. 04-15 of 10 November 2004 amending and supplementing Law No. 66-156 containing the Penal Code, Official Gazette of the People's Democratic Republic of Algeria, No. 71, 2004.
3. Law No. 04-15 of 10 November 2004 amending and supplementing the Penal Code concerning attacks on automated data processing systems, Official Gazette, No. 75, 2004.
4. Law No. 06-23 of 20 December 2006 amending and supplementing Ordinance No. 66-156 (Penal Code), extending criminalization to include illegal access to or remaining in an information system and manipulation of electronic data, Official Gazette, No. 84, 2006.



The Algerian Public Security Policy on Combating Cybercrime: Implemented Strategies, Evaluation Frameworks, and Approaches to Enhancing Effectiveness

5. Law No. 09-04 of 5 August 2009 on special rules for the prevention and repression of crimes related to information and communication technologies, Official Gazette, No. 46, 2009.
6. Ordinance No. 05-03 on Copyright and Related Rights, Official Gazette of the People's Democratic Republic of Algeria, No. 04, 2005.
7. Presidential Decree No. 04-183 of June 2004 establishing the National Institute of Criminal Evidence and Criminology of the National Gendarmerie, Official Gazette, No. 41, 2004.
8. Presidential Decree No. 15-261 of 8 October 2015 on the establishment of the National Authority for the Prevention and Repression of Crimes Related to Information and Communication Technologies, Official Gazette, No. 53, 2015.
9. Presidential Decree No. 20-05 of 22 January 2020 on the establishment of the National Council for the Security of Information Systems, Official Gazette, No. 04, 2020.

Second: Books

1. Ibn Manzur, ed. Abdullah Ali Al-Kabir et al., *Lisan al-Arab*, Cairo: Dar Al-Ma'arif, 1979, pp. 140–141.
2. Ben Antar, Abdelnour, *The Mediterranean Dimension of Algerian Security: Algeria, Europe, and NATO*, Algiers: Al-Maktaba Al-Asriya for Printing and Publishing, 2005.
3. Williams, Paul D., ed., *Security Studies: An Introduction*, London: Routledge, 2008.
4. Easton, David, *A Systems Analysis of Political Life*, New York: Wiley, 1965.
5. Anderson, James E., *Public Policy Making*, trans. Amer Al-Kaisi, Amman: Dar Al-Masira, 1999.
6. Khairy, Abdel Qawi, *Public Policy Studies*, Kuwait: That Al-Salasil, 1988.
7. Saifan, Ahmed, *Dictionary of Political, Constitutional and International Terms*, 1st ed., Beirut: Librairie du Liban, 2004.
8. Al-Hussein, Ahmed Mustafa, *An Introduction to Public Policy Analysis*, 2nd ed., Amman: Scientific Center for Studies, 2002.
9. Bayoumi, Ali Mahmoud, *Elite States in Political Decision-Making*, Cairo: Dar Al-Kitab Al-Hadith, 2004.
10. Naji, Abdelnour, and Sahli, Mabrouk, *An Introduction to Public Policy Studies*, Annaba: Dar Al-Olum, 2014.
11. Al-Tayyib, Hassan Abshar, *The Modern State as an Institutional State*, Cairo: Dar Al-Fajr, 2000.
12. Al-Hamdani, Qahtan Ahmed, *Introduction to Political Science*, Amman: Dar Al-Thaqafa, 2012.
13. Duncan, Jean-Marie, *Political Science*, trans. Mohamed Arab Sassila, Beirut: University Foundation for Studies, 1997.
14. Buse, Kent, Nicholas Mays, and Gill Walt, *Making Health Policy*, Maidenhead: Open University Press, 2005.

Fourth: Journal Articles

1. Roché, Sébastien, *Sociologie politique de l'insécurité*, Paris: Presses Universitaires de France, 1998, cited in Laurent Mucchielli, *Revue française de sociologie*, Vol. 40, No. 1 (1999), p. 151.
2. Goudri, Ali, and Amal Al-Aysh, "Cybercrime: Concept and Prevention Methods," *Nomiers Economic Journal*, Vol. 3, No. 1, 2022.
3. Chahid, Elias; Al-Hallaj, Arraba; and Defrou, Abdelnaim, "Evaluating the Experience of E-Government Implementation in Algeria," *Algerian Journal of Accounting and Financial Studies*, No. 3, 2016.
4. Agence nationale de la sécurité des systèmes d'information (ANSSI), *Activity Report 2019–2023*, Paris: ANSSI, 2023.



Fifth: Conferences and Forums

1. Bouriche, Riadh, “Approaches and Conceptions of Public Security Policies,” in International Forum: Algiers and Security in the Mediterranean, Mentouri University of Constantine, Faculty of Law and Political Science, 29–30 April 2008.

Sixth: Electronic and Web Sources

1. Mayar, Adel Fathi Abdelhamid, and Tuqa Hamed Moawad Abdelhamid, “The Role of Russian Political Leadership in Enhancing Cybersecurity (2012–2023),” Arab Democratic Center, 22 June 2023, <https://democraticac.de/?p=>, accessed 6 April 2025.

2. Khalifa, Mahmoud, and Mohamed Jouha, “The Elite Approach in the Study of Comparative Political Systems,” Arab Democratic Center, <https://democraticac.de/?p=550>, accessed 5 April 2025.

3. Mahni, Sofiane, “Establishing a Center for Combating Cybercrime in Algeria,” El Fadjr Newspaper, 17 May 2008, <https://www.djazairress.com/alfadjr/71333>, accessed 4 June 2025.

4. Ben Mera, Mustapha, “5G in Algeria: Between the Dream of Digital Transformation and the Nightmare of Cyber Threats,” El Ayem News, 6 May 2025, <https://elayem.news/>, accessed 16 May 2025.

5. Algerian Ministry of Health, “Training Course on Health Data Security,” Facebook post, June 2024, accessed 12 January 2025.

6. Algerian Ministry of National Defense, “The Multidisciplinary Military Polytechnic School,” <https://www.mdn.dz/>, accessed 4 June 2025.

7. Korea Internet & Security Agency (KISA), Official Website, <https://www.kisa.or.kr/EN>, accessed 3 March 2025.

8. Presidency of the Republic of Turkey, National Cyber Security Strategy and Action Plans 2016–2023, Ankara: Republic of Turkey, 2023