International and Comparative
Corporate Law Journal
ISSN: 1388-7084 & E- ISSN: 1875-8290

Cybersecurity in Algeria: Building National Resilience in the Digital Era - Strategic Framework, Legal Challenges, and Future Perspectives

Dr. Bourdima Meriem[1] & Dr. Nouiri Samia[2]

[1]Specialist in Business Law

[2]Lecturer A, University 8 May 1945 Guelma & Laboratory of Environmental Legal Studies (Laboratoire d'Études Juridiques Environnementales)

Email: [1]bourdima.meriem@gmail.com & [2]nouiri.samia@univ-guelma.dz

Received: 18/09/2026 **Accepted:** 11/01/2026 **Published:** 13/04/2026

Abstract

This paper provides a comprehensive examination of cybersecurity in Algeria, analyzing the nation's strategic framework, legal environment, threat landscape, and future perspectives. Algeria faces a complex cyber threat environment, with over 70 million attempted cyberattacks in 2024, targeting critical infrastructure, government systems, and private sector organizations. The country has responded with the development of a comprehensive National Cybersecurity Strategy for 2025-2029, updated legislation including the Digital Identity and Trust Services Law, and institutional reforms such as Presidential Decree 26-07 requiring cybersecurity units in all government agencies.

The paper identifies key vulnerabilities in Algeria's cybersecurity posture, including legacy systems, skills gaps, limited investment, and organizational challenges. It examines the current threat landscape, including malware, ransomware, phishing, DDoS attacks, data breaches, and advanced persistent threats. The paper also analyzes implementation challenges, including technical infrastructure limitations, fragmented governance, and limited institutional capacity. The study presents strategic initiatives and mechanisms for strengthening cybersecurity, including institutional and governance reforms, technical and operational measures, capacity

building, and international cooperation. It explores emerging technologies such as artificial intelligence and machine learning, as well as anticipated policy and regulatory developments. The paper concludes that while Algeria has made significant progress in developing its cybersecurity framework, substantial challenges remain in implementation and capacity building. The recommendations address the needs of government, organizations, educational institutions, and international partners, emphasizing the importance of sustained investment, international cooperation, and a comprehensive, multi-stakeholder approach to building national cyber resilience.

Introduction

Algeria, as a developing nation in North Africa, stands at a critical juncture in its digital transformation journey. The country has witnessed unprecedented growth in internet penetration, with over 33 million internet users as of 2024, representing approximately 75% of the population.[1] This rapid digitalization has brought significant economic and social benefits, yet it has simultaneously exposed the nation to increasingly sophisticated cyber threats. In 2024 alone, Algeria faced more than 70 million attempted cyberattacks, underscoring the urgency of establishing robust cybersecurity frameworks.[2]

The importance of cybersecurity for Algeria extends beyond mere technological considerations; it encompasses national security, economic stability, and social development. The Algerian government has recognized this critical imperative and has initiated comprehensive measures to strengthen the nation's cyber defense capabilities. In December 2025, President Abdelmadjid Tebboune validated Algeria's 2025-2029 National Cybersecurity Strategy, marking a significant milestone in the country's commitment to digital security.[3]

This paper provides a comprehensive examination of cybersecurity in Algeria from multiple perspectives: the strategic and legal frameworks, the practical challenges and threats, and the emerging solutions and future directions. The study is structured into three main sections: the first analyzes the national cybersecurity strategy and legal framework; the second examines the current threat landscape and implementation challenges; and the third explores innovative solutions and future perspectives for strengthening Algeria's cyber resilience.

The objective of this research is to provide policymakers, security professionals, and stakeholders with a thorough understanding of Algeria's cybersecurity landscape, identifying key vulnerabilities, assessing current initiatives, and proposing evidence- based recommendations for enhancing the nation's digital security posture. By doing so, this paper contributes to the broader discourse on cybersecurity governance in developing nations and

offers practical insights for building sustainable cyber resilience.

Section One: National Cybersecurity Strategy and Legal Framework

Part One: Conceptual Foundations and Strategic Vision

Definition and Scope of Cybersecurity

Cybersecurity, in its broadest sense, refers to the practice of protecting computer systems, networks, and digital information from unauthorized access, theft, damage, or disruption.4 It encompasses technical measures, organizational policies, and human practices designed to ensure the confidentiality, integrity, and availability of digital assets. In the context of national security, cybersecurity extends beyond individual organizations to include critical infrastructure protection, national defense capabilities, and economic resilience.

The scope of cybersecurity in Algeria encompasses multiple dimensions:

Technical Dimension: This includes the protection of information systems, networks, and digital infrastructure through firewalls, encryption, intrusion detection systems, and other technological safeguards.[5]

Organizational Dimension: This refers to the policies, procedures, and governance structures that organizations implement to manage cyber risks and ensure compliance with security standards.[6]

Legal and Regulatory Dimension: This encompasses the laws, regulations, and international agreements that establish the legal framework for cybersecurity and cyber crime prosecution.[7]

Human and Social Dimension: This includes awareness, training, and behavioral aspects that influence how individuals and organizations handle digital security.[8]

Algeria's Strategic Vision for Cybersecurity

Algeria's approach to cybersecurity is embedded within its broader digital transformation agenda, encapsulated in the "Digital Algeria 2030" strategy.[9] This comprehensive vision aims to leverage digital technologies to drive economic growth, improve public services, and enhance social development. Within this framework, cybersecurity is recognized as a foundational pillar that enables safe and secure digital transformation.

The strategic objectives of Algeria's cybersecurity approach include:

Building Cyber-Resilience: Developing the capacity of national information systems to withstand, recover from, and adapt to cyber threats.[10]

Protecting Critical Infrastructure: Ensuring the security of essential services such as energy, water, telecommunications, healthcare, and financial systems that are vital to national

functioning.[11]

Fostering Digital Trust: Creating an environment where citizens, businesses, and government institutions can confidently engage in digital transactions and communications.[12]

Enhancing Sovereignty: Ensuring that Algeria maintains control over its digital infrastructure and data, reducing dependence on foreign technology providers and services.[13]

Promoting Innovation: Supporting the development of local cybersecurity capabilities and fostering a thriving cybersecurity industry within Algeria.[14]

National Cybersecurity Strategy 2025-2029

The 2025-2029 National Cybersecurity Strategy represents Algeria's most comprehensive and forward-looking approach to cyber defense.[15] Approved through Presidential Decree No. 25-321 of December 30, 2025, this strategy establishes a multi- year roadmap for strengthening the nation's cybersecurity posture.

Key Strategic Pillars:

The strategy is built upon several interconnected pillars:

Prevention and Deterrence: Implementing proactive measures to prevent cyber attacks and deter potential adversaries through demonstrated capabilities and consequences.[16]

Detection and Response: Developing rapid detection capabilities and establishing effective incident response procedures to minimize damage from cyber incidents.[17]

Recovery and Resilience: Ensuring that systems can quickly recover from cyber attacks and that critical services can continue operating even under adverse conditions.[18]

Capacity Building: Developing human resources, technical capabilities, and institutional capacity to sustain long-term cybersecurity efforts.[19]

International Cooperation: Engaging with international partners to share threat intelligence, coordinate responses, and harmonize cybersecurity standards.[20]

Part Two: Legal and Regulatory Framework

Existing Cybersecurity Legislation

Algeria's cybersecurity legal framework has evolved significantly over the past decade, reflecting the growing importance of digital security. Key legislative instruments include:

Law No. 12-05 (2016): Establishing the legal foundation for cybersecurity, this law defined cybercrime, established penalties for cyber offenses, and created institutional mechanisms for cyber defense.[21] The law criminalizes unauthorized access to computer systems, data theft, system disruption, and other cyber offenses, with penalties ranging from imprisonment to

substantial fines.

Law on Personal Data Protection (2018): This law establishes requirements for the collection, processing, and protection of personal data, aligning Algeria with international standards such as the General Data Protection Regulation (GDPR).[22] It grants individuals rights to access, rectify, and object to the processing of their personal data, while imposing obligations on data controllers and processors.

Decree on Information Systems Security (2019): This regulatory instrument establishes minimum security standards for government information systems and critical infrastructure, requiring organizations to implement specific technical and organizational measures.[23]

Recent Legislative Developments

Algeria has accelerated its legislative efforts to address emerging cyber threats and digital transformation challenges:

Digital Identity and Trust Services Law (2025): Approved in November 2025, this draft legislation regulates digital identity systems and electronic trust services, including digital signatures and electronic documents.[24] The law grants electronic documents full legal status equivalent to paper documents, modernizing Algeria's legal framework for digital transactions.

Presidential Decree 26-07 (2026): This recent decree mandates that every Algerian ministry, agency, and state enterprise establish dedicated cybersecurity units.[25] This represents a significant institutional commitment to cybersecurity, requiring organizations to designate specific resources and personnel for cyber defense.

Cybersecurity Standards and Certification Framework (2025-2026): Algeria is developing national standards for cybersecurity aligned with international frameworks such as ISO/IEC 27001 and NIST Cybersecurity Framework.[26] These standards establish minimum requirements for information security management systems across both public and private sectors.

Alignment with International Standards and Agreements

Algeria is working to align its cybersecurity framework with international standards and agreements:

Budapest Convention on Cybercrime: While Algeria has not yet formally ratified the Budapest Convention, the country is moving toward alignment with its provisions, particularly regarding the criminalization of cyber offenses and international cooperation mechanisms.[27]

International Standards: Algeria is adopting international cybersecurity standards including

ISO/IEC 27001 (Information Security Management Systems), ISO/IEC 27035 (Incident Management), and NIST Cybersecurity Framework.[28]

African Union Initiatives: Algeria participates in African Union cybersecurity initiatives, including the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which establishes a continental framework for cyber defense and data protection.[29]

Section Two: Cyber Threat Landscape and Implementation Challenges

Part One: Current Threat Environment and Vulnerabilities

Threat Landscape Overview

Algeria faces a complex and evolving cyber threat landscape characterized by diverse threat actors, sophisticated attack methods, and increasing attack volumes. The threat environment can be categorized into several dimensions:

Volume and Intensity of Attacks:

In 2024, Algeria experienced more than 70 million attempted cyberattacks, representing a significant increase from previous years.[30] This volume reflects both the growing attractiveness of Algeria as a target and the increasing sophistication of attack tools available to threat actors. The attacks target a wide range of sectors, including government, finance, telecommunications, energy, and healthcare.

Types of Cyber Threats:

Malware and Ransomware: Malicious software designed to infiltrate systems, steal data, or encrypt files for ransom has become increasingly prevalent.[31] Ransomware attacks targeting critical infrastructure and government agencies have caused significant disruptions and financial losses.

Phishing and Social Engineering: Attackers use deceptive emails, messages, and social engineering tactics to trick users into revealing sensitive information or installing malware.[32] These attacks are particularly effective because they exploit human psychology rather than technical vulnerabilities.

Distributed Denial of Service (DDoS) Attacks: These attacks overwhelm systems with massive volumes of traffic, rendering services unavailable.[33] DDoS attacks have targeted government websites, financial institutions, and telecommunications infrastructure.

Data Breaches and Theft: Attackers target databases containing personal information, financial data, and intellectual property, seeking to steal valuable information for profit or espionage.[34]

Advanced Persistent Threats (APTs): Sophisticated, targeted attacks by state- sponsored or

well-resourced non-state actors that establish persistent access to systems for long-term espionage or sabotage.[35]

Supply Chain Attacks: Attackers compromise software, hardware, or service providers to gain access to their customers' systems.[36]

Vulnerable Sectors and Critical Infrastructure

Certain sectors are particularly vulnerable to cyber threats due to their critical importance and often-inadequate security measures:

Government and Public Administration: Government systems are prime targets for cyber espionage and disruption. Vulnerabilities in government IT infrastructure can compromise sensitive information and disrupt essential services.[37]

Financial Sector: Banks and financial institutions are targeted for theft of funds and customer data. The financial sector's digital interconnectedness creates systemic risks where a successful attack on one institution can have cascading effects.[38]

Energy Sector: Power generation, transmission, and distribution systems are increasingly digitalized and vulnerable to cyber attacks that could cause widespread blackouts and economic disruption.[39]

Healthcare Sector: Hospitals and healthcare providers are vulnerable to ransomware attacks that can disrupt patient care and compromise medical records.[40]

Telecommunications: Telecommunications infrastructure is critical for national communications and increasingly targeted by attackers seeking to intercept communications or disrupt services.[41]

Water and Sanitation: Water treatment and distribution systems are essential for public health, and cyber attacks on these systems could pose significant risks to public safety.[42]

Root Causes of Vulnerabilities

Several factors contribute to Algeria's cyber vulnerabilities:

Legacy Systems: Many Algerian organizations, particularly in government and critical infrastructure, operate legacy systems that lack modern security features and cannot be easily updated or patched.[43]

Skills Gap: There is a significant shortage of cybersecurity professionals in Algeria, limiting the capacity to implement and maintain robust security measures.[44] The demand for cybersecurity expertise far exceeds the available supply of trained professionals.

Limited Investment: Many organizations, particularly in the public sector, have limited budgets for cybersecurity investments, resulting in outdated systems and inadequate security measures.[45]

Organizational Culture: In some organizations, cybersecurity is not prioritized, and security policies are not consistently enforced.[46] Users may not follow security best practices, and management may not allocate sufficient resources to cyber defense.

Regulatory Compliance Challenges: While Algeria has established cybersecurity regulations, enforcement and compliance monitoring remain inconsistent, particularly in smaller organizations and the private sector.[47]

Part Two: Implementation Challenges and Institutional Gaps

Technical and Infrastructure Challenges Network Infrastructure Limitations:

Algeria's network infrastructure, while improving, still faces limitations in terms of capacity, redundancy, and security.[48] Many regions lack high-speed internet connectivity, and network infrastructure is often concentrated in urban areas. This creates vulnerabilities where critical services may depend on limited network paths that could be disrupted by cyber attacks.

Legacy System Integration:

Many Algerian organizations operate a mix of legacy and modern systems that were not designed to work together securely.[49] Integrating these systems while maintaining security is technically challenging and resource-intensive. Legacy systems often cannot support modern security protocols and require expensive upgrades or replacement.

Incident Response Capabilities:

While Algeria has established incident response mechanisms, the capability to detect, respond to, and recover from sophisticated cyber attacks remains limited in many organizations.[50] Response times are often slow, and coordination between organizations and government agencies needs improvement.

Organizational and Institutional Challenges Fragmented Governance:

Cybersecurity responsibilities are distributed across multiple government agencies, including the Ministry of Defense, Ministry of Interior, Ministry of Communications, and others.[51] This fragmentation can lead to duplication of efforts, gaps in coverage, and coordination challenges.

Limited Institutional Capacity:

Many government agencies and organizations lack the institutional capacity to implement comprehensive cybersecurity programs.[52] This includes inadequate staffing, limited training opportunities, and insufficient funding for cybersecurity initiatives.

Coordination and Information Sharing:

Effective cyber defense requires rapid sharing of threat intelligence and coordination of responses across organizations and sectors.[53] Algeria is developing mechanisms for information sharing, but significant gaps remain in the timeliness and completeness of shared information.

Human and Organizational Factors Awareness and Training:

While cybersecurity awareness is increasing, many Algerian citizens and employees lack basic knowledge of cyber threats and protective measures.[54] Training programs are limited in availability and often not tailored to specific organizational needs.

Resistance to Change:

Organizations may resist implementing new security measures due to concerns about operational disruption, cost, or perceived inconvenience.[55] Overcoming this resistance requires strong leadership commitment and clear communication about the importance of cybersecurity.

Insider Threats:

Disgruntled employees, inadequate access controls, and insufficient monitoring create risks of insider threats where authorized users misuse their access for malicious purposes.[56]

Section Three: Solutions, Mechanisms, and Future Perspectives

Part One: Strategic Initiatives and Implementation Mechanisms

Institutional and Governance Reforms Establishment of Dedicated Cybersecurity Units:

Presidential Decree 26-07 requires every Algerian ministry, agency, and state enterprise to establish dedicated cybersecurity units.[57] This institutional reform ensures that cybersecurity is given appropriate priority and resources within organizations. These units should be staffed with qualified cybersecurity professionals and given authority to implement security policies and procedures.

Creation of National Cybersecurity Center:

Algeria is developing a National Cybersecurity Center (or similar institution) to serve as the focal point for national cyber defense efforts.[58] This center would coordinate threat intelligence sharing, incident response, capacity building, and policy development across government and critical infrastructure sectors.

Inter-Agency Coordination Mechanisms:

Establishing formal mechanisms for coordination between government agencies, critical infrastructure operators, and private sector organizations is essential for effective cyber defense.[59] These mechanisms should include regular meetings, joint exercises, and established

protocols for information sharing and incident response coordination.

Technical and Operational Measures Critical Infrastructure Protection:

Algeria is implementing specific measures to protect critical infrastructure, including:

Network Segmentation: Separating critical systems from general networks to limit the impact of potential breaches.[60]

Redundancy and Failover Systems: Implementing backup systems and failover mechanisms to ensure continuity of critical services.[61]

Advanced Monitoring and Detection: Deploying security information and event management (SIEM) systems and intrusion detection systems to identify potential attacks.[62]

Regular Security Assessments: Conducting penetration testing and vulnerability assessments to identify and remediate security weaknesses.[63]

Cybersecurity Standards Implementation:

Algeria is promoting the adoption of international cybersecurity standards including ISO/IEC 27001, NIST Cybersecurity Framework, and other recognized frameworks.[64] Organizations are encouraged to implement these standards and obtain relevant certifications to demonstrate their security maturity.

Incident Response and Crisis Management:

Developing and regularly testing incident response plans ensures that organizations can quickly detect, contain, and recover from cyber incidents.[65] National incident response playbooks and coordination procedures are being established to facilitate rapid response to major cyber incidents affecting critical infrastructure.

Capacity Building and Human Resource Development Cybersecurity Education and Training:

Algeria is expanding cybersecurity education at universities and technical institutes to develop a skilled workforce.[66] Programs include undergraduate and graduate degrees in cybersecurity, as well as professional certifications such as Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH).

Professional Development:

Establishing continuous professional development opportunities for cybersecurity professionals ensures that the workforce remains current with evolving threats and technologies.[67] This includes conferences, workshops, and specialized training programs.

Public Awareness Campaigns:

Launching public awareness campaigns to educate citizens about cyber threats and protective measures is essential for building a cybersecurity-conscious society.[68] These campaigns should target different audiences, including government employees, business professionals, and the

general public.

Part Two: International Cooperation and Knowledge Exchange

Regional Cooperation Initiatives African Union Cybersecurity Framework:

Algeria participates in African Union cybersecurity initiatives, including the Malabo Convention on Cyber Security and Personal Data Protection.[69] This framework establishes common principles and standards for cybersecurity across African nations and facilitates cooperation in addressing cyber threats.

Maghreb Region Cooperation:

Algeria is developing bilateral and multilateral cooperation agreements with neighboring countries in the Maghreb region to coordinate cyber defense efforts and share threat intelligence.[70]

International Partnerships Cooperation with Developed Nations:

Algeria is establishing partnerships with cybersecurity leaders such as the United

States, European Union, and other developed nations to access technical expertise, training, and resources.[71]

Participation in International Forums:

Algeria participates in international cybersecurity forums and organizations, including the International Telecommunication Union (ITU), INTERPOL, and others, to stay informed about global cyber threats and best practices.[72]

Part Three: Future Perspectives and Emerging Trends

Technological Advancements

Artificial Intelligence and Machine Learning:

AI and machine learning technologies are increasingly being deployed for cybersecurity purposes, including threat detection, anomaly identification, and automated response.73 Algeria is exploring the application of these technologies to enhance its cyber defense capabilities.

Quantum Computing and Post-Quantum Cryptography:

As quantum computing advances, current encryption methods will become obsolete.74 Algeria is beginning to prepare for this transition by exploring post- quantum cryptography standards and planning for the migration of critical systems.

Zero Trust Architecture:

The Zero Trust model, which assumes no implicit trust and requires verification of every access

request, is becoming increasingly important for cybersecurity.75 Organizations are transitioning from traditional perimeter-based security to Zero Trust
architectures.

Policy and Regulatory Evolution Harmonization with International Standards:

Algeria is working toward greater harmonization of its cybersecurity regulations with international standards and agreements.76 This includes potential ratification of the Budapest Convention and adoption of additional international frameworks.

Data Localization and Sovereignty:

Algeria is considering policies to require certain categories of data to be stored within the country to ensure data sovereignty and reduce dependence on foreign cloud services.77 This reflects broader concerns about national control over digital
infrastructure and data.

Cyber Insurance and Risk Management:

The development of cyber insurance markets and risk management frameworks is expected to grow, providing organizations with mechanisms to transfer and manage cyber risks.78

Anticipated Challenges and Opportunities Emerging Threat Vectors:

As technology evolves, new threat vectors will emerge, including attacks on Internet of Things (IoT) devices, cloud infrastructure, and emerging technologies.79 Algeria must remain vigilant and adaptable to address these evolving threats.

Balancing Security and Innovation:

A key challenge will be balancing the need for robust cybersecurity with the desire to foster innovation and digital transformation.80 Overly restrictive security measures could stifle innovation, while insufficient security could leave the nation vulnerable.

Building Sustainable Capacity:

Developing sustainable, long-term cybersecurity capacity requires sustained investment, continuous training, and institutional commitment.81 This is particularly challenging in developing nations with limited resources.

Conclusion

Key Findings

This comprehensive examination of cybersecurity in Algeria reveals several critical findings:

First: Algeria faces a significant and growing cyber threat landscape, with over 70 million attempted cyberattacks in 2024 alone. The threats target critical infrastructure, government systems, financial institutions, and other vital sectors. The vulnerability of these sectors stems

from legacy systems, skills gaps, limited investment, and organizational challenges.

Second: Algeria has made substantial progress in developing a comprehensive cybersecurity framework, including the 2025-2029 National Cybersecurity Strategy, updated legislation, and institutional reforms. The approval of Presidential Decree 26- 07 mandating cybersecurity units in all government agencies represents a significant commitment to cyber defense.

Third: Despite these positive developments, significant implementation challenges remain. These include technical infrastructure limitations, fragmented governance, limited institutional capacity, and gaps in human resources and awareness. Addressing these challenges will require sustained effort and investment.

Fourth: International cooperation and knowledge exchange are essential for Algeria to strengthen its cybersecurity posture. Participation in African Union initiatives, partnerships with developed nations, and adoption of international standards will enhance Algeria's cyber defense capabilities.

Fifth: The future of cybersecurity in Algeria will be shaped by technological advancements, evolving policy frameworks, and the nation's ability to balance security with innovation. Emerging technologies such as AI and machine learning offer opportunities to enhance cyber defense, while quantum computing and new threat vectors present future challenges.

Recommendations

Based on these findings, the following recommendations are proposed:

For Government and Policymakers:

Strengthen Institutional Coordination: Establish clear mechanisms for coordination between government agencies, critical infrastructure operators, and private sector organizations to ensure coherent and effective cyber defense efforts.

Increase Cybersecurity Investment: Allocate sufficient budgetary resources to cybersecurity initiatives, including infrastructure upgrades, training programs, and research and development.

Accelerate Legislative Implementation: Ensure rapid and consistent implementation of cybersecurity regulations, including the 2025-2029 Strategy and recent legislative instruments.

Develop National Incident Response Capabilities: Establish a national incident response center with the capacity to coordinate responses to major cyber incidents affecting critical infrastructure.

Promote International Cooperation: Actively pursue partnerships with international cybersecurity leaders and participate in regional and global cybersecurity initiatives.

For Organizations and Private Sector:

Implement Cybersecurity Standards: Adopt recognized cybersecurity standards such as ISO/IEC 27001 and NIST Cybersecurity Framework to establish baseline security measures.

Invest in Security Infrastructure: Upgrade legacy systems, implement modern security technologies, and establish redundancy and failover mechanisms for critical systems.

Develop Incident Response Plans: Create and regularly test incident response plans to ensure rapid and effective response to cyber incidents.

Invest in Human Resources: Hire qualified cybersecurity professionals and provide ongoing training and professional development opportunities.

Establish Security Culture: Promote a security-conscious organizational culture where cybersecurity is valued and security best practices are consistently followed.

For Educational and Research Institutions:

Expand Cybersecurity Education: Develop comprehensive cybersecurity education programs at universities and technical institutes to build a skilled workforce.

Conduct Applied Research: Conduct research on cybersecurity challenges specific to Algeria and developing nations, contributing to the development of contextually appropriate solutions.

Support Professional Development: Provide professional development opportunities for cybersecurity practitioners through conferences, workshops, and specialized training programs.

Promote Public Awareness: Participate in public awareness campaigns to educate citizens about cyber threats and protective measures.

For International Partners:

Provide Technical Assistance: Offer technical expertise and assistance to help Algeria strengthen its cybersecurity infrastructure and capabilities.

Support Capacity Building: Provide training, educational resources, and financial support for capacity building initiatives.

Facilitate Knowledge Exchange: Create mechanisms for sharing best practices, threat intelligence, and lessons learned in cybersecurity.

Support Standards Harmonization: Assist Algeria in harmonizing its cybersecurity standards and regulations with international frameworks.

Footnotes

Digital Policy Alert, "DPA Digital Digest: Algeria [2025 Edition]," April 2025.

Algeria Strengthens Cybersecurity Framework to Protect National Infrastructure, TechAfricanNews, January 26, 2026.

Presidential Decree No. 25-321 of December 30, 2025, approving the National Cybersecurity Strategy for 2025-2029.

National Institute of Standards and Technology (NIST), "Cybersecurity Framework," 2024 Edition.

Stallings, W., "Cryptography and Network Security: Principles and Practice," 7th Edition, Pearson, 2016.

ISO/IEC 27001:2022, "Information Security Management Systems."

Draou, A., "Cyber Security in Algeria: A Strategic Approach to Address Regional Challenges and Strengthen National Sovereignty," Economic Integration Review, 2025.

Heartfield, R., & Loukas, G., "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks," ACM Computing Surveys, 2016, Vol. 48, No. 3.

Ministry of Digital Transformation, Algeria, "Digital Algeria 2030 Strategy," 2023.

National Information Systems Security Strategy (NSISS), Ministry of Defense, Algeria, 2024.

International Telecommunication Union (ITU), "Cybersecurity and Critical Infrastructure Protection," 2024 Report.

World Economic Forum, "Global Risks Report 2025: Digital Trust and Cybersecurity."

Kello, L., "The Virtual Weapon and International Order," Yale University Press, 2017.

Ministry of Communications, Algeria, "Digital Transformation and Cybersecurity Strategy," 2024.

Presidential Decree No. 25-321 of December 30, 2025.

Libicki, M. C., "Cyberwar as an Intelligence Operation," Journal of Strategic Studies, 2014, Vol. 37, No. 2.

NIST, "Cybersecurity Framework Implementation Guidance," 2024.

Resilience Engineering Institute, "Building Organizational Resilience," 2023.

Dahmani, F., & Brada, A., "Cybersecurity Readiness in Algeria: An Assessment of Infrastructure, Legislation, and Crisis Management," Revue Universitaire de Sociologie, 2025.

United Nations Office on Drugs and Crime (UNODC), "International Cooperation on Cybercrime," 2024.

Law No. 12-05 of June 12, 2016, on Information Systems Security, Algeria.

Law on Personal Data Protection, Algeria, 2018.

Decree on Information Systems Security, Algeria, 2019.

Algeria Approves Law to Strengthen Digital Trust and E-Transactions, WeAreTech Africa, 2025.

Presidential Decree 26-07, Algeria, 2026.

ISO/IEC 27001:2022, ISO/IEC 27035:2023, NIST Cybersecurity Framework.

Council of Europe, "Budapest Convention on Cybercrime," 2001.

International Organization for Standardization (ISO), "Information Security Standards," 2024.

African Union, "Convention on Cyber Security and Personal Data Protection (Malabo Convention)," 2014.

Algeria Orders Cybersecurity Units in Public Sector Amid Surge in Cyberattacks, EcofinAgency, January 28, 2026.

Symantec, "Internet Security Threat Report 2024," 2024.

Phishing Activity Trends Report, Anti-Phishing Working Group, 2024.

Kaspersky, "DDoS Attack Trends Report 2024," 2024.

Identity Theft Resource Center, "2024 Data Breach Report," 2024.

Mandiant, "Advanced Persistent Threats: Threat Intelligence Report 2024," 2024.

CISA, "Supply Chain Attacks," Cybersecurity and Infrastructure Security Agency, 2024.

Dahmani, F., & Brada, A., "Cybersecurity Readiness in Algeria," 2025.

Financial Stability Board, "Cyber Risk and Financial Stability," 2024.

Department of Energy, "Cybersecurity, Energy Security, and Emergency Response (CESER)," 2024.

Healthcare Information and Management Systems Society (HIMSS), "Healthcare Cybersecurity Survey 2024," 2024.

Telecommunications Industry Association, "Cybersecurity in Telecommunications," 2024.

American Water Works Association, "Water Infrastructure Cybersecurity," 2024.

Sipos, Z., "Cybersecurity in Algeria," Journal of Security & Sustainability Issues, 2023, Vol. 12, No. 4.

Bureau of Labor Statistics, "Occupational Outlook for Cybersecurity Professionals," 2024.

International Monetary Fund (IMF), "Cybersecurity Investment in Developing Nations," 2024.

Ponemon Institute, "State of Cybersecurity Culture 2024," 2024.

CMS Law, "Data Protection and Cybersecurity Laws in Algeria," Expert Guide, January 27, 2026.

International Telecommunication Union (ITU), “Measuring Digital Development: Facts and Figures 2024,” 2024.

Gartner, “Legacy System Modernization Strategies,” 2024.

Verizon, “Data Breach Investigations Report 2024,” 2024.

Draou, A., “Cyber Security in Algeria,” 2025.

Dahmani, F., & Brada, A., “Cybersecurity Readiness in Algeria,” 2025.

Cormack, A., “Threat Intelligence Sharing,” GÉANT Association, 2024.

Kaspersky, “Cybersecurity Awareness Survey 2024,” 2024.

Kotter, J. P., “Leading Change,” Harvard Business Review Press, 2012.

Insider Threat Program, CISA, “Combating the Insider Threat,” 2024.

Presidential Decree 26-07, Algeria, 2026.

Ministry of Digital Transformation, Algeria, “National Cybersecurity Center Establishment Plan,” 2025.

National Cybersecurity Strategy 2025-2029, Algeria, 2025.

NIST, “Network Segmentation Best Practices,” 2024.

International Organization for Standardization (ISO), “Business Continuity and Disaster Recovery,” 2024.

Gartner, “Security Information and Event Management (SIEM) Market Guide,” 2024.

OWASP, “Penetration Testing Guide,” 2024.

ISO/IEC 27001:2022, NIST Cybersecurity Framework.

NIST, “Incident Response Guide,” 2024.

Ministry of Higher Education, Algeria, “Cybersecurity Education Programs,” 2024.

(ISC)², “CISSP and Professional Development,” 2024.

CISA, “Cybersecurity Awareness Campaign,” 2024.

African Union, “Malabo Convention on Cyber Security and Personal Data Protection,” 2014.

Union for the Mediterranean, “Regional Cybersecurity Cooperation,” 2024.

U.S. State Department, “International Cybersecurity Partnerships,” 2024.

International Telecommunication Union (ITU), “Global Cybersecurity Index,” 2024.

Gartner, “Artificial Intelligence for Cybersecurity,” 2024.

National Institute of Standards and Technology (NIST), “Post-Quantum Cryptography Standardization,” 2024.

Forrester Research, “Zero Trust Security Model,” 2024.

Budapest Convention Secretariat, “Cybersecurity Treaty Harmonization,” 2024.

World Bank, “Data Localization and Digital Sovereignty,” 2024.

Lloyd's of London, "Cyber Insurance Market Report 2024," 2024.

Gartner, "Emerging Cybersecurity Threats," 2024.

World Economic Forum, "Balancing Security and Innovation," 2024.

UNDP, "Building Sustainable Cybersecurity Capacity in Developing Nations," 2024.