European Journal of Philosophical Research. 2026. 13(1)
E-ISSN: 2413-7286
Volume-13/Issue-1/2026

Cyber Security Between Deterrence and Defense: A National Strategy for a Secure Digital Age

Bouchenafa Karima
University Oran 1 Ahmed ben bella .Algeria
Email: Karimacomunication@gmail.com
Abdssemed Yousra
University Oran 1 Ahmed ben bella .Algeria
Email: abdessemedyousra@gmail.com

Soumission : 08/12/2025 Acceptation :01/06/2026 Publication : 15/06/2026

Abstract:
Currently, the world is witnessing a significant increase in the volume of cyber-attacks targeting various countries as a result of the widespread spread of the Internet and thus the widespread use of information and communication technology, which was accompanied by electronic piracy and crimes related to technological development and the communications revolution, as these attacks result in significant damage to various vital institutions in the country, such as security and financial institutions In this context, protecting information systems has become an inevitable necessity to confront the various cyber threats facing the Algerian state. Through this research paper, we review to read the most important items of the National Strategy for Information Systems Security for the period (2025–2029), which was launched by the Algerian Ministry of National Defense through the Information Systems Security Agency. The study concluded several results, the most important of which are: There are several mechanisms to confront cyber risks which depends on the extent of qualification of the human, technical and legislative elements; the international dimension of cyber security, which requires international cooperation to confront it.

Keywords: Cyber security, digital age, national strategy for security

Introduction

The world is witnessing an accelerating digital transformation that is reshaping the economic, social and security structures of countries. In light of this transformation, cyber security stands out as one of the most important pillars of comprehensive national security, as it is no longer just a technical sub-issue, but has become a strategic pillar that directly affects the stability of countries and the prosperity of their economies This research paper aims to provide an extensive scientific analysis of cyber security while linking it to the Algerian regulatory framework represented by the National Cyber security Strategy issued by the National Cybersecurity Authority (NCA).

In recent decades, the world has witnessed radical transformations in the field of digital technology, as technology has become an integral part of our daily lives. With the widespread

spread of the Internet and the frequent use of smart devices, new challenges have emerged related to cyber security and cybercrime. The virtual world has become the scene of many criminal activities targeting individuals, institutions and even countries through electronic piracy, theft of personal data, and attacks on critical infrastructure Electronic financial fraud is just a few examples of crimes that threaten the stability and security of societies.

Cyber security, in turn, represents a protective shield against these threats, as it works to protect digital systems and sensitive information from breaches and attacks. However, the challenges facing cyber security are increasing day by day, especially with the development of cyber-attack tools and the use of artificial intelligence technologies in carrying out cybercrimes. This reality has led to the need to search for comprehensive and integrated solutions to confront these threats.

Cyber security is a legal guarantee for the protection of bioinformatics assets that directly impact national security. Cyber-attacks targeting critical infrastructure, such as energy, water, and health, may lead to violations of laws related to public security and the disruption of essential facilities protected by legislation as inalienable rights. Cybercrimes, such as electronic piracy and data manipulation, constitute a clear violation of legal articles prohibiting attacks on intellectual property or information systems which requires criminalizing its perpetrators under criminal laws.

In addition, cyber security plays a pivotal role in enhancing legal trust in electronic transactions. With many countries adopting e-commerce and digital government, the need for a secure electronic environment has become a legal and ethical requirement. Cyber security reflects countries' commitment to applying the principles of the rule of law in the digital space, as its role is to achieve a balance between digital freedom and public security In light of the growing cross-border cyber threats, national and international laws related to judicial cooperation and combating cybercrimes become necessary tools to ensure comprehensive protection of the digital society, and thus cyber security emerges not only as a technical necessity but also as a legal and ethical obligation to preserve the rights of individuals and institutions in the digital age.

Problematic

Cyber security today constitutes one of the basic pillars for protecting national sovereignty in light of the accelerating digital transformation, as threats are no longer limited to physical space, but have extended to virtual space with the growing risks it carries. In this context, it is important to balance deterrence strategies that aim to prevent attacks by demonstrating the ability to detect and punish, and defense strategies that focus on strengthening digital infrastructure, securing systems, and building rapid response capabilities. Developing an effective national strategy requires integration between technical, legal, and institutional dimensions, in addition to developing community awareness and human competencies, in a way that ensures the achievement of a safe and sustainable digital environment that supports development and protects the vital interests of the state.

In this research paper, we will discuss Algeria's national strategy for cyber security, which was launched by the Algerian Ministry of National Defense through the Information Systems

Security Agency and is called the National Strategy for Information Systems Security for the period (2025–2029), which is the comprehensive reference framework for protecting cyberspace in Algeria In light of the accelerating digital transformation and increasing cyber threats, this strategy aims to enhance the country's cyber resilience, protect digital infrastructure and sensitive data, ensure the continuity of public services, and consolidate the concept of national digital sovereignty. It is based on a set of basic axes, including developing national capabilities in responding to cyber incidents, strengthening the legal and regulatory framework, and training specialized human resources, in addition to supporting national and international cooperation This strategy is a qualitative step towards building a safe and reliable digital environment that enhances citizens' confidence and supports economic and social development in the digital age.

Through these data, we raise the following main question: How can Algeria's national cyber security strategy achieve an effective balance between enhancing cyber deterrence capabilities and protecting digital infrastructure, in light of accelerating technical challenges, weak societal awareness, and growing cross-border threats?

Definition of cyber security:

Cyber security is the cornerstone of the information society and a fundamental legal pillar for protecting governmental and individual activities. Cyber security raises critical legal issues that affect public and private life, as it directly affects intellectual property rights, the protection of confidentiality and privacy, as well as the preservation of personal data and ensuring the right to privacy In light of the rapid technological development and the accompanying information and communication revolution, new legal concepts have emerged, the most prominent of which is the concept of cyber security. This field has gained strategic importance as it has become a basic protection tool that countries seek to employ to ward off cyber risks that may target their national security and stability. Today, governments realize the extent of the threats and challenges arising from cybercrimes that may affect the country in its vital infrastructure, from its official institutions and individuals in general. From this Starting from there, we will discuss the concept of cyber security.

Cyber security is the field concerned with protecting digital systems, networks, software, and data from cyber-attacks, including protecting the confidentiality (Confidentiality), integrity (Integrity), and availability (Availability) of information, known as the "CIA Triangle." As threats evolve, the concept expands to include resilience (Resilience) and trust (Trust) as essential elements.

Cyber security is defined as a set of measures taken to defend against cyber-attacks launched by computer hackers, in addition to dealing with their consequences and implementing the necessary countermeasures. **(Al-Shammari and Zaid Muhammad Ali Ismail, 2020, page 277)**

Cybernetics is defined as the science of remote control and control, as its basic concept is related to managing and controlling systems through advanced mechanisms, and therefore, the term emerges as a pivotal tool for understanding and controlling modern digital systems, whether in the contexts of technology, law, or daily life. **(Mahdi, 2020, p. 148)**

International reports indicate that cyber-attacks are multiplying rapidly and that the cost of a single hack could reach millions of dollars. However, what is more dangerous is not only the lost money but also the lost trust. A citizen who loses confidence in digital services and an investor who is reluctant to enter an insecure digital market represent a strategic loss that outweighs the financial loss.

In the national context, the legislator defined cyber security in the third paragraph of Article Ten of Law 2 No. 29-58, which stipulates that: "Cyber security: the set of tools, policies, security concepts, security mechanisms, guidelines, risk management methods, business, composition, good practices, guarantees, and technologies that can be used to protect electronic communications against any event that would compromise the provision and integrity of data stored, processed, or sent". **(Official, 2018, p. 27).**

Cyber security through associated concepts:

Cyber security has several concepts related to it, such as cyberspace, cybercrime, cyber threat, and cyber warfare, and therefore we can provide a detail of these concepts:

1- **Cyberspace:** It is an interactive digital environment that combines physical and non-physical elements, including digital devices, network systems, software, and users, whether operators or regular users. Cyberspace is also called "the fourth arm of modern armies" due to its strategic importance in national security **(Mustafa, 2022, p. 07).**

2- **Cybercrime:** Refers to any harmful act that enters cyberspace, such as electronic fraud, publishing illegal content, or attacks targeting the systems of institutions and individuals with the aim of espionage, sabotage, blackmail, or negatively influencing public opinion. (Al-Rafei, 2021, p. 73)

3- **Cyber threat:** It is a malicious program or activity originating in cyberspace that aims to target the security of digital devices such as computers, smartphones, tablets, and networks connected to the Internet. The perpetrator of this threat may be an individual, a country, a group of hackers, or an organization with geopolitical goals. **(Bouqras, 2022, page 125).**

4- **Cyber-attacks:** Any action aimed at weakening the capabilities and functions of the computer network to achieve personal or political goals. This is done by exploiting weak points in the system, which enables the attacker to manipulate or disable it. **(Shlosh, 2018, p. 191)**

5- **Cyber deterrence:** It is defined as harmful actions that target national assets in the digital space or assets related to space operations, by taking proactive and preventive measures to protect cyber infrastructure. **(Mustafa, 2022, page 725)**

6- **Cyber security services:** Technical, administrative, and advisory activities in the field of cyber security, such as security services, includes security assessment, continuous monitoring, security auditing, and technical consultations related to enhancing cyber protection. **(Al-Samhan, 2020, page 11)**

7- **Cyber terrorism:** This term has recently emerged and refers to cyber-attacks aimed at threatening or attacking governments to achieve political, religious, or ideological goals. These attacks can have destructive or subversive effects equivalent to the physical acts of traditional terrorism.**(Kamal, 2022, page 02).**

8- **Cyber warfare:** It is a deliberate attack aimed at disrupting, deceiving, weakening, or destroying computer systems, communication and information networks, and the software contained therein. It also includes the use of cyber means such as hacking, espionage, and leaking sensitive information related to national security. **(Al-Ali and Ali Hussein, 2022, page 103)**

Cyber security applications:

With the rapid development of digital technology, cyber security has become an essential part of our daily lives. This field aims to protect electronic systems and sensitive data from attacks and breaches that may lead to material or moral losses. The areas of application of cybersecurity are expanding to include various vital sectors, starting from government institutions to the personal lives of individuals, whether in protecting national infrastructure, securing financial transactions or maintaining health privacy. The need for effective cybersecurity strategies has become more urgent. In light of the growing cyber threats, each sector must identify its own needs to ensure the security of its data and operations. Hence, the importance of understanding the areas of cybersecurity application and their vital role in achieving stability and protection arises. Thus, we will address the institutional aspect of applying cybersecurity through government and private institutions as a first branch and applying cybersecurity in confronting cyber threats as a second branch.

Cybersecurity in government and private institutions:

Whether in government or private institutions, the main challenges include combating malware, denial-of-service attacks, and targeted attacks such as phishing. Therefore, investments are being made in integrated solutions that combine firewalls, threat detection systems, and employee awareness programs. Incident response has also become an essential part of cybersecurity plans, as specialized teams are being developed to deal with breaches and repair damage as quickly as possible.

First: Cybersecurity in government institutions.

Government institutions are considered one of the most prominent targets of cyber-attacks due to their sensitivity and impact on national security. Cybersecurity here focuses on protecting critical infrastructure such as electricity, water and transportation networks, which are the backbone of any country. Government data management systems are secured to prevent the leakage of confidential information or its exposure to manipulation Advanced technologies are also used to monitor any cyber hacking attempts that may target defense or military systems. In addition, governments are working to

develop national cybersecurity strategies that include training employees and updating systems on an ongoing basis. **(Ali, 2019, p. 89).**

Cybersecurity in private institutions

In the private sector, cybersecurity plays a pivotal role in protecting digital assets and maintaining corporate reputation. Its applications range from securing customer data, such as personal and financial information, to preventing attacks aimed at disrupting business operations. For example, financial companies seek to secure online banking transactions using encryption and behavior analysis techniques to detect suspicious activity. Large companies also pay great attention to protecting intellectual property from industrial espionage, which could lead to competitive losses.

The impact of cyber-attacks on public security

In light of Algeria's digital transformation, cyber-attacks have become a direct threat to national security. Algerian law defines a cyber-attack as any act aimed at disrupting or obstructing information systems or stealing sensitive data. These attacks may target critical infrastructure such as energy, communications, health, and transportation systems, disrupting essential services on which citizens depend.

If the electricity or water system is compromised, it leads to economic and social paralysis, as factories stop working and health and educational facilities are disrupted. Targeting government institutions and security agencies could lead to the leakage of sensitive information or the disruption of military communications systems, threatening a state's sovereignty and ability to make strategic decisions**. (Al-Qahtani, 2020, p. 150).**

The role of cybersecurity in enhancing national stability:

Cybersecurity is a fundamental pillar for enhancing national stability and ensuring the continuity of the operation of public institutions and services in Algeria, in accordance with Algerian Law No. 18-05 on Electronic Commerce **(Official, Law 90-01 on Electronic Commerce, 2018),** in accordance with the provisions of Articles 2, 3, and 5 thereof: Cybersecurity requires protecting digital infrastructure from cyber breaches and attacks, thus ensuring the continuity of the provision of essential services such as health, education, and energy. In doing so, it contributes to achieving social stability and preventing any disturbances that may result from the disruption of these services.**(Nadia, 2022)**

On the economic level, cybersecurity plays a pivotal role in protecting companies and financial institutions from cyber-attacks that aim to steal data or disrupt operations. It also enhances international confidence in the local economy by ensuring a safe digital environment that attracts foreign investments. Thanks to cybersecurity, Algeria can achieve sustainable economic development based on innovation and technology without worrying about cyber threats**.**

At the political level, cybersecurity protects government systems and security institutions from foreign interference or electronic espionage and ensures the confidentiality of

sensitive information related to domestic and foreign policies, which enhances the state's ability to make independent strategic decisions and contributes to combating malicious media campaigns that seek to destabilize political and social stability. At the military level, cybersecurity is an integral part of modern national security in Algeria It protects defense systems and smart weapons from breaches that could lead to the loss of control over them or their use against the state itself. It also contributes to strengthening armed capabilities to confront cyber threats and develop defensive and offensive strategies in cyberspace. **(Issa, 2019, p. 45).**

Cybersecurity enhances national stability by raising community awareness of the importance of cyber protection. By teaching individuals how to deal with cyber threats such as phishing and malware, the risks from human error can be reduced. Thus, society becomes better able to confront cyber threats and contribute to building a safe and stable digital environment.

Cyber threats: their nature and evolution

Cyber threats can be classified into several categories:

Malware: This is software that harms systems, such as viruses and ransom ware (Ransom ware)

Phishing attacks: These involve tricking users into stealing their data, examples of which are fake emails.

Denial of Service Attacks (DDOS): These involve flooding servers with fake requests such as disabling government websites.

Targeted attacks (APT): These are advanced and ongoing attacks that involve targeting critical infrastructure.

Supply chain attacks: These focus on targeting software vendors, such as hacking software updates.

Threats caused by:

With the advent of new technologies, the attack surface (Attack Surface) has evolved:

• **AI in Attack:** Attackers use AI to create sophisticated phishing attacks and quickly hack systems.

• **Internet of Things (IoT):** Devices connected to the Internet (cameras, smart home devices) often lack adequate protection.

• **Cloud computing:** Despite its benefits, it poses challenges in protecting externally stored data.

• **Industrial Control Systems (ICS/SCADA):** Target critical infrastructure such as power plants and desalination.

Efforts made by the Algerian state to achieve cybersecurity

In light of the rapid technological development witnessed by the world, cybersecurity has become one of the basic pillars for protecting countries from growing digital threats. Cybersecurity represents a protective shield for information systems and critical infrastructure, as it works to secure sensitive data and prevent electronic attacks that may lead to huge losses on

the economic and social levels. This research paper highlights the concept of cybersecurity and its importance in enhancing national and international stability. Studies have shown that countries that adopt strong cybersecurity strategies are more capable of confronting contemporary security challenges. The importance of cybersecurity is not limited to protecting individuals and institutions, but extends to ensuring the workflow of vital sectors such as energy, health, and communications, which are the backbone of modern life Cyber threats are no longer just traditional attacks, but have become tools aimed at destabilizing the political and economic stability of countries, making it necessary to adopt comprehensive national policies that enhance cyber awareness and develop technical competencies.

In light of the growth of cybercrime and the complexity of its methods, it has become necessary for governments and institutions to cooperate with local and international experts to develop legal and technical legislation capable of confronting these threats. Thus, it can be said that cybersecurity is not just an option or a luxury, but a strategic necessity to achieve sustainable development and ensure national stability in an era that relies heavily on technology. Investing in enhancing cybersecurity is an investment in a safer and more stable future for future generations Algeria recognized this importance and developed a national strategy to achieve cybersecurity with a forward-looking vision aimed at ensuring national cyber resilience by strengthening the capabilities of prevention, detection and response to cyber incidents to support our country's digital transformation and preserve national digital sovereignty. **(Algerian W., 2026)**

National Cybersecurity Strategy: The Algerian Regulatory Framework

The Algerian National Strategy for Information Systems Security (Cybersecurity) 2025-2029 is the comprehensive official framework approved by Algeria to enhance national cyber resilience, protect digital infrastructure, and support secure digital transformation. Within the framework of protecting and immunizing state institutions and national bodies from all forms of threats that they may face in their cyber space, the Information Systems Security Agency of the Ministry of National Defense published, today, Tuesday, March 3, 2026, The National Strategy for Information Systems Security for the period 2025-2029, in its first version, approved by the President of the Republic, Supreme Commander of the Armed Forces and Minister of National Defense. **(Algerian, 2026)**

This national strategy for information systems security represents the comprehensive framework that aims to ensure national cyber resilience and protect the country's digital infrastructure and data, as well as protect citizens from the threats they may face in cyberspace, especially in light of the country's highest authorities' move to accelerate the pace of digital transformation at the level of all state institutions It is also a roadmap that will preserve national digital sovereignty, ensure basic public services, and enhance citizens' confidence in their digital environment.

Algeria's National Cybersecurity Strategy is based on a regulatory, legal, and normative framework that aims to protect sensitive information systems and infrastructure, ensure cyber resilience and the continuity of public services, enhance digital sovereignty, and protect state and citizen data.

European Journal of Philosophical Research. 2026. 13(1)
E-ISSN: 2413-7286
Volume-13/Issue-1/2026

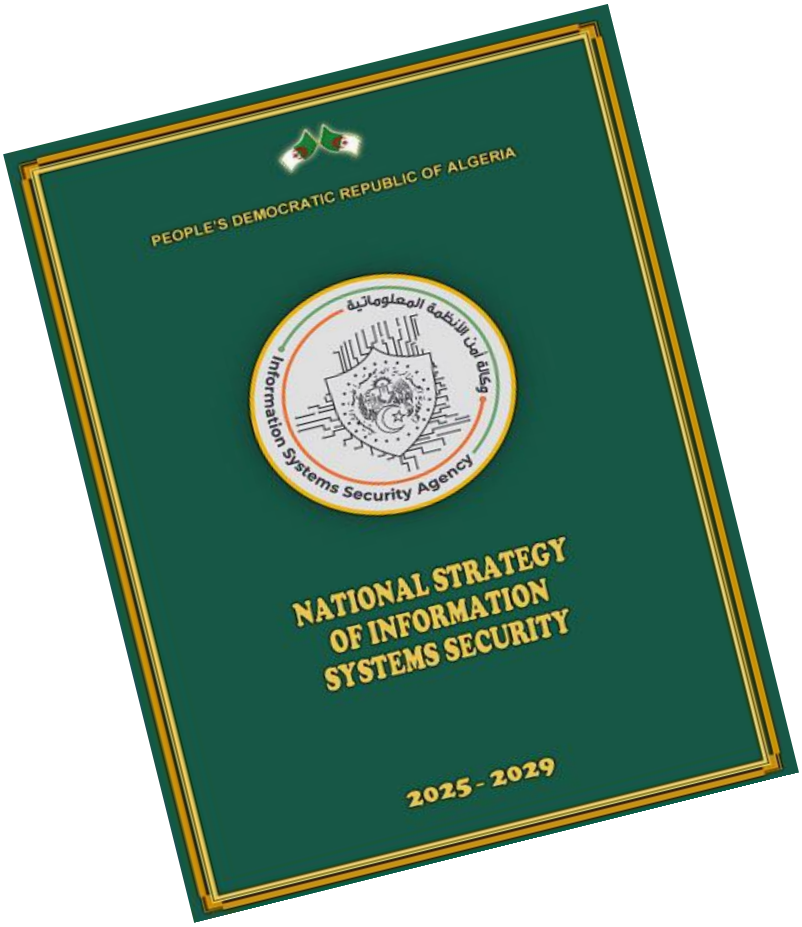

Figure 1 : National Strategy for Information Systems Security 2025-2029

The main objectives of the National Information Systems Security Strategy for the period 2025-2029

The strategy aims to: (Algerian and., 2026)

• Ensuring national cyber resilience by strengthening capabilities to prevent, detect, and respond to cyber incidents.
• Protecting the country's digital infrastructure and sensitive data.
• Building a safe and reliable digital environment that enhances citizens' confidence.
• Support comprehensive digital transformation while maintaining digital sovereignty.
• Develop qualified human resources and a strong legal and regulatory framework.
• Achieving maximum cyber performance in critical sectors while determining sensitivity levels.

The six basic guidelines

The strategy is based on six main principles: **(Algerian W., 2026)**

1. Strengthening national digital sovereignty.
2. Keeping pace with digital transformation.
3. Maintaining the technical gains achieved.
4. Comprehensive coordination between all relevant institutions.
5. Valuing resources (human and technical).
6. Achieving measurable goals within specific deadlines.

The main axes of the Algerian cybersecurity strategy

This strategy comes as part of the broader national trend towards digitalization (Digital Transformation Strategy to 2030), and relies on a participatory approach that benefited from the reports of the National Committee on Cybersecurity (Joan 2023) and analysis of national vulnerabilities. It is also linked to previous efforts such as the National Information Systems Security Directives (DNSSI) and the establishment of the National Cybersecurity Agency.

The strategy is divided into four main axes: technical-operational capabilities, the legal, regulatory, and normative framework, training, research, development, and awareness-raising, and national and international cooperation. The second axis appears to be the heart of the regulatory system because it aims to build a unified framework that coordinates technical protection, standards, and institutional compliance. These four axes are derived from a comprehensive approach known as comprehensive cybersecurity governance.

The first axis relates to technical-operational capabilities: This axis focuses on building the state's "digital immunity" by developing defensive and offensive infrastructure by protecting sensitive systems and structures with the aim of enhancing prevention and early detection of threats and thus responding quickly to incidents by taking the following actions and measures:

1- **Protecting critical infrastructure:** by identifying sensitive sectors (energy, health, finance, transportation) and imposing strict security standards to protect them from breaches that may halt their services.

2- **Establishing observatories:**

Cybersecurity observatories: to monitor networks and systems around the clock and analyze threats in real time.

Computer emergency response teams: These are specialized teams to deal with incidents when they occur, contain them, and restore services.

Risk Management and Compliance: Apply risk management frameworks and information to identify vulnerabilities before exploiting them.

Hybrid and proactive cybersecurity: moving from passive to proactive defense and the ability to detect ongoing advanced threats using artificial intelligence.

The second axis is specific to the legal, regulatory, and normative framework: This axis aims to create a legal environment that criminalizes malicious acts and regulates the use of data, thereby enhancing digital trust. It focuses primarily on building legislation and standards to achieve alignment with international standards. Strengthening the legal framework by following the following measures:

1- Cybercriminal legislation: Enacting laws that define cybercrimes (hacking, fraud, defamation) and specify deterrent penalties.

2- Protecting personal data: Issuing laws governing how individuals' data is collected, stored, and processed, to ensure their rights and privacy.

3- Regulatory control: defining the powers of government agencies responsible for cybersecurity and imposing licensing and professional practice on security service providers.

4- Harmonization with international standards: Adopting the standards of the Organization for Economic and Development Cooperation or the International Telecommunication Union to ensure the compatibility of local legislation with international law.

The third axis is training, research, development, and awareness: This axis focuses on the human element by forming competencies and consolidating a culture of cybersecurity while supporting research and innovation in this field, this axis is considered the most important because "the human being is the strong and original link of weakness in any system, and the most important thing that depends on him depends on:

1- Capacity building: Academic education through integrating cybersecurity specializations into universities and technical institutes, vocational qualification through establishing advanced training programs and granting accredited professional certificates to raise the efficiency of workers in the government and private sectors.

2- Public awareness and sensitization: Media campaigns to educate citizens about the dangers of electronic phishing, weak passwords, and electronic blackmail.

3- Innovation and scientific research: Funding research projects in the field of quantum cryptography, artificial intelligence for cybersecurity, and supporting startups working in this field to achieve technical self-sufficiency.

The fourth axis: National and international cooperation: No country can confront organized cyber threats alone. Therefore, this axis requires building alliances, as it is based on building partnerships aimed at enhancing cooperation between the public and private sectors, as well as international cooperation at the strategic and technical levels, through:

1- Public-private partnership: The private sector possesses the vast majority of infrastructure and technical expertise. This requires establishing mechanisms to share threat information between the government and large corporations such as banks and large corporations.

2- International cooperation: exchanging information and experiences with brotherly and friendly countries, participating in international forums, international legal cooperation to extradite cyber criminals fleeing across borders.

3- Establishing regional alliances: to secure the geographical region as a whole, such as Arab, African, or joint agreements.

From the above, we reach a conclusion that answers the question from which we started our study, which is that the National Cybersecurity Strategy in Algeria (2025-2029) achieves an effective balance between deterrence and infrastructure protection by moving from «the logic of technical protection» to «the logic of comprehensive cyber deterrence», with a focus on digital sovereignty as part of national sovereignty. This balance depends on four integrated axes:

1- Combining proactive deterrence and preventive protection: meaning cyber deterrence through early detection of attacks, building containment and rapid recovery capabilities, as well as adopting the logic of expectation and probability in anticipating threats. **(Bamrah and Rafiqah Zabdah, 2025)** Protecting infrastructure by securing government systems, reducing technical vulnerabilities, ensuring the continuity of vital services (energy, water,

communications), responding to incidents, developing rapid intervention mechanisms, containing digital damage, digital emergency plans).

2- Confronting accelerating technical challenges: by strengthening technical infrastructure and secure communication networks by investing in advanced security systems and artificial intelligence technologies, keeping pace with the accelerating digital transformation within state institutions by building a «parallel cyber shield» for digital expansion, and modernizing the legislative system to keep pace with technological developments.

3- Addressing weak community awareness: by organizing comprehensive awareness campaigns for citizens and institutions, as well as including the issue of cybersecurity in educational and training programs from the early stages, in addition to building a bloc of national competencies by establishing specialized training centers and encouraging scientific research.

4- Confronting cross-border threats: This is achieved by actively engaging in regional and international partnerships to confront cross-border threats. **(Asmaa, 2026, p. 96)** Strengthening cooperation between the government, the private sector, civil society, and international organizations, relying on international cooperation as a fundamental building block in Algerian politics.

Although this national cybersecurity strategy addresses many aspects to achieve the objectives for which it was developed, it faces challenges in implementing them. Therefore, enhancing effective coordination between relevant security, technical, and research institutions, overcoming limited specialized human resources, and providing sustainable funding and effective coordination between civilians and the military are required.

Conclusion:

We conclude from the above that the National Cybersecurity Strategy is not just an administrative document, but rather a "protective umbrella" for the national economy, state security, and citizens' privacy. Betting on technology alone without deterrent laws, qualified human competencies, and effective international cooperation is a losing bet. Therefore, activating these four axes is the inevitable approach to building a safe and stable digital state, capable of keeping pace with rapid developments and transforming cyber challenges into opportunities for innovation and leadership.

To ensure the strategy's transition from theory to actual implementation, we can monitor a set of practical recommendations, according to experts in the field, based on assigning responsibility and empowering the national authority. The role of the national authority responsible for cybersecurity should be activated and it should be granted full powers to oblige vital sectors to implement cybersecurity standards, monitor compliance, and impose sanctions when necessary, away from conflicts of powers with other authorities In addition to adopting a security-by-design approach, by not treating cybersecurity as a deterrent added after the completion of systems construction, but rather as an essential element integrated into the design of any government or private digital project from its inception, which reduces the financial and security cost in the future, it is also necessary to update legislation flexibly by reviewing laws periodically to keep

pace with technical developments and ensure that legislation does not become outdated, allowing for the prosecution of new criminals who invent unprecedented means of hacking Activating intelligence sharing mechanisms by creating secure, shared platforms between the public and private sectors to share information on threats in real time, creating "collective immunity" for the sector. Also, promoting a culture of security is everyone's responsibility, making every citizen a guardian of their own digital security.

List of References and Sources:

Books:

1- Eid, Fatima Ali. (2019). Cairo, Modern University, Cyber Challenges in Institutions. Egypt: Dar Al Nahda Al Arabiya.
2- Mohamed Kamal. (2022). Cyber terrorism. Cairo: Dar Kalim for Printing, Publishing and Distribution.
3- Ali Ziad Al-Ali and Hamid Ali Hussein. (2022). Modern warfare tactics: cybersecurity, enhanced warfare, and hybrid warfare. Al Arabi Publishing and Distribution.

Articles

1- Ahmed bin Issa. (2019). The role of cybersecurity in enhancing Algerian national security. Journal of Humanities and Social Sciences (44), page 45.
2- Islam Mustafa Jumaa Mustafa. (2022). The crime of hacking cybersecurity and protecting the use of data and information in Egyptian law. The Legal Journal is a journal specialized in legal studies and research, 12(03), page 07.
3- Rabie Al-Rafei. (01/31/2021). International terrorism and its relationship to organized crime: cyber terrorism as an example. Journal of Law and Political Science, 07(01), p. 73.
4- Help with a pinch. (2022). Cybersecurity: risks, threats and challenges that require special practices, recommendations and strategies. Journal of Research in Social Protection, 03(01), p. 125.
5- Saleh Mahdi Hadi Al-Shammari and Zaid Muhammad Ali Ismail. (2020). Cybersecurity as a new pillar of Iraqi strategy. Journal of Political Issues (62), page 277.
6- Qasim, Nadia. (2022). Cyber policies in Algeria. National Conference on Cybersecurity. National Center for Strategic Studies.
7- Lubna Khamis Mahdi. (2020). The impact of cyber on the development of power. Hammurabi Magazine, 33-34, p. 148.
8- Mona Abdullah Al-Samhan. (2020). Requirements for achieving cybersecurity and administrative information systems at King Saud University. Journal of the College of Education (11), page 11.
9- Nasser bin Abdullah Al-Qahtani. (2020). Cyber-attacks and their impact on national security. Journal of Security and Strategic Studies, 35(02), p. 150.
10- Warat Shaloush. (2018). Cyber piracy in cyberspace is a "rising threat to the security of states." Journal of the Babylon Center for Human Studies, 08(02), p. 191.

11- Muhammad Jawad Bamrah and Rafiqah Zubdah. (13 03, 2025). Algeria's Defense Strategy for Addressing Cyber Threats. Al-Risala Journal of Human Studies and Research, 10(01), p. 880.

Theses:

1- Ben Jeddo Asmaa. (2026). Cybersecurity policies in Algeria in light of international threats (2008-2025). Doctoral thesis, 96. Amhamed Bougherra Boumerdes University: Faculty of Law and Political Science, Algeria.

Official publications:

1- Official Gazette. (2018). Law 90-01 on e-commerce. Official Gazette (28).
2- Official Gazette. (2018). Law No. 18-04 establishing general rules relating to mail and electronic communications. Official Gazette (27), 27.

Websites:

1- Algerian Ministry of Defense. (03 03, 2026). Ministry of National Defense. Recovery date: 05/19/2026, from the Ministry of National Defense: https://www.mdn.dz/assi/nsiss_ar.pdf
2- Algerian News Agency. (03 03, 2026). Revealing the content of the National Strategy for Information Systems Security for the period 2025-2029. Refund date 05/19/2026, from Wag Online: https://www.aps.dz/algerie/actualite-nationale