

Requirements for Enhancing Cybersecurity in Algerian Banks to Support Modern Payment Systems

Souaad El miloudi

Chlef University (Algeria), s.elmiloudi@univ-chlef.dz ,

ORCID: <https://orcid.org/0009-0003-5442-233X>

Fatima Fouka

Chlef University (Algeria), f.fouka@univ-chlef.dz

ORCID: <https://orcid.org/0009-0001-7146-6081>

Received : 17.10.2025

Accepted: 30.12.2025

Published : 01.01.2026

Abstract: This study aims to analyse the role of cybersecurity in supporting and enhancing electronic payment systems amid the rapid pace of digital transformation, with particular attention to the extent of integration of information and communication technology within the banking sector. To achieve its objectives, the study employs an analytical and applied methodology through a case study of Algerian banks, aiming to assess the effectiveness of cybersecurity systems in improving the efficiency and security of electronic payment mechanisms. The results indicate a complementary relationship between cybersecurity and the activation of electronic payment systems: the higher the level of cybersecurity protection, the greater the efficiency and reliability of these systems. Although Algeria's experience remains in its developmental stage, it represents a vital step toward enhancing the performance of electronic banking services and fostering greater confidence in digital financial transactions.

Keywords: Cybersecurity; Electronic payment methods; Information and communication technology; Algerian banks.

JEL Classification Codes : E42, G21, G28, L86.

Corresponding author: Souaad El miloudi, s.elmiloudi@univ-chlef.dz.

Introduction:

In recent years, the global economy has undergone profound transformations driven by globalization, which has bridged geographical distances, erased traditional boundaries, and compressed time. These shifts have been further accelerated by the emergence of information and communication technologies and their extensive application across all facets of human activity, particularly within the economic sphere. The aim has been to deliver high-quality and cost-efficient services capable of maximizing institutional profitability and ensuring long-term competitiveness in increasingly dynamic markets. Among the sectors that have notably expanded their investments in information technology are banks and financial institutions, given their substantial financial capacities, which enable them to market their services effectively within the virtual economy—an economy that has evolved into a necessity rather than a mere option under the pressures of intense competition.

In parallel with technological advancement and the rise of electronic payment methods, these institutions have faced new technological challenges, foremost among them the threat of cyberattacks—one of the most severe economic crimes targeting bank accounts. Such attacks undermine operational integrity, damage institutional reputation, and erode public confidence, ultimately threatening the sustainability of financial institutions in the marketplace. In light of this evolving digital landscape and the recurring risks associated with the continuous implementation of electronic services, it has become crucial to identify viable solutions to the challenges obstructing the development and activation of electronic payment systems within Algerian banks. Addressing these challenges requires the adoption of comprehensive measures to protect information, devices, and software from illicit acts of hacking—a process that constitutes the foundation of cybersecurity and enables banks to maintain operational resilience in an increasingly competitive financial environment.

Research Problem: Based on the foregoing, the central research problem can be articulated as follows: **What are the essential requirements for strengthening cybersecurity in Algerian banks to effectively support and secure modern electronic payment systems?**

Research Hypotheses:

- Enhancing cybersecurity infrastructure contributes to the advancement and support of electronic payment methods within Algerian banks.
- Flexibility in cybersecurity strategies enables banks to confront the evolving and diverse nature of cyberattacks resulting from the multiplicity of actors and the variability of their techniques.
- The greater the dependence on electronic payment methods, the stronger the need for a resilient and secure cyber environment.

Study Significance: The significance of this study lies in its exploration of cybersecurity—a field that has become increasingly essential for the activation and protection of electronic banking services against diverse threats. This importance stems from the implementation of security measures designed to safeguard information, devices, and systems from any unlawful acts of hacking or unauthorized access.

Study Objectives: This study aims to achieve the following objectives:

- To examine the evolution of electronic payment methods and cybersecurity;
- To determine the relationship between cybersecurity and the development of electronic payment methods in the banking sector;

- To assess the status of electronic payment methods in Algerian banks and identify the constraints that have limited their expansion;
- To highlight the role of cybersecurity in activating electronic payment methods by presenting relevant mechanisms and frameworks and applying them to the Algerian context.

Research Methodology: This study adopts a deductive approach employing descriptive and analytical methods to clarify the importance of enhancing the implementation of cybersecurity for the development and protection of electronic payment systems, with particular reference to Algerian banks.

2. Conceptual Framework of Cybersecurity and Cyber Risks

Cybersecurity refers to a comprehensive set of procedures and measures implemented to safeguard information from threats, breaches, and unauthorized access. Its primary goal is to ensure the confidentiality, integrity, and availability of data and information for authorized stakeholders.

2.1. Cybersecurity Threats

Definition of Cybercrime: To begin, it is essential to understand the nature of cybercrime, which represents the principal threat that must be addressed. Based on the legal principle of “no crime and no punishment without a legal provision,” many countries have enacted specific legislation to combat such offenses, which encompass a broad spectrum of unlawful activities. These include acts in which computers and communication networks are used either as tools for committing crimes or as direct targets—ranging from hacking information systems and communication infrastructures to launching attacks that disrupt or disable services.

Nevertheless, due to the absence of a comprehensive and universally accepted definition of cybercrime, it is more appropriate to rely on definitions established by specialized international bodies. In a workshop addressing crimes associated with digital networks, these offenses were classified into two primary categories: (Baghdawi, 2021, pp. 1459–1460)

- The first category, based on the narrow definition, includes “any unlawful act committed through electronic means that targets the security of information systems and the data they contain.”
- The second category, based on the broader definition, encompasses “any unlawful act committed through or in connection with information systems,” including crimes such as unauthorized possession, the provision of illegal services, or the dissemination of information via information systems or communication networks.

Furthermore, the European Convention on Cybercrime identifies acts considered illegal, addressing crimes that infringe upon the confidentiality, integrity, and availability of systems and data, as well as offenses related to content and intellectual property rights.

Definition of Cyber Risks: Cyber risks are defined as “operational risks associated with information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems.” When compared to the categories of risks covered by insurance, cyber risks share certain characteristics and liabilities with property, liability, catastrophic, and operational risks. (Baghdawi, 2021, pp. 1460–1461)

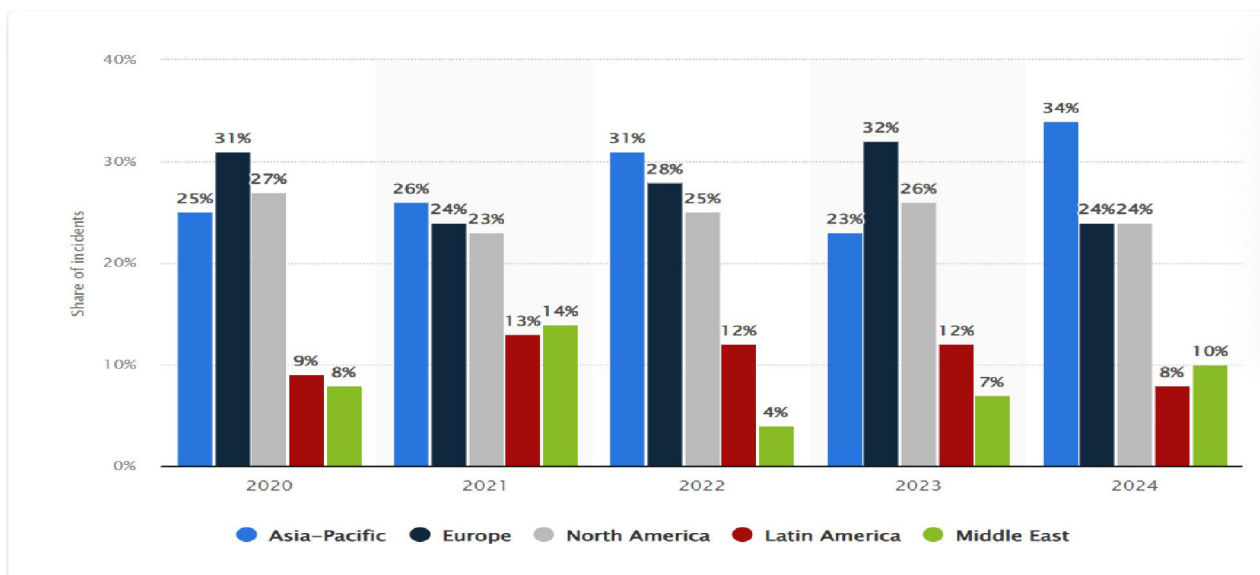
From another perspective, cyber risks may initially affect the targeted entity and subsequently its counterparties. The losses resulting from such risks are often minor and isolated;

however, in some cases, they may occur infrequently yet produce large-scale impacts—a phenomenon referred to as the “opacity policy.”

Cyber risks can also be described as “all criminal practices occurring in cyberspace that target individuals, institutions, or governments.” These risks can be categorized into two types: the first targets digital devices and information networks, while the second targets individuals who use the internet either for personal purposes or within their professional roles in governmental institutions.

Personal purposes or within their professional roles in governmental institutions. In this context, the International Monetary Fund (IMF) provides estimates regarding the financial impact of cyberattacks on the banking sector, based on actual loss data collected from 50 countries worldwide. According to these estimates, the potential average annual losses resulting from cyberattacks could be considerable—amounting to approximately 9 percent of banks’ net income globally, or about USD 100 billion, assuming that future incidents occur on a scale similar to previous attacks. In a high-risk scenario, where the frequency of cyberattacks doubles compared with past levels and the scope of losses widens, total losses could increase up to threefold, ranging between USD 270 and 350 billion. (Ismail, 2019, pp. 1–2)

Figure 01. Distribution of Cybercrimes Worldwide, 2020–2024



Source: Statista 2025

In 2024, the Asia-Pacific region was the most affected by cyberattacks compared with other regions, accounting for 34% of total incidents—representing a significant rise from 23% recorded the previous year. Europe and North America ranked second and third, each representing approximately 25% of reported cases. Meanwhile, Middle Eastern countries accounted for 10% of total global cyberattacks. Regarding the geographical distribution of cyberattacks, China and the United States hold the leading positions in terms of the number of victims, due to their strong economic and political influence and their advanced use of financial technology. The extensive adoption of digital systems in these countries has made them frequent targets of cyberattacks. Consequently, both nations—along with others—have adopted multiple cybersecurity strategies to protect themselves against these recurring threats.

In 2024, the Asia-Pacific region was the most affected by cyberattacks compared with other regions, accounting for 34% of total incidents, marking a significant increase from the 23% recorded the previous year. Europe and North America ranked second and third, each representing approximately 25% of reported attacks. Meanwhile, Middle Eastern countries accounted for 10% of total global cyber incidents.

Regarding the distribution of cyberattacks by country, China and the United States hold the leading positions in terms of the number of victims, owing to their strong economic and political influence and their advanced use of financial technology. This extensive reliance on digital systems has made both countries frequent targets of cyberattacks. Consequently, they—along with other nations—have implemented multiple cybersecurity strategies to safeguard against these recurring threats.

2.2 The Nature and Types of Cyber Risks

Cyber risks manifest in various forms, including viruses, cyberbullying, defamation, hacking, and phishing. According to 2020 statistics, 28% of cyberattacks on data involved the use of viruses, while 52% were executed through hacking techniques.

The main types of cyber risks can be summarized as follows: (Kaoua, 2020, pp. 174–175)

Viruses: These are malicious computer programs that spread across digital devices in multiple ways, replicating among files and causing serious damage. They differ in form, intensity, and persistence within digital environments, and their impact can escalate to the extent of destroying digital infrastructures and disrupting operations.

Cyberbullying: Cyberbullying is among the most prevalent forms of cybercrime, particularly affecting school and university students. It is classified as a type of digital harassment that inflicts sustained harm on victims through monitoring, intimidation, threats, or humiliation, and often involves coercion through exposure or disgrace. This phenomenon has witnessed a notable increase in recent years.

Defamation: This form of cyber risk targets individuals by spreading false or misleading information intended to damage reputations or diminish social standing. It may involve falsified or manipulated images and videos created for criminal purposes and disseminated through social media platforms or email. Institutions may also be targeted to tarnish their public image and undermine their competitive position in the market.

Hacking: Hacking refers to unauthorized intrusion into digital information systems with the purpose of breaching security defenses and accessing confidential data belonging to individuals, institutions, or governments, thereby causing financial or reputational harm. To gain a clearer understanding of the situation, it is useful to consider relevant global statistics. As of April 2022, there were five billion internet users worldwide, of whom 93% were social media users—representing approximately 60% of the global population, with an annual growth rate of 300 million new users.

Phishing: Phishing is among the simplest forms of cyber risk to execute. In such attacks, the perpetrator creates a counterfeit website—often impersonating a legitimate organization or company—and sends fraudulent emails from that domain to obtain personal data and information for criminal use.

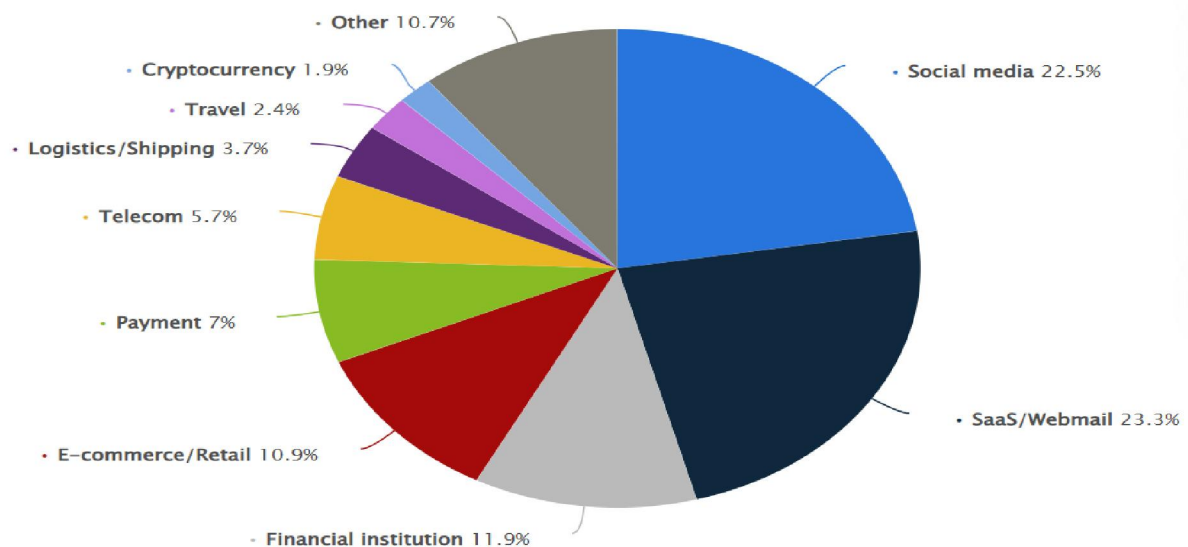
Cyberterrorism: Terrorist organizations exploit the internet to conduct a variety of activities, including recruitment, financing, propaganda, training, incitement to commit acts of terrorism,

and gathering or disseminating information for terrorist purposes. The internet also facilitates communication and coordination among different terrorist groups.

Information Security Breaches: All uses of information systems and digital applications hosted on computer networks are vulnerable to harmful attacks, failures, or breaches of data confidentiality. Such incidents can compromise the privacy of institutional and client information or delay data accessibility when urgently required. The risks arise from unauthorized access, improper or illegal use, or system failure caused by accidental factors. Numerous information systems and digital applications—both public and private, including those used in military, security, banking, and medical contexts—constitute fertile ground for the escalating threat of information terrorism.

Intellectual Property: This includes damages resulting from acts such as attributing a scientific work to a false claimant, falsifying an author's seal, or infringing upon any of the rights of authors or related rights.

Figure 02. Proportions of Cyberattacks by Sector in 2024



Source: Statista 2024

Certain sectors captured the largest share of global phishing attacks according to Statista data:

- **Social Media Networks:** approximately **23%** of attacks;
- **Web-based Software Services (SaaS) and Online Webmail:** more than **23%** of attacks;
- **Financial Institutions:** **12%** of attacks.

2.1 The Concept of Cybersecurity

The term *cyber* originates from the Latin word *cyber*, meaning imaginary or virtual. It is commonly used to describe the space encompassing computerized web networks, communication and information systems, and remote-control technologies. The term broadly refers to everything associated with computers, information technology, and virtual reality. From it is derived the adjective *cybernetic* or *cyber*, which signifies the science of automatic control or regulation and also denotes command or guidance. (Al-Baalbaki, 2008, p. 243)

The applications and uses of cyberspace differ across countries depending on their national priorities-whether these are security, political, intelligence, civil, or purely informational. Generally, the cyber domain in most nations consists of three essential components: hardware systems, digital software, and human resources, including programmers and users. (Abdel Sadiq, 2013, p. 35)

To clarify the notion of “risks,” it is first necessary to understand the environment in which they arise—namely, cyberspace. Cyberspace is defined as “the medium within which cyber computer networks exist and operate, including computers, network systems, software, data processing, transmission and storage, as well as their human, institutional, and organizational users.” Hence, cyberspace emerges as a network formed by interconnected computer systems. (Abdel Sadiq, 2013, p. 36)

Cybersecurity is defined as the science that aims to “provide a degree of protection against internet crimes.” (Al-Deeb, 2005, p. 19) This involves safeguarding information and protecting it from unauthorized access or hacking attempts.

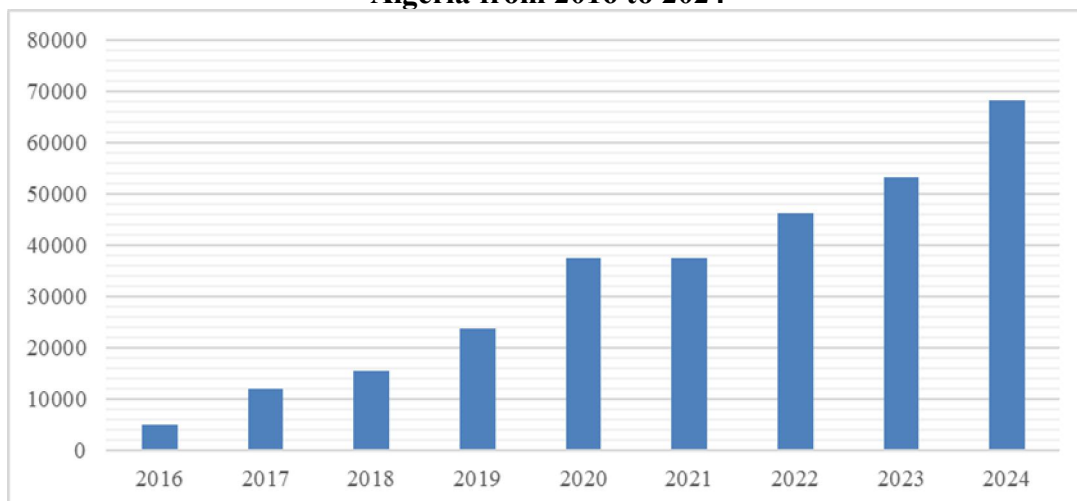
“Cybersecurity involves the application and management of techniques with the aim of protecting the confidentiality, integrity, and availability of information and information assets in cyberspace.” (Grispos, 2021)

3. The Development of Electronic Payment Methods in Algeria

With the technological advancements witnessed globally in the fields of information and communication, vast and diverse markets have opened up for the banking sector in many developed countries. Through the adoption of electronic banking methods, banks have achieved substantial financial returns. In response to the global shift toward electronic banking, Algerian banks have found it necessary to modernize their services by adopting the foundations of electronic banking. (Ben Omar & Bourzama, 2019, p. 98)

Despite the efforts made to promote a culture of electronic banking in Algeria, the reality of the sector reveals a significant delay and a noticeable gap compared to international banking standards. The services provided by Algerian banks have remained largely traditional, failing to align with the modern banking services offered by financial institutions in developed countries.

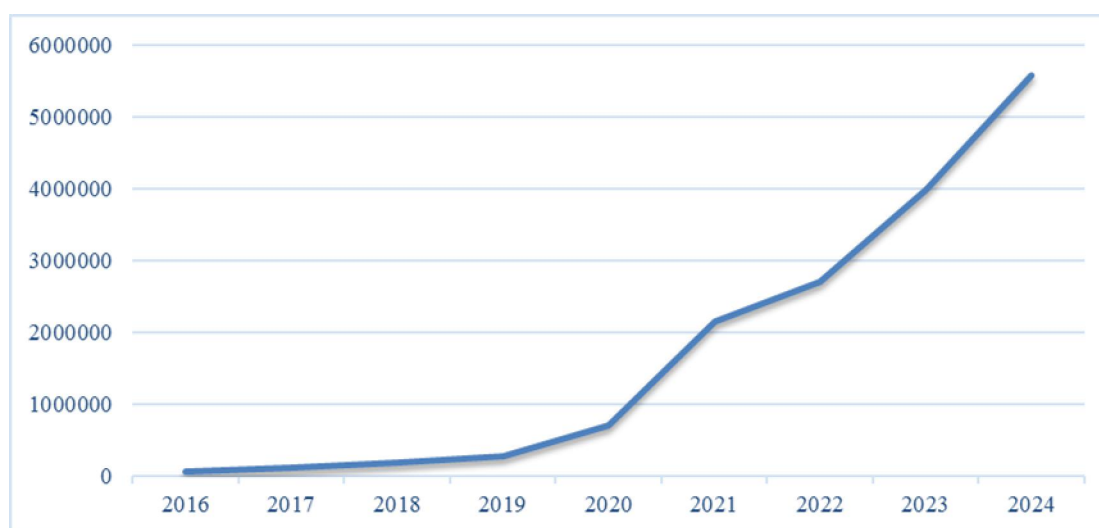
Figure 03. The Evolution of the Number of Electronic Payment Terminals Operating in Algeria from 2016 to 2024



Source: Prepared by the researchers based on data from the Groupement d'Intérêt Économique Monétique (GIE Monétique), accessed on 10/07/2025 – <https://giemonetique.dz>

From the bar chart in the figure above, it is observed that there has been growth in the total number of active payment terminals in Algeria, showing a continuous increase from year to year. In 2016, the number of payment terminals was estimated at 5,049, reaching 68,140 in 2024—an increase of 63,091 terminals over eight years. This reflects a genuine commitment to narrowing the gap and demonstrates a significant expansion in the infrastructure of electronic payment systems.

Figure 04. The Evolution of Electronic Payment Activity in Algeria from 2016 to 2024



Source: Prepared by the researchers based on data from the Groupement d'Intérêt Économique Monétique (GIE Monétique), accessed on 10/07/2025 – <https://giemonetique.dz>

Based on the curve above, it is clear that the total number of payment transactions experienced a gradual yet strong increase from 2016 to 2019. This period represents the actual starting point of electronic payments in Algeria, with the introduction of online payment systems and point-of-sale (POS/TPE) operations. Between 2019 and 2024, the sector entered a phase of rapid expansion and diversification, marked by the emergence of mobile payment services and a significant acceleration in online activities.

The sharp rise in cash withdrawal transactions in 2020 was primarily due to Algérie Poste joining the Automated Teller Machine (ATM) network, which enabled interoperability between the Bank Card and the Gold Card, effective from January 5, 2020. This development resulted in a substantial increase in electronic payment activities through both types of cards. Additionally, the exceptional circumstances caused by the COVID-19 pandemic affected traditional payment practices, encouraging a greater reliance on electronic payment methods and supporting the implementation of financial inclusion principles.

4. Mechanisms for Establishing a Secure Cyber Environment to Develop Electronic Payment Systems in Algerian Banks

4.1. The Algerian Strategy for Cybersecurity

Algeria has adopted a comprehensive approach to cybersecurity that includes legal, technical, operational, and capacity-building measures, along with international cooperation aimed at strengthening national cyber resilience.

4.2 The State of Cybersecurity in Algeria

Algeria's interest in the legal dimension of cybersecurity began relatively early. In 2004, Law No. 04-15 was enacted, amending the Penal Code. This law introduced Section 7 bis, which specifically addresses offenses related to automated data processing systems. It established penalties for any act or behavior that could damage or compromise data, institutions, or organizations, as stated in Article 394 bis (Law No. 04-15, 2004, p. 8).

In 2009, Law No. 09-04 was issued, defining the specific rules for preventing and combating crimes related to information and communication technologies (Law No. 09-04, August 5, 2009, p. 5). Article 2 of this law provides a detailed explanation of the concept of crimes associated with information and communication technologies and sets out the procedural rules for monitoring electronic communications and inspecting information systems.

In 2018, Law No. 18-07 was introduced, concerning the protection of natural persons in the processing of personal data (Law No. 18-07, June 10, 2018, p. 11). This law elaborates on the concept of personal data, its processing mechanisms, and the fundamental principles for protecting such data in a manner that upholds human dignity and prevents any violation of privacy.

From a technical perspective, ensuring cybersecurity requires the availability of material resources capable of limiting the risks of cyberattacks and electronic crimes. Within this framework, Algeria established the National Space Strategy for 2020–2040, which aims to secure institutional communications, reduce the digital divide, and enable citizens to actively participate in the global information society.

Furthermore, Algeria created the DZ-CERT (Computer Emergency Response Team), affiliated with the Research Center for Scientific and Technical Information (CERIST) (Bouriah, 2023, pp. 285–286). This team plays a vital role in safeguarding sensitive information by detecting emerging digital threats such as viruses, spyware, and system vulnerabilities, providing appropriate measures, and recommending solutions to address them.

Additionally, Algérie Télécom launched cybersecurity services for national companies and institutions aimed at protecting corporate resources from cyberattacks and internet-based threats (Algeria, 2025). This initiative is particularly significant given the widespread use of non-original and counterfeit software, which exposes data to hacking and theft. Such vulnerabilities remain one of the main challenges to cybersecurity for institutions and individuals alike, emphasizing the necessity of adopting effective protection mechanisms.

4.3 Algeria's Efforts to Build Technical Capacities and Foster International Cooperation in the Field of Cybersecurity

Regarding the development of technical and specialized capacities, Algeria officially opened the field of cybersecurity education in 2018, announcing the training of 24,000 engineers and technicians specialized in cybersecurity. (Bouziyan, 2018) The country also provided advanced and specialized training for security and space experts in the fields of electronic crime technologies and related legislation. The government's new orientation toward encouraging technological innovation led to the creation of Algerian start-up companies specializing in cybersecurity, such as Secure Network (securenetworkdz.com, 2016).

Furthermore, the Ministry of Higher Education and Scientific Research launched pedagogical training programs in technical, social, and institutional disciplines aimed at

strengthening focus on cybersecurity, particularly in the development of national expertise. This initiative culminated in the establishment of the National Higher School specialized in Cybersecurity in 2023.

In terms of international cooperation, Algeria has signed a number of international and regional agreements in the field of cybersecurity, including the Budapest Convention of 2001 (the European Convention on Cybercrime). It also participated in drafting and ratifying several agreements under the League of Arab States concerning the exchange of information and expertise, cooperation in data protection, combating cybercrime, and the extradition of offenders in cases related to cybersecurity. Among these is the *Arab Convention on Combating Information Technology Crimes*, adopted in Cairo in 2010.

Additionally, Algeria hosted the first meeting of the Regional Office of the Arab Telecommunication Union on February 25–26, 2013. This office includes specialized working groups responsible for coordinating Arab efforts, harmonizing strategic visions, and establishing unified legal frameworks. (Khalaf, 2015, p. 14)

At the African Union level, Algeria ratified the *African Union Convention on Cybersecurity and the Protection of Personal Data* (2014). Furthermore, within the framework of the cooperation agreement launched by AFRIPOL, Algeria supervises the training of cybercrime experts from member states of the African Union.

The Algerian legislator has also structured the legal procedures for international cooperation through Law No. 09-04. Article 15 of this law grants Algerian criminal courts jurisdiction over cybercrimes committed outside the national territory when the perpetrator is a foreign national targeting Algerian state institutions, national defense, or the strategic interests of the national economy.

Supervision of such crimes was entrusted to the *National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies*, as stipulated in Article 13. This article defines the Authority's responsibilities, which include the exchange of information with its foreign counterparts to collect data useful for identifying cybercrime perpetrators and determining their locations. (Kadri, 2023, p. 313)

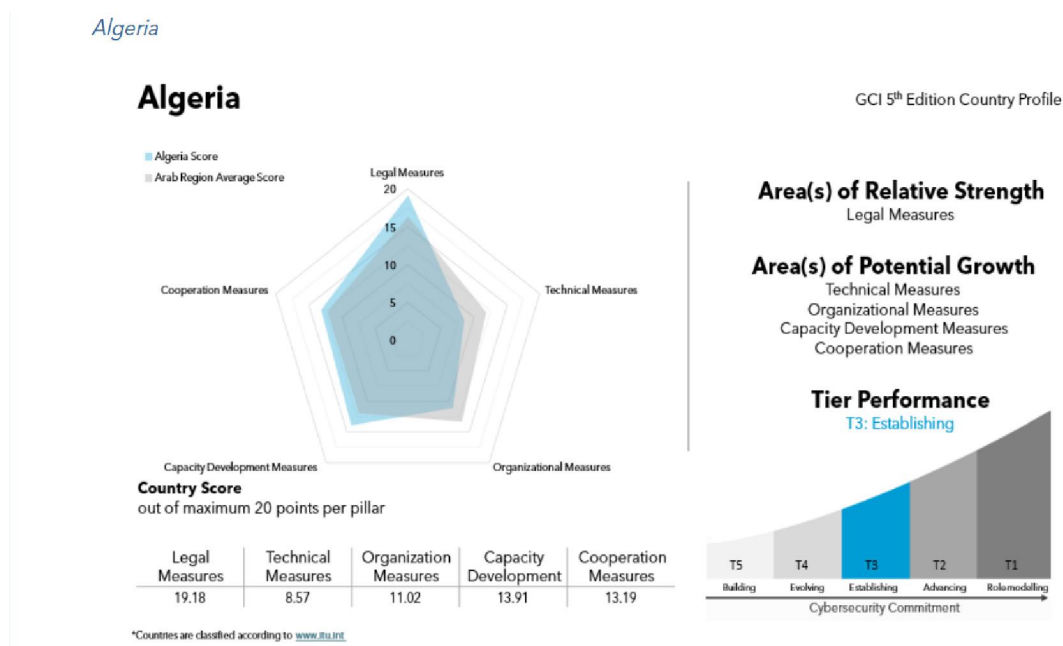
Algeria has also concentrated its efforts on technical and operational dimensions by participating in several international training workshops organized in cooperation with the *European Cybercrime Program*. The country has chaired the *INTERPOL Expert Group* specialized in combating cybercrime, a role granted in recognition of the expertise and experience of Algerian law enforcement authorities in this field.

Within the framework of exchange and cooperation, Algeria consistently takes part in major international exhibitions on innovation and technological development, such as *GITEX Technology Week 2019* and *Axxir Expo*. It also organizes the annual *DIGITECH International Exhibition for Information and Communication Technologies*—whose fourth edition was held in 2023—alongside various national exhibitions conducted in partnership with prominent companies in the fields of telecommunications and information technology. (Mahmoudi, 2023, pp. 206–207)

According to the *Global Cybersecurity Index 2024* report issued by the *International Telecommunication Union (ITU)*:

- Algeria was ranked within Tier 3 – Establishing, representing the foundational stage in the maturity of its cybersecurity framework.

- The country achieved an overall score of 65.87 out of 100, indicating that it has made notable progress in building its cybersecurity infrastructure but still requires further development to reach higher stages of maturity.



Source: ITU, 2024, p. 70

Furthermore, according to the *DIGITAL 2024* report issued by *DataReportal*—a company specializing in global internet and mobile statistics—Algeria recorded significant growth in internet and social media usage in 2024. The number of internet users in Algeria reached 33.49 million, corresponding to a connectivity rate of 72.9%. This indicates that approximately three out of every four Algerians are connected to the internet, a remarkable achievement for a developing nation that only a few years ago faced considerable challenges in digital infrastructure.

4.4 Institutions and Bodies Specialized in Cybersecurity in Algeria:

Like many other nations, Algeria has established specialized institutions for implementing cybersecurity measures to ensure the safety of its cyberspace. These institutions are divided into administrative and operational entities, as follows:

- The National Authority for the Control and Combating of Crimes Related to Information and Communication Technologies
- The Agency for Information Systems Security
- The National Council for Information Systems Security
- The Center for the Prevention of Computer and Information Crimes
- The National Institute of Forensic Evidence and Criminology
- The Central Department for Combating Cybercrime

4.5 Requirements for Establishing Cybersecurity to Develop Electronic Payment Systems in Algerian Banks

To achieve a secure banking environment for electronic operations, banks must adhere to the following strategies:

Developing Cyber Maps and Quantitative Risk Assessment: Assessing cybersecurity risks in the banking sector helps in prioritizing and implementing appropriate controls and procedures to mitigate cyber risks and ensure compliance with relevant regulations and standards. This involves examining best practices in managing cybersecurity risks within the banking sector, including quantitative and qualitative approaches, threat modeling, and scenario analysis—each possessing strengths and weaknesses that must be evaluated according to the banking context. Emphasis should be placed on integrating proactive threat intelligence and continuous monitoring (Akindote, Omotosho, Dawodu, Adegbite, & Ewuga, 2023).

Developing Cybersecurity Culture: Assessing cybersecurity risks within the banking sector is essential for determining priorities and implementing effective controls and procedures to mitigate cyber threats while ensuring compliance with relevant regulations and standards. This process entails an in-depth examination of best practices in cybersecurity risk management in the banking environment, encompassing both quantitative and qualitative methodologies, threat modeling, and scenario analysis. Each of these approaches presents distinct advantages and limitations that must be assessed in accordance with the specific operational and regulatory context of banking institutions. Particular attention should be directed toward the integration of proactive threat intelligence and continuous monitoring mechanisms to strengthen resilience and maintain preparedness against evolving cyber threats (Akindote, Omotosho, Dawodu, Adegbite, & Ewuga, 2023).

Developing Cybersecurity Culture: Cyber culture constitutes a crucial element in reinforcing information security within financial institutions, as it embodies the collective awareness, understanding, and behavioral practices of employees in addressing digital threats. The establishment of cyber awareness within banks is based on four core pillars: adherence to cybersecurity compliance requirements, active support from senior management, adequate budgetary allocation, and the cultivation of an overarching security-oriented organizational culture. This is primarily achieved through comprehensive training and awareness programs targeting users and employees at various institutional levels (Al-Alwi & Al-Bassam, 2019).

Regulatory Convergence: International regulatory convergence represents a fundamental driver for enhancing cybersecurity of the financial sector. It directly contributes to reducing compliance costs and promoting cross-border regulatory cooperation. Disparities and inconsistencies among national regulatory frameworks increase the operational burden on financial institutions, diverting their resources toward navigating complex compliance requirements rather than strengthening effective cybersecurity measures (Zhou, Liu, & Zhang, 2021).

Furthermore, regulatory convergence fosters a robust foundation for enhancing the exchange of information and expertise among national and international regulatory authorities. This cooperation facilitates more rapid, coordinated responses to cross-border cyber incidents and bolsters the confidence of users and investors in the digital financial ecosystem (Arora & Rahman, 2022). In this context, national authorities must engage collaboratively with international organizations to activate and implement unified regulatory frameworks, ensuring the development of a secure, resilient, and advanced cyber environment capable of safeguarding financial systems and sensitive data against escalating cyber risks (Bada, Sasse, & Nurse, 2021).

Willingness for Joint Action: Enhancing the exchange of information on cyber threats, attacks, and response measures between public and private sector entities significantly strengthens deterrence capabilities and response effectiveness. Nevertheless, substantial challenges persist,

primarily arising from national security considerations and data protection legislation. Consequently, supervisory authorities and central banks must establish well-defined protocols and practices for information sharing that remain effective within these constraints. These barriers can be mitigated through the adoption of globally harmonized models for information exchange, the expansion of shared data platforms, and the strengthening of trusted communication networks (Elliott & Jenkinson, 2020).

Expansion of Secured Digital Services: This expansion encompasses services such as *Switch Mobile* and the widespread adoption of its use, as Algeria's electronic payment ecosystem undergoes a rapid digital transformation supported by the growth of secured digital services. A notable example is the launch of the *Switch Mobile* platform in June 2024, a strategic initiative aimed at achieving interoperability among various banks and the Algerian Post through payment technologies utilizing QR codes. This innovation enables users to perform instant payments and transfers via smartphones, thereby improving efficiency and accessibility (APS, 2024).

The platform recorded over 26.7 million transactions during the first half of 2024, totaling more than 19.6 billion Algerian dinars, representing a 60% increase compared to the same period of the previous year (EcoTimesDz, 2024).

Capacity Development: Effectively leveraging technology while maintaining security and safety remains a central pillar of sustainable development. It is therefore imperative to ensure that cybersecurity risks are properly identified, monitored, and managed in alignment with broader developmental and institutional objectives (Elliott & Jenkinson, 2020).

Cybersecurity Governance: Numerous researchers have examined and defined the concept of Information Security Governance (ISG), emphasizing its crucial role in safeguarding organizations and enabling them to achieve their strategic objectives. ISG is defined as a set of processes that determine how information security is managed and directed at the senior management level. It has also been described as a framework of procedures that delineate the degree of involvement and responsibility of senior management and departments within the organization (Al Ghamdi, Khin Than, & Vlahu-Gjorgievska, 2020).

Moreover, ISG facilitates the establishment of responsibility, accountability, and risk management mechanisms at the senior management level, ensuring continuous commitment and support for organizational objectives. This alignment between corporate goals and security protection strengthens overall governance. Various studies have demonstrated that ISG represents an effective solution to many cybersecurity challenges, as it promotes executive-level commitment, reinforces accountability and transparency, aligns organizational objectives with security priorities, enhances both corporate and security culture, and fosters effective communication among stakeholders within the organization (Al Ghamdi, Khin Than, & Vlahu-Gjorgievska, 2020).

5. Conclusion

This study aimed to analyze the role of cybersecurity in protecting electronic payment systems by exploring the relationship between electronic payment mechanisms and cyber risks, and by highlighting the complementary connection that exists between them. The stronger the cybersecurity infrastructure, the more efficient and reliable electronic payment systems become, as cybersecurity ensures confidentiality, integrity, and speed—core principles essential to banking operations and service enhancement.

The adoption of comprehensive cybersecurity measures plays a pivotal role in safeguarding electronic payment systems and achieving efficient electronic banking in Algeria. Therefore, Algerian banks should advance electronic banking practices within a secure and well-structured framework by adhering to the following recommendations:

- Regulatory authorities and institutions should provide advanced training programs, organize seminars, workshops, and conferences in collaboration with leading international technology companies and specialized institutions. These initiatives would enable professionals to stay abreast of rapid global developments in electronic services, creating a highly skilled workforce capable of addressing emerging technological challenges and developing effective responses to them.
- Algerian financial institutions and banks must acquire and implement the latest technologies—both hardware and software—to counter emerging cyber threats and international hacking techniques. This will allow for the establishment of more resilient security infrastructures capable of preventing and mitigating sophisticated cyberattacks.
- Introducing cybersecurity as a specialized academic field within Algerian universities focused on information technology is essential for developing professionals with advanced expertise in this increasingly vital domain.
- Regulatory authorities should issue clear and binding regulations governing the relationships between banks, financial institutions, and third-party entities specializing in information systems security. Such external partners entrusted with sensitive operational tasks must be subjected to strict supervision by national security agencies to minimize fraud, data breaches, and hacking attempts targeting financial systems.
- Financial institutions should allocate adequate budgets and resources to procure and maintain the most advanced cybersecurity technologies, given the substantial costs involved in securing critical information systems.
- Public awareness efforts should be intensified through media programs and educational seminars to foster a stronger cybersecurity culture among clients in the financial and banking sectors. Enhancing users' understanding of cybersecurity principles and best practices will reduce risks and strengthen overall resilience.
- Greater emphasis should be placed on conducting both partial and comprehensive stress tests to evaluate the potential impacts of cyber risks on banking operations and to enhance institutional preparedness.

6. References

- Abdel-Sadik, A. (2013). *Cyberspace and Public Opinion: Social Change, Tools, and Influence*. Arab Center for Cyber Research: Strategic Issues Series, 2459.
- Akindote, O., Omotosho, A., Dawodu, S., Adegbite, A., & Ewuga, S. (2023). *Cybersecurity Risk Assessment in Banking: Methodologies and Best Practices*. *Computer Science & IT Research Journal*, 3(4), 220–243. doi:10.51594/csitrj.v4i3.659
- Al Ghamdi, S., Khin Than, W., & Vlahu-Gjorgievska, E. (2020). *Information Security Governance Challenges and Critical Success Factors: Systematic Review*. *Computers & Security*, 99(102039). doi:<https://doi.org/10.1016/j.cose.2020.102030>
- Al-Alwi, A., & Al-Bassam, S. (2019). *Assessing the Factors of Cybersecurity Awareness in the Banking Sector*. *Arab Gulf Journal of Scientific Research*, 37(4), 17–32. doi:doi.org/10.51758/AGJSR0420190014
- Al-Baalbaki, M. (2008). *Al-Mawrid: English–Arabic Dictionary*. Beirut: Dar Al-Ilm Lilmalayin.
- Al-Baghdawi, M. (2021). *The Economics of Cybersecurity in the Banking Sector*. *Journal of Legal and Economic Research*, (76).
- Al-Deeb, M. (2005). *Legal Protection of Intellectual Property in the Field of Computers and the Internet*. New University House for Publishing.
- Algeria Telecom. (2025). Retrieved from <http://algeriatelecom.dz/ar/entreprises/packs-cybersecurity-prod142>
- APS. (2024). *Launch of Mobile Payment Interoperability*. Retrieved from <https://www.aps.dz>
- Arora, A., & Rahman, Z. (2022). *Cross-Border Regulatory Coordination for Cybersecurity: A Financial Sector Perspective*. *Computers & Security*, 114(102621). doi:10.1016/j.cose.2021.102621
- Bada, M., Sasse, M., & Nurse, J. (2021). *Cybersecurity Regulation and Its Impact on Organizations: A Review*. *Computers & Security*, 105(102242). doi:10.1016/j.cose.2021.102242
- Ben Omar, K., & Bourzama, J. (2019). *The Reality of Electronic Banking in Algeria Between Expansion Constraints and Success Requirements*. *Arab Economic Research Journal*, 80.
- Bouria, S. (2023). *Algerian Public Policies in the Field of Cybersecurity*. *Journal of Politics and Law Notebooks*, 15(1).
- Bouzian, Y. (2018, April 17). *24,000 Cybersecurity Specialists to Confront Electronic Crimes*. *Al-Ain News*, Abu Dhabi. Retrieved on 08 October 2025, from <https://al-ain.com/article/algeria-cyber-security>
- EcoTimesDz. (2024). *Towards the Generalization of Mobile Payment in Algeria*. Retrieved from <https://ecotimesdz.com>
- Grispos, G. (2021). *Cybersecurity: Practice*. *Encyclopedia of Security and Emergency Management*, 212–217. doi:10.1007/978-3-319-70488-3_81
- Ismail, M. (2019). *Cybersecurity in the Banking Sector*. *Arab Monetary Fund Policy Brief*, 4.
- ITU. (2024). *Global Cybersecurity Index 2024*. ITU Publications.
- Jennifer Elliott & Nigel Jenkinson. (December 7, 2020). *Cyber Risks: The New Threat to Financial Stability*. Retrieved October 9, 2025, from *International Monetary Fund*: <http://www.imf.org>
- Kadri, N. (2023). *Cybercrime and Mechanisms for Its Combat: Facing Cybersecurity Challenges*. *Algerian Journal of Law and Political Science*, 08(01).
- Kaouah, A. (2020). *Cybersecurity Policies to Enhance Digital Transformation in Egyptian Universities: A Proposed Vision in Light of Global Experiences*. *Journal of Educational and Social Studies*, 26.
- Khalaf, F. (2015). *Legal Mechanisms for Combating Cybercrime*. *Journal of Rights and Freedoms*, 03(02).
- Law No. 04-09. (August 5, 2009). *Specific Rules for the Prevention and Combat of Crimes Related to Information and Communication Technology*. *Official Gazette No. 47*.
- Law No. 04-15. (2004). *Law No. 04-15 Amending and Supplementing Ordinance 66-155 of 27 Ramadan 1425 (November 10, 2004) Concerning the Amendment of the Penal Code*. *Official Gazette No. 71*, Issued on 27 Ramadan 1425 (November 10, 2004).
- Law No. 07-18. (June 10, 2018). *Official Gazette No. 34*.
- Mahmoudi, S. (2023). *Cybersecurity in Algeria: Between Security Management and Legal Protection*. *Al-Naqid Journal for Political Studies*, 07(02).
- Mohamed, A. (2019). *Eco*. Illizi: Illizi.

- Saliha Mabrouk & Saber Cherad. (December, 2019). *Information Technology*. *Al-Manhal Journal of Economics*, Vol. 02, Issue 02.
- Securenetworkdz.com. (2016). Retrieved from <https://securenetworkdz.com/>
- Zhou, Z., Liu, W., & Zhang, Y. (2021). *Regulatory Harmonization and Cybersecurity Risk Management in Financial Institutions*. *Journal of Financial Regulation and Compliance*, 29(2), 135–151. [doi:10.1108/JFRC-11-2020-0083](https://doi.org/10.1108/JFRC-11-2020-0083)
- Zuheir Abdul Karim Jaafar Qabas & Kazem Turki Ai Saniya. (2016). *The Impact of Information Technology*. *Baghdad College Journal of Economic Sciences*, (49), 393.

To cite this article according to (APA):

Souaad El miloudi, Fatima Fouka. (2026). Requirements for Enhancing Cybersecurity in Algerian Banks to Support Modern Payment Systems. *Journal of New Economy*, Vol 17 / Issue 01-2026.