European Economic Letters
ISSN 2323-5233
Vol 14, Issue 04 (2024)
http://eelet.org.uk

Cybersecurity Strategy in Light of Digital Transformation for Algerian Institutions

Oualid Mortadha Naoua [1]

[1] University of El Oued , (ALGERIA), Email: naoua-oualidmortadha@univ-eloued.dz

Received: 03/07/2024 Accepted: 14/10/2024 Published: 28/11/2024

Abstract:

This study aimed to assess the extent of the application of the cybersecurity strategy in light of the digital transformation of Algerian institutions, in response to the risks and threats witnessed globally, as well as those threatening sensitive information and information systems of all countries. Therefore, Algeria seeks to develop its security infrastructure, improve government policies, and increase awareness among individuals and institutions regarding the risks and threats of cybersecurity. The study concluded with several findings, the most important of which is that Algeria is making progress in the field of cybersecurity; however, it still requires more efforts to catch up with the more advanced countries.

Keywords: Algerian Institutions, Cyberattacks, Cybersecurity, Digital Transformation.

Introduction:

In light of the rapid pace of technological development and the digital transformation of institutions and governments, which has become an urgent necessity, institutions are striving to develop the digital systems on which they rely in their operations. However, the security challenges that now threaten both institutions and individuals have led to widespread attention from governments and institutions to protect data and ensure individuals' privacy, especially with the rise of increasingly complex and aggressive cyberattacks. Therefore, it is essential to adopt cybersecurity strategies to contribute to creating a secure digital environment and protecting vital information.

Based on this, we raise the following main question:

To what extent is the cybersecurity strategy effective in light of the digital transformation of Algerian institutions?

To answer this main question, we present the following sub-questions:

1. What are the components of cybersecurity, and what are the most important cyber threats to institutions?
2. What are the requirements for achieving digital transformation, and what is their impact on institutions?
3. What is the current state of cybersecurity in Algerian institutions?

Study Hypotheses:

In order to answer the questions, the following hypotheses were formulated:

Main Hypothesis: There is a cybersecurity strategy in Algerian institutions, but it needs further development to increase its effectiveness.

The following sub-hypotheses are derived from the main hypothesis:

- The components of cybersecurity focus on protecting electronic data, devices, and networks from various cyber threats and attacks.
- Digital transformation requires an advanced technological infrastructure, which leads to a change in the work patterns within institutions.
- Algerian institutions adopt a unified cybersecurity guide that they implement to maintain their security and confidentiality of their information.

Importance of the Study :

- Protecting sensitive information of institutions and individuals from cyberattacks.
- Ensuring the continuity of Algerian institutions' operations in a stable condition and maintaining their sustainability.
- The issue of cybersecurity has become a concern for all institutions striving for digital transformation.

Study Objectives :

- Enhance trust in the digital services provided by Algerian institutions.
- Protect personal data, as its leakage poses a threat to individuals' privacy.
- Develop legal and regulatory standards within Algerian institutions to assist in adapting to international cybersecurity standards.

Methodology:

To answer the research problem, the descriptive methodology was used to describe the phenomenon related to the topic. The analytical methodology was also employed to analyze and interpret the phenomenon and address the research problem.

2. Cybersecurity

2.1. Definition of Cyberspace:

Cyberspace is a virtual space created through the interconnection of all computers, smartphones, tablets, and Internet-connected devices, along with the information and software within them worldwide. (Bougrass, 2022, p. 63) Cyberspace has also been defined as a virtual world that intersects with our physical world, affecting and being affected by it in a complex manner. The relationship between the two worlds is based on a holistic view that contains both advantages and risks that do not cease. Some describe it as the fourth arm of modern armies, alongside the land, sea, and air forces, especially as the internet witnesses’ real battles in this virtual world. Others view it as representing the fifth dimension of war. It is also defined as a physical and non-physical space consisting of elements such as computers, networks, software, information processing, content, transport data, control systems, and users of all these elements. These elements are the common factor in all aspects of cyberspace use, whether the users are capable of maximizing their values and capabilities, including improving the efficiency of the human element, or whether they are in a late stage. (Klaa, 2022, p. 297)

2.2. Concept of Cybersecurity:

Cybersecurity is defined as the protection of networks, information systems, data, and internet-connected devices. It involves the measures, standards, and protocols required to address threats, prevent intrusions, or minimize their impacts in the worst-case scenarios. This security is closely linked to information security, as accessing, broadcasting, viewing, trading, altering, or exploiting information is often behind cyberattacks on networks and the internet. (Qataf, 2022, p. 41)

Thus, cybersecurity is a combination of practices and technologies aimed at protecting programs, applications, networks, computers, and data from attacks. It includes the physical security of programs, applications, networks, and computers, as well as the non-physical or intangible security related to protecting data and information from any attacks, intentional harm, theft of information, and controlling access to devices, applications, and networks to protect them from potential damage that could occur over networks. (Klaa, 2022, p. 298)

Therefore, cybersecurity in its general concept is a strategy adopted by countries or specialized bodies to protect systems and programs from digital attacks, which usually aim to access, alter, destroy, or extort sensitive information from institutions and countries in exchange for money. Successful cybersecurity follows a certain approach, usually consisting of high-flow strategies, systems protection linked to computers, software, or data, and counter and backup data in case of any breach that certain parties may attempt to access through data breaches or password violations. (Klaa Al-Doros, 2022, p. 252)

2..3. Cybersecurity Objectives:

Cybersecurity aims to: (Husseini, 2023, p. 61)

- Provide a secure and reliable environment for transactions in the information society.
- Ensure the resilience of critical infrastructure against cyberattacks.
- Strengthen the protection of operational technology systems at all levels, including their components (hardware, software), services provided, and the data they contain.
- Counter information security attacks and incidents targeting government devices and institutions in both the public and private sectors.
- Provide necessary requirements to mitigate the risks and cybercrimes targeting users.
- Eliminate vulnerabilities in computer systems and mobile devices of all types.
- Address security gaps in information security systems and combat malware that may cause significant damage to users.
- Limit espionage and cyber sabotage at the governmental and individual levels.
- Take all necessary measures to protect citizens and consumers from potential risks in various internet usage areas.
- Train individuals on new mechanisms and procedures to face challenges related to breaches of their devices that may harm their personal information, either by destruction or theft.

2.4. Stages of the Evolution of Cybercrime:

Cybercrime has passed through three main stages as follows: (Khenish, 2023, p. 25)

- **First Stage:** This began with the early use of computers and their connection to networks, leading to debates on whether these crimes were just a passing phenomenon or a new criminal trend. Initially, these acts were framed as unethical behaviors, without legal context.
- **Second Stage:** In the early 1980s, the concept of computer and internet crimes became clearer due to the rise in illegal remote access to computers and the spread of viruses that destroy data, files, and programs. The term "hackers" also became common, referring to intruders of information systems.
- **Third Stage:** Starting in the early 1990s, there was a massive increase in cybercrime due to the growing use of the internet. This led to new and more dangerous forms of cybercrime. Initially, there was little focus on security; the main concern was expanding the network and its activities

without considering security challenges. This gap encouraged the growth of cybercrimes and caused severe damage, prompting the need for stringent security standards and the identification of vulnerabilities that made computers targets for crime.

2.5. Dimensions of Cybersecurity:

Economic Dimension: The cyber space has become attractive to all sectors of society, with knowledge becoming a key driver of production and economic growth. It is now recognized that focusing on information and technology is essential for economic progress, which has led countries to increase investment in knowledge. The modernization of the economy is now closely linked to controlling the digital economy by various economic and social actors. The use of computers and the internet in developing industries, driving the economy, and managing economic and financial transactions has emphasized the need for cybersecurity to protect this information. (Bara, 2017, p. 261)

Social Dimension: Raising awareness among all participants in global information networks about the importance of correctly understanding security and the basic steps to enhance security is essential. If these steps are clearly formulated, identified, and wisely implemented, they can have a major impact. A responsible information society requires media campaigns and civic education that address the challenges, risks, and preventive security measures. There is also a need for security awareness and personal responsibility, as well as understanding the legal consequences of not complying with security obligations. Additionally, it is necessary to provide education and training in information and communication technology, not only in security measures but also in deterrence. A security culture should be embedded within information technology culture, and ethical security standards must be established and respected by all who work in cyberspace. (Qataf, 2022, p. 47)

Legal Dimension: Technological developments require legal frameworks to keep up with them, through the establishment of regulations for legal and illegal activities in cyberspace. It is noticeable that cybercrime lacks legal frameworks in many countries, and there is a need for effective international cooperation to confront it. Legal risks stem from the absence of legal security or contradictory laws and legal systems, leading to increased risks. There is also a lack of effective prosecution mechanisms that align with the nature of cross-border cybercrimes, which can affect any citizen anywhere on Earth, threatening the security and stability of nations. The risks to individuals and countries are vast and unrestrained by current legal frameworks that are insufficient for the cyber age. (Rahim, 2024, p. 50)

Political Dimension: The political aspects of cybersecurity are based on protecting a state's political system and sovereignty. Technologies can be used to disseminate information and data that could destabilize the security of states and governments. These can spread rapidly to large segments of the population, regardless of the accuracy of the information being shared. (Husseini, 2023, p. 64)

Military Dimension: The internet was initially created in the military environment and later moved to the scientific community for military research and development. For example, in cases like Georgia, Estonia, South Korea, and Iran, cyberattacks and intrusions have occurred, whether due to armed conflict or to disrupt internet connections between a state and its citizens, disable government circles, or breach nuclear facility systems in Iran. The strength of cyber power lies in its ability to move through cyberspace, where military networks are interconnected to facilitate information exchange and decision-making for achieving military goals. If protected or armed with this technology, the military can prevent external intrusions, but failure to do so may lead to retaliatory cyberattacks that harm their databases. (Qataf, 2022, pp. 45-46)

2.6. Cybersecurity Threats:

The forms of threats facing cyberspace are varied, including, for example, the following: (Bougors, 2022, p. 66)

- Data interception
- Data destruction and sabotage
- Digital identity theft
- Disruption of interests and services
- Espionage
- Extortion
- Fraud and phishing
- Negative influence on public opinion

3.Digital Transformation

3.1. Concept of Digital Transformation:

Digital transformation is defined as the process by which companies transition to business models that rely on digital technologies to support the development and innovation of products and services, and to provide new channels of excitement and job opportunities that increase the value of their products, whether goods or services. (Sharif, 2022, p.407)

It is also defined as the process of transitioning organizations from the traditional business model to one that relies on digital technologies for product and service innovation, as well as methods of management and marketing, while providing new revenue channels by building a digital strategy. This can only happen through evaluating digital capabilities, studying the requirements of digital investment in the context of digital marketing activities, and having a willingness to change from management toward digital transformation. (Chawshi, 2022, p. 19)

3.2. Requirements for Digital Transformation:

Digital transformation is applied through a set of elements that include technologies, data, human resources, and processes, as detailed below: (Hassan & Al-Ghabiri, 2020, p. 17-18)

1. Clearly defining the vision, which means explaining what the organization wants to become in the future.
2. Continuous review of the digital transformation plan.
3. Maintaining ongoing leadership and management support for transformation efforts, by focusing leaders and all officials on administrative practices related to technology, and providing necessary human, financial, material, and legislative resources.
4. Developing existing organizational structures by avoiding complex structures, seeking flexible organizational structures, and focusing on effective teams.
5. Building a digital transformation strategy based on market analysis and its needs, analyzing strengths and weaknesses, and surveying opportunities and threats in the external environment.
6. Focusing on the technological dimension: by renewing the basic IT infrastructure in terms of providing modern devices and diverse software.

7. Developing human resources by considering recruitment processes and developing the skills and capabilities of all youth through training and self-development programs.
8. Changing the prevailing organizational culture by promoting the culture of using technology and the internet, which requires changing and managing culture as a competitive advantage.

3.3. Effects of Digital Transformation:

Digital transformation impacts an organization through three main levels, which can be illustrated in the following table:

Table (1.1) Effects of Digital Transformation

Customer Relationship (Customer Experience)	Operational Processing	Business Model
Understanding the customer: Analytical retail, social network information	**Digitization of operations:** Performance improvement, new features	**Business transformation through digitization:** Increased product/service, transition from physical to digital, digital packages
Sales growth: Improved sales through digitalization, predictive marketing, rationalized operations	**Independence of collaborators:** Work from anywhere, anytime; broader and faster connectivity, knowledge sharing within the community	**New digital work:** Digital products, redefinition of organizational boundaries
Customer touchpoints: Customer service, consistency across communication channels, self-service	**Performance management:** Operational transparency, data-driven decision making	

3.4. Obstacles to Digital Transformation

The process of digital transformation faces a range of challenges, the most important of which are: (Abd Al-Jabbar & Abd Al-Khalek, 2022, p. 65)

Rejection of a culture of change: Digital innovation can only succeed through fostering a culture of collaboration. Employees must be able to work and collaborate together. However, the current reality shows that most institutions are stuck in a culture that rejects change.

Limited participation and collaboration: The reluctance to participate and collaborate not only presents a challenge within the organization’s work system but also within the institution itself. Issues like control over processes, information, and systems make employees hesitant to share their knowledge and expertise.

Unpreparedness of institutions: Many leaders were drawn to the buzz surrounding digital business, but when technology managers and heads of data and digital operations attempt to initiate digital transformation, it becomes clear that institutions still lack the required skills and resources to undertake the process.

Talent gap: Most institutions follow a traditional work approach by organizing work into separate tasks such as information technology. In such work environments, change can be slow. Organizations must adopt a different approach that blends employees, operations, and technology together to create new services.

Current practices within the institution do not support talent: While having talented staff is important, the right practices must allow them to work more effectively. Additionally, traditional processes are highly structured and slow to form, which means they cannot support digital transformation efforts.

Difficulty of innovation: Change is not easy. Digital business applications are often difficult and expensive from a technical standpoint. Developing platforms, changing the organizational structure, and creating a work system with the private sector require significant time, resources, and funding.

4. Cybersecurity Strategies in Algeria

The Algerian state gives top priority to cybersecurity within the country's overall security strategy by implementing the necessary measures to provide the highest level of protection for its information infrastructure. This ensures appropriate cybersecurity for the ongoing digital transformation and the modernization of state sectors, which poses significant challenges in achieving the necessary security for various government agencies and citizens. These efforts are made possible by the mechanisms and strategies adopted by the state, which have been acknowledged by many stakeholders and officials, particularly cybersecurity managers. (Ben Boughouth, 2023, p. 452)

4.1. Challenges Facing Algeria in Implementing Cybersecurity

Among the challenges facing Algeria in the field of cybersecurity are: (Ben Boughouth, 2023, p. 453)

- **Increase in internet users and social media subscribers in Algeria:** With over 10 million subscribers, this surge amplifies the risks, making it difficult to trace the perpetrators of cybercrimes.
- **Spread of high-speed internet technologies (ADSL/VSAT/SDSL):** This presents a challenge for the rapid tracking of criminals, requiring appropriate devices and software.
- **Wireless internet (WIFI/3G/4G/5G):** This also creates a barrier to fighting cybercrime.
- **Concealment during internet usage (Proxy):** This is classified as one of the major challenges and obstacles facing cybercrime fighting agencies.
- **Lack of coordination between countries and governments:** Due to the nature of cybercrime, it allows perpetrators to easily access information systems and keeps information, as well as the programs used to protect and share it, secret.
- **Difficulty in adapting and enforcing laws against cybercrime:** This is due to the rapid technological advancements, the ever-evolving virtual identities, software, and techniques, as well as the professionalism in concealment and the viruses capable of hiding.
- **Other factors common to many developing countries, including Algeria:** These include Algeria's relatively young experience in communication and information technology.
- **Dominance of developed countries in technology:** The monopolization of modern technologies by developed nations hinders the ability to predict the threats faced by Algeria.

4.2. Combating Cybercrime in Algeria

Cybercrime is characterized by the ability of its perpetrators to hide and evade punishment, which necessitates the adoption of technical methods for combating it, such as using filtering and blocking techniques to control the flow of information from unwanted sources outside the protected environment. Another approach is encryption, which ensures that information cannot be understood without knowing the code. This is one of the most effective means of maintaining the confidentiality and integrity of electronically exchanged information, serving as an optimal solution to prevent information hackers. There are many protective measures such as backing up data, acquiring antivirus software, firewall programs, and using physiological characteristics like fingerprints, retina scans, and voice recognition. (Kheniche, 2023, p. 190).

In accordance with the amendments to the Penal Code of 2004, Algeria criminalized cybercrimes that began to spread in Algerian society with the rise of digital technology. A special section was introduced in the Penal Code to address crimes affecting automated data processing systems. With the beginning of the electronic transformation of all institutions, agencies, and public administrations, the Algerian legislator issued the first legal text in 2009 related to cybercrimes and their prevention. This law provided a definition of cybercrimes, referring to crimes related to information and communication technologies, particularly those affecting automated data processing systems. It also includes crimes committed or facilitated through an information system or electronic communication network (Kheniche, 2023, p. 182).

Therefore, it is crucial to focus on the regional and international threats surrounding Algeria. This can be achieved by relying on a set of necessary strategies to strengthen Algeria's cybersecurity system, which include the following: (Qala'a Al-Durus, 2022, pp. 261-262).

- **Mandatory activation of firewalls** using electronic fingerprints, digital signatures, and strengthening password systems. These techniques enhance protection against breaches and prevent email forgery. This includes creating high-precision security policies for institutions and devices that monitor potential terrorist or criminal sites, particularly in economic institutions, banks, the stock market, official ministries, the presidency, and other governmental bodies that hold sensitive data like the Supreme Audit Council, the National Economic, Social, and Environmental Council, and Parliament.
- **Implementing antivirus protection programs:** The state can support this process by reducing the cost of these programs. For example, antivirus applications like Kaspersky are often not affordable for everyone in Algeria.
- **Enforcing legal procedures against hackers** and system breaches, establishing a legal framework that protects citizens, companies, and the state. This task falls under the jurisdiction of the central unit for combating cybercrime within the national police and the cybercrime prevention center of the gendarmerie. Internationally, the state must sign agreements to protect its digital and virtual systems, establishing international policies that impose severe penalties on internet criminals. Government and international intervention is required due to the significant risks faced by states and institutions.
- **Creating a digital generation** that is well-trained in electronic and cybersecurity education. This is essential for future generations, considering the growing importance of technology in their lives. The aim is to raise awareness about internet use and advise on the dangers of cybercrimes, including their security, political, economic, and social implications. Additionally, it is important to strengthen effective training programs for

researchers at universities, encouraging research centers, scientific teams, training centers, and security agencies in Algeria.

4.3. National Cybersecurity Reference

The National Cybersecurity Reference is a document issued by Algeria's Ministry of Post and Telecommunications. Its goal is to establish a unified framework for information security governance within Algerian institutions and agencies, defining the minimum-security requirements for managing and mitigating the impact of potential threats to information systems.

Through this reference, a set of recommendations was provided, along with a comprehensive information security policy that covers all aspects. The document stresses the regular alignment of security policies to ensure compliance with legislative and technological developments. It also outlines how to handle security incidents, isolate affected systems, report incidents, and prepare analytical reports. Additionally, it emphasizes improving security procedures after an incident to minimize its impact. The National Reference also calls for organizing periodic training programs for employees to foster a cybersecurity culture within institutions, reducing human errors, and preventing potential threats before they occur. It further emphasizes the importance of proactive planning to reduce the impact of risks. (Ministry of Post and Telecommunication, 2020, pp.12-24).

4.4.Global Ranking of Algeria in Cybersecurity

According to the International Telecommunication Union's 2024 report, Algeria's performance in the five aspects of cybersecurity indicators: legal, technical, organizational, capacity building, and international cooperation, was classified in the third stage, along with Tunisia and Nigeria, known as the "Establishment Phase." This means that Algeria has made significant progress but needs to further develop its national strategies to improve its ranking. Algeria has national strategies and initiatives, but they have not yet achieved optimal execution or tight integration between sectors. (International Telecommunication Union, 2024, pp. 24-26)

The report shows performance in the five areas as follows:(International Telecommunication Union, 2024, pp. 06-23)

- **Legal procedures:** Algeria has made progress in adopting cybersecurity-related legislation. However, the report recommends that the legislation be clarified to ensure effective implementation, such as those related to personal data protection and breach reporting.
- **Technical procedures:** There is a team or center for responding to cybersecurity incidents, but there is a need to strengthen cooperation between technical sectors and improve readiness to respond to cyberattacks.
- **Organizational procedures:** Algeria has a national cybersecurity strategy, but it needs to develop a clear and effective action plan to implement the strategy and improve coordination mechanisms between sectors.
- **Capacity building:** Algeria has awareness-raising activities on cybersecurity, but training and integration into educational curricula remain limited. There is a need to enhance capacity-building programs for youth and professionals in cybersecurity.
- **Cooperation:** Algeria needs to join additional international agreements to enhance cybersecurity cooperation and improve partnerships with the private sector to develop infrastructure.

Conclusion:

In light of the rapid transformations in the digital environment of institutions, data, information, and electronic equipment now require continuous protection. Cybersecurity is the primary means of defense against risks and threats, ensuring the confidentiality and security of information and protecting privacy. Institutions must adopt effective strategies and use modern tools and technologies to address these challenges while keeping up with the rapid technological changes.

Results :

- Algeria has developed its cybersecurity infrastructure by establishing national bodies to confront the threats and risks to its information systems.
- Algeria has made notable progress in adopting legal frameworks and legislation, such as the Anti-Cybercrime Law and other laws protecting the personal data of individuals and institutions, although further development is needed.
- Algeria collaborates internationally on cybersecurity issues, sharing efforts with the African Union and the Arab League in this field.
- Algeria is working on training national capabilities, both scientific and professional, to enhance the skills of technicians and cybersecurity specialists.
- New institutes and specializations have been opened in Algerian universities to teach cybersecurity.
- There is a set of guidelines or a manual for Algerian institutions, prepared by the Ministry of Post and Telecommunications, to adopt a cybersecurity strategy.

Recommendations :

- There is a need for more legislation and laws, as well as their increased activation, to ensure alignment with global standards.
- International cooperation in cybersecurity should be expanded with more advanced countries to benefit from their expertise.
- Institutions should expand the scope of training to include more sectors and individuals, as cybersecurity concerns everyone who works or interacts in a digital environment.
- Institutions must equip themselves with the latest software and hardware to ensure broader protection for their information systems and maintain privacy.
- Educational institutions at all levels and disciplines should teach cybersecurity and encourage scientific research and innovations related to it through competitions and awards.

References:

1. Ahmed, F. H. (2023). Cybersecurity awareness: A luxury or a necessity in the age of informatics. *Research and Education Journal*, 13(02), National Institute for Educational Research, Algeria, pp. 54-74.
2. Algerian Ministry of Post and Telecommunications. (2020). National Information Security Framework (L06-Final Version). https://www.mpt.gov.dz/wp-content/uploads/2023/12/Referentiel-National-de-la-Securite-de-lInformation-2020-VERSION-FINALE-1-1.pdf
3. Bara, S. (2017). Cybersecurity in Algeria: Policies and Institutions. *Algerian Journal of Human Security*, 02(02), Batna 1 University, Algeria, pp. 255-280.

4.Ben Berghouth, L. (2023). Cybersecurity and Digital Data Privacy Protection in Algeria in the Era of Digital Transformation and Artificial Intelligence: Technical Threats, Challenges, and Countermeasures. *Contemporary Economic Research Journal*, 10(01), Mostaganem University, Algeria, pp. 443-457.

5.Bougueras, S. (2022). Cybersecurity: Risks, Threats, and Challenges that Require Specific Practices, Recommendations, and Strategies. *Journal of Research in Social Protection*, 30(10), High School of Social Security, Algeria, pp. 61-77.

6.Kallaa, S. (2022). Cybersecurity and the Challenges of Espionage and Electronic Breaches of States through Cyberspace. *Journal of Law and Humanities Sciences*, 15(01), University of Algiers, Algeria, pp. 292-314.

7.Khnech, D. (2023). Cybercrime and Social Security. *University Publications House*, Algeria.

8.Khalaf, Z., & Shaoushi, K. (2022). Digital Transformation in Algeria. *Journal of Accounting, Auditing, and Finance*, 5(01), Khmies Miliana University, Algeria, pp. 15-30.

9.Rahim, M. (2024). Cybersecurity as a Necessity for the Success of the E-Government Project: The Case of Algeria. Ph.D. Thesis in Management Sciences, University of Algiers 3, Algeria.

10.Sleimani, K., & Bouguerin, A. H. (2022). Cybersecurity and the Conceptual Implications Associated with It. *Tebna Journal for Scientific and Academic Studies*, 05(02), Briqa University Center, Algeria, pp. 37-56.

11.Slemani, S. (2022). National Cybersecurity: An Analysis of the Key Security and Technical Strategies to Counter Cybercrime in Algeria. *Al-Rawaq Journal for Social and Human Studies*, 08(02), University of Relizane, Algeria, pp. 249-267.

12.Telecommunication International Union. (2024). *Global Cybersecurity Index 2024 (5th ed.)*. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

13.Tawfiq, H., & Khaloufi, W. (2022). The Trend Toward Digital Transformation: Necessity or Choice? *Journal of Economics, Finance, and Business*, 6(01), Mila University Center, Algeria, pp. 276-291.