

Cyber security in Algeria: A Strategic Approach to Address Regional Challenges and Strengthen National Sovereignty

الأمن السيبراني في الجزائر: مقاربة استراتيجية لمواجهة التحديات الإقليمية وتعزيز السيادة الوطنية

Dr. Azzeddine DRAOU¹

¹ Oran 2 University- Oran (Algeria), draou.azzeddine@univ-oran2.dz

Received: 06/04/2025

Accepted: 29/06/2025

Published: 30/06/2025

Abstract:

This study aims to define the cyber security policy and its importance in protecting countries from various regional threats. It also seeks to study the potential effects of cyber-attacks and the devastating consequences that they may cause for the entities and economies of countries. On the other hand, the study concluded the need to present a strategy of cyber deterrence as a mechanism to enhance and protect national security, because it can provide protection for databases and information on the one hand, as well as to ensure the continuity of international cooperation for Algeria on the other hand.

Keywords: Cyber security; cyber deterrence; cyber-attacks; Algerian national security

JEL Classification Codes: O33, F51, D73, H56

ملخص:

تهدف هذه الدراسة إلى التعريف بسياسة الأمن السيبراني ومدى أهميتها في حماية الدول من مختلف التهديدات الإقليمية. كما تسعى أيضا لدراسة الآثار المحتملة للهجمات السيبرانية وما يمكن أن تتسبب فيه من نتائج مدمرة لكيانات واقتصاديات الدول. في المقابل، توصلت الدراسة إلى ضرورة تقديم استراتيجية الردع السيبراني كآلية لتعزيز وحماية الأمن الوطني، لما يمكن أن توفره من حماية لقواعد البيانات والمعلومات من جهة، وكذا ضمان استمرارية التعاون الدولي للجزائر من جهة أخرى.

كلمات مفتاحية: الأمن السيبراني، الردع السيبراني، الهجمات السيبراني، الأمن الوطني الجزائري

تصنيفات JEL : O33, F51, D73, H56

Introduction

In today's increasingly digitized world, cyber security has become a cornerstone of national security, economic stability, and societal resilience. Nations across the globe are facing an unprecedented wave of cyber threats, ranging from state-sponsored attacks and cyber espionage to ransom ware, data breaches, and digital terrorism. As Algeria advances its digital transformation efforts, it finds itself at the crossroads of significant opportunities and growing vulnerabilities. The country's increasing reliance on digital infrastructures in sectors such as finance, energy, telecommunications, and government services has necessitated the development of robust cyber security frameworks to mitigate potential risks.

The strategic importance of cyber security in Algeria is further amplified by its geographical and geopolitical positioning. As the largest country in Africa, Algeria plays a crucial role in regional security dynamics, particularly in the Maghreb and the broader Sahel region. The nation shares borders with several countries experiencing varying degrees of political instability and cyber security vulnerabilities, making it a potential target for cyber threats emanating from hostile actors, terrorist organizations, and transnational cybercriminal networks. Strengthening cyber security is, therefore, not just a technical necessity but a strategic imperative to safeguard national sovereignty and protect critical infrastructure.

Algeria has taken several initiatives to reinforce its cyber security posture. The establishment of the National Cyber security Strategy and the introduction of legal frameworks to regulate digital security reflect the country's commitment to addressing cyber risks. However, challenges remain, including the need for enhanced cyber awareness, improved coordination between public and private sectors, and greater investments in local cyber security expertise. Furthermore, as cyber threats evolve in sophistication, Algeria must adopt a forward-looking approach, leveraging artificial intelligence, block chain, and other emerging technologies to stay ahead of potential attacks.

This study explores Algeria's cyber security landscape, examining both the threats and the strategic responses adopted by the government and key stakeholders. It also highlights regional challenges that influence Algeria's cyber security policies and assesses the extent to which these measures contribute to strengthening national sovereignty. By adopting a proactive and integrated cyber security strategy, Algeria can not only protect its digital frontiers but also position itself as a regional leader in cyber security governance.

Cyber security in Algeria: A Strategic Approach to Address Regional Challenges and Strengthen National Sovereignty

Study Problem:

The study focuses on the question: "How important are cyber deterrence mechanisms in ensuring protection against regional and international threats, and what role do national security agencies, particularly the National People's Army, play in achieving this?"

Sub-questions:

- ✓ What do we mean by Cyber security?
- ✓ What is the nature of cyber attacks?
- ✓ What are the most significant current cyber attacks and threats?

Hypotheses:

Cyber attacks constitute a regional threat to Algeria's national security.

Adhering to a national strategy for cyber deterrence and protection is essential for ensuring Algeria's information security.

Importance of the Study:

- ✓ This study is distinguished by its focus on a new type of cyber attacks.
- ✓ It relies on the analysis of major cyber risks and their implications for international security and peace.

Objectives:

- ✓ To provide a clear and concise definition of cyber security and cyber attacks.
- ✓ To identify solutions for addressing cyber attacks.
- ✓ To examine countries' experiences in countering cyber piracy and offering necessary solutions.

Methodology:

This study employs a descriptive-analytical approach to collect data and diagnose the problem scientifically, aiming to yield significant insights into managing cyber attacks.

1. Cyber Threats and Their Implications:

Cyber threats encompass a broad spectrum of attacks aimed at compromising the integrity, confidentiality, and availability of digital systems. These threats range from unauthorized access to sophisticated state-sponsored attacks. In the context of Algeria, understanding these threats is crucial for developing effective defense mechanisms.

1.1. Understanding Cyber security

1.1.1. Information Security:

Traditionally, security was synonymous with physical protection. However, with the digital revolution, security concepts have expanded to include the protection of online assets and data. Cyber security, a subset of this broader security framework, focuses on safeguarding information systems from cyber threats.

✓ *Definition of Security:*

Security, in a general sense, is the protection of wealth and property, encompassing national security, economic security, and computer security. It involves preventive measures to protect assets and responsive actions to mitigate damage from security breaches (Al-Sheikh, 2015, p. 2).

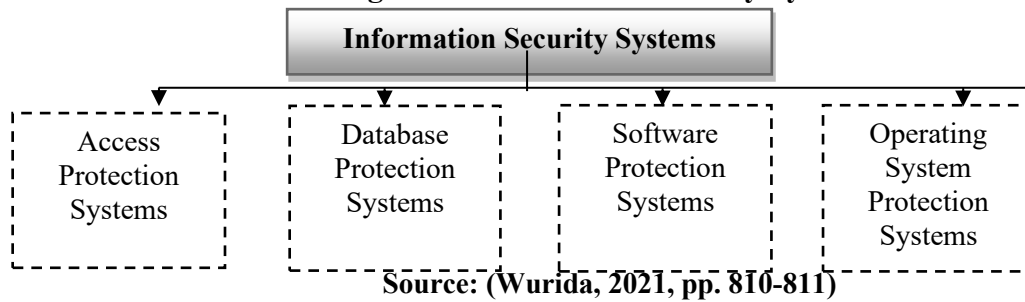
✓ *Concept of Information Security:*

The concept of information security varies depending on the nature of each economy and country. It can be defined as: "the science that aims to provide protection for information from the risks that threaten it, or the barrier that prevents attacks on it, by providing the necessary tools and means to protect information from internal and external risks" (Ouarda, 2021, p. 810). Indeed, security tasks always emphasize protection and prevention, and the same applies to information security. Subsidiary systems for protection and deterrence are prepared, which also constitute a set of security foundations for information systems.

✓ *Foundations of Information Security:*

Information security is based on several systems, including those related to operating systems and their protection, as well as systems for protecting software and various applications used. Additionally, there are systems for protecting and ensuring the secrecy of databases, and systems for protecting access through passwords and complex codes (see the figure below).

Figure 1: Information Security Systems



In this context, we note that information security is considered insufficient in light of the ongoing digital revolution. Therefore, the scope of protection and safeguarding must be expanded from internal networks to external and international networks. Consequently, a broader and more comprehensive concept than information security emerges, namely Cyber security.

1.2. Fundamentals of Cyber Attacks:

As a result of the evolution of cyberspace, it has become necessary to define the contours of cyber attacks by addressing information warfare, cyber terrorism, and cybercrime.

1.2.1. Information Warfare:

Recently, the concept of warfare within cyberspace, or what is termed information warfare, has spread, taking on various dimensions, whether defensive or offensive. These include: (Hamida Lahmar, 2021, p. 534)

- Attacks on personal information;
- Information warfare between companies;
- Attacks and information wars between states.

1.2.2. Cyber terrorism:

In addition to information warfare, which occurs at multiple levels, the concept of cyber terrorism has also emerged alongside the spread of cyber attacks. It is defined as illegal attacks and threats of attacks against computers, networks, and stored information to intimidate or coerce a government or its people to further political or social objectives. To be considered terrorism, it must result in violence against individuals or property, or at least cause harm that generates fear.

1.2.3. Cyber crime:

Within the framework of cyber attacks, it was necessary to define several concepts, including cybercrime, which allows legislators to adapt appropriate penalties for those responsible for such attacks. Cybercrime is defined as: "offenses committed against individuals or groups with criminal intent to harm the victim's reputation or cause direct or indirect physical or mental harm, using communication networks such as the internet" (Hamida Lahmar, 2021, p. 546).

1.2.4. Nature of Cyber Attacks:

The nature of cyber attacks varies depending on the purpose of the attack, including: (Farhat, 2019, p. 90).

- Attacks aimed at gathering intelligence information;
- Attacks seeking to demoralize;
- Offensive and defensive operations.

1.2.5. Risks Resulting from Cyber Attacks:

There are several negative and sometimes severe consequences in the event of cyber attacks, the most notable of which include: (Hamida Lahmar, 2021, p. 90)

- Potential breaches and destruction of communication and digital infrastructure;
- Identity theft and manipulation of personal data;
- The risk of terrorism and the outbreak of cyber wars.

Table 1: Top Ten Countries Committed to Cyber security Strategy

Country	Index Value	Legislation	Technology	Organization	Capacity Building	Cooperation
Singapore	0,92	0,95	0,96	0,88	0,97	0,87
United States	0,91	1	0,96	0,92	1	0,73
Malaysia	0,89	0,87	0,96	0,77	1	0,87
Oman	0,87	0,98	0,82	0,85	0,95	0,75
Estonia	0,84	0,99	0,82	0,85	0,94	0,64
Mauritius	0,82	0,85	0,96	0,74	0,91	0,70
Australia	0,82	0,94	0,96	0,86	0,94	0,44
Georgia	0,81	0,91	0,77	0,82	0,90	0,70
France	0,81	0,94	0,96	0,60	1	0,61
Canada	0,81	0,94	0,93	0,71	0,82	0,70

Source: Global Cyber security Index (GCI) 2024

2. Cyber Deterrence Strategy:

The Desert Storm operation launched by U.S. forces against Iraq in 1991 is considered the best example of cyber deterrence. Deterrence is not only a tool for defense but also for offense, where military communication networks were paralyzed. This situation highlights the importance of cyber deterrence and its role in contemporary warfare.

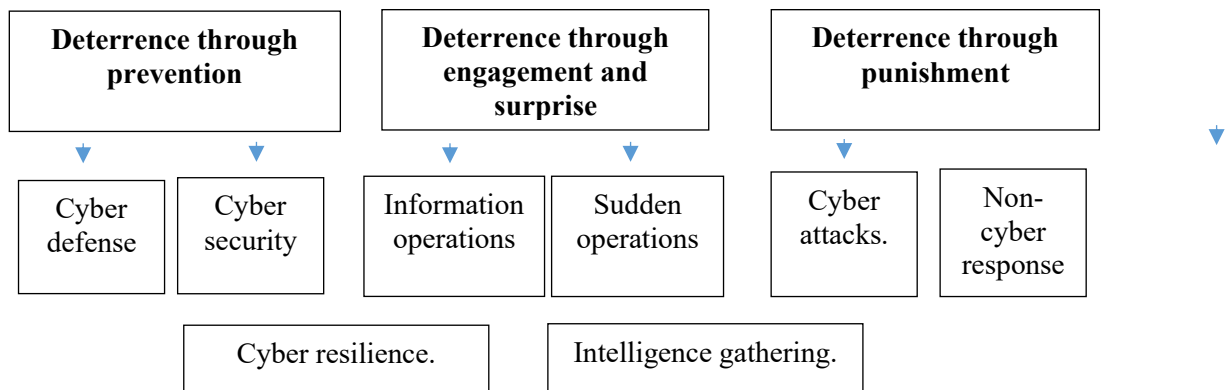
Similarly, a distinction must be made between the concept of a cyber attack and cyber warfare. The term "cyber attack" refers to the use of computer codes by adversaries to interfere with the functions of information systems and networks, including government and military services, to achieve strategic and political advantages by disrupting these networks and systems, such as taking them offline or completely destroying them. As for the term "cyber warfare," it refers to actions taken by a state to infiltrate the computers or networks of another country with the aim of causing damage or disruption (Qouadra, 2020, p. 522)

2.1. Military Operations in Cyberspace:

There are several complex and well-planned operations conducted in cyberspace, the most notable of which include: (Farhat, 2019, p. 100)

- Intelligence-gathering operations;
- Operations targeting morale;
- Offensive operations;
- Defensive operations.

Figure 2: Cyber Deterrence Strategies



Source: (Farhat, 2019, p. 274)

2.2. Stages of Implementing a Security Solution in the World of Information Security:

Ensuring robust protection for databases and information requires a set of policies and mechanisms, the most prominent of which include:

2.2.1. Security Policy:

This aims to define the required security objectives. A security policy is essentially a set of rules that determine what is permitted and what is prohibited.

2.2.2. Security Mechanisms:

These involve selecting tools that help achieve the objectives outlined within the framework of the security policy.

2.2.3. Identifying Vulnerabilities:

This stage involves pinpointing weaknesses in the system that could leave it exposed to attacks.

2.2.4. Maintenance Mechanisms:

These work to improve security solutions by addressing vulnerabilities and proposing new mechanisms.

3. Algerian National Security and International Efforts to Counter Cyber Threats:

3.1. Algeria's Natural, Economic, and Human Potential:

Algeria is a country with economic, ethnic, and environmental diversity. Its total area is estimated at 2,381,741 km², with a coastline stretching 1,200 km along the Mediterranean Sea. Additionally, it has a demographic growth rate of 2.2%.

On the other hand, most of Algeria's revenue comes from hydrocarbon exports, accounting for 95% to 98% of total exports. Hydrocarbons also make up more than 60% of fiscal revenues (Hjira, 2017, p. 75). This makes Algeria a rentier economy par excellence, which has also led to the presence of corrupt practices and various types of crime (Hjira, 2017, pp. 75-77)

3.2. Overview of the National People's Army:

Defense is a tool of protection, sovereignty, and strength. Responding to such challenges ensures strategic independence, a goal that consistently guides the National

Cyber security in Algeria: A Strategic Approach to Address Regional Challenges and Strengthen National Sovereignty

People's Army in accordance with its tasks and authorized responsibilities in the areas of: organization and general structure of forces, coherence of capacity-building choices, preparation, and utilization. In this regard, it is essential to oversee operational foresight activities. Accordingly, the National People's Army has an organic command represented by the command of the forces and an operational command formed by the commands of military regions. (Army, 2021, p. 1)

3.3. The Legal Aspect of Cyber security in Algeria:

The Algerian legislator has defined cybercrime and included it among the punishable acts under Article 2 of Law No. 09-04, dated May 9, 2009, which outlines specific rules for preventing and combating crimes related to information and communication technologies. The law also adopted the first and second criteria: the means of the crime and the subject of the crime. As for the third criterion: penalties, the legislator addressed it through Article 323 of Law No. 05-10, issued on June 20, 2005, which deals with electronic evidence. The legal framework is further supported by new technologies, such as the issuance of Law No. 03-16, dated June 19, 2016, which includes criminal fingerprints in criminal procedures to identify individuals. Additionally, the judicial authorities at the national level have been strengthened with four specialized courts (Algiers, Constantine, Oran, and Ouargla) to facilitate investigations by security agencies and adjudicate cases without referral to higher authorities. (Bouazidia, 2019, p. 1278)

On the other hand, domestic legislation has been aligned with international laws, particularly the International Convention signed in Budapest, Hungary, on November 23, 2001, which addresses cybercrime. This convention serves as the legal reference for all international legislation issued in this field.

3.4. The Operational Aspect of Cyber security in Algeria:

Algeria possesses several institutions and bodies responsible for ensuring information security, the most notable of which include:

- The Central Service for Combating Cybercrime;
- The Center for the Prevention of Computer and Cyber Crimes;
- The National Institute of Forensic Evidence and Criminology of the National Gendarmerie.

3.5. The Administrative Aspect of Cyber security in Algeria:

Under Presidential Decree No. 261-15, which came into effect on October 8, 2015, the tasks of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies were defined as follows: (Bouazidia, 2019, p. 1278)

- Using available information to monitor cyberspace and limit illegal activities;
- Coordinating between the public and private sectors, on one hand, and civil society, on the other, to promote a culture of combating illegal practices in cyberspace;
- Establishing a digital database for the central framework of informatics;
- Coordinating efforts among various security, financial, and administrative bodies specialized in network and information systems.

3.6. Developing a National Cyber security Strategy:

Developing a National Cyber security Strategy involves a comprehensive approach that addresses the security of national digital infrastructure, protects sensitive data, and prepares the country to respond to cyber threats. The strategy must be adaptable to the rapidly changing landscape of technology and cyber threats. Below is an outline of key components that should be considered when developing a National Cyber security Strategy:

- Establish a clear vision for Cyber security, focusing on protecting national interests while enabling innovation and digital transformation.
- Define strategic objectives, such as safeguarding critical infrastructure, ensuring public trust in digital systems, and fostering a secure and resilient digital economy.
- Develop a legal and regulatory framework for Cyber security that covers issues such as data privacy, cybercrime, incident reporting, and the responsibilities of government and private entities.
- Establish partnerships with universities, research institutions, and the private sector to create a pipeline of Cyber security professionals and experts.
- Facilitate collaboration between the public and private sectors in sharing Cyber security information, best practices, and responding to incidents.

Cyber security in Algeria: A Strategic Approach to Address Regional Challenges and Strengthen National Sovereignty

- Adopt and promote the use of advanced Cyber security technologies like artificial intelligence (AI), machine learning (ML), and blockchain for better detection and prevention of cyber threats.
- Establish a national incident response framework that includes processes for detecting, responding to, and recovering from cyber incidents.
- Work with other nations to combat cybercrime and develop norms for responsible state behavior in cyberspace.
- Set clear metrics and benchmarks to assess the country's Cyber security posture and progress toward achieving strategic goals.

4. Global Cyber security:

4.1. The Global Cyber security Index (GCI):

This index measures the level of commitment of countries and governments to Cyber security fundamentals. It also provides essential information for analyzing and comparing the performance of countries globally through the following dimensions:

- Legal Aspect: Determined based on the existence of institutions and legal frameworks that address Cyber security and cybercrime within the country;
- Technical Aspect: Measured by the presence of institutions and technical frameworks that handle Cyber security in the country;
- Organizational Aspect: Assessed through the existence of institutions and strategies that coordinate Cyber security development policies at the national level;
- Capacity Building: Determined by the presence of research, development, education, and training programs for certified professionals and public sector agencies that enhance capacity building in the country;
- Cooperative Aspect: Measured by the existence of partnerships, collaborative frameworks, and information-sharing networks between the country and the international community.

4.2. Targeted Attacks:

Most targeted attacks involve intelligence gathering, accounting for approximately 90% of such attacks. These are carried out by various entities, including states and political groups, aiming to conduct espionage and collect information for military, political, industrial, and financial purposes. Additionally, these attacks aim to cause economic and financial damage while simultaneously creating confusion and disruption.

Table 2: Performance Level of Arab Countries According to the GCI

Region	Legal	Technical	Regulatory	Training	Cooperative
Africa	0.29	0.18	0.16	0.17	0.25
The Americas	0.40	0.30	0.24	0.28	0.26
Arab Countries	0.44	0.33	0.27	0.34	0.29
Asia and the Pacific	0.43	0.38	0.31	0.34	0.39
Russian-Independent States	0.58	0.42	0.37	0.38	0.40
Europe	0.61	0.60	0.45	0.49	0.46

Source: Global Cyber security Index (GCI) 2024

4.3. Cyber Risks and Their Impact on International Peace and Security:

In their pursuit of digitizing various sectors, many governments and countries face regional and international threats through what is known as cyber attacks. The relationship between Cyber security and national security is very close, as Cyber security has established itself as a new dimension within the framework of international security. This has led to several fundamental changes in the concepts of international relations, such as the nature of conflicts and threats between states.

However, on the other hand, there are international efforts to enhance and ensure the national security of countries through the enactment of laws and regulations. These efforts are carried out by various international bodies and organizations, most notably: the United Nations, the International Telecommunication Union, the Organization for Economic Cooperation and Development, and the Organization of American States. Article 2, Paragraph 4 of the United Nations Charter states: All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations

Additionally, international legislation allows for the defense of borders and state sovereignty in the event of an attack of any kind, in accordance with Article 52 of the Charter (Gawad, 2020, p. 448). In this context, regarding Cyber security, a report issued in May 2011 indicated that: "The Internet is one of the most powerful tools of the century, enabling increased transparency and faster access to information. It facilitates citizen participation in building a democratic society. Based on the facts of recent demonstrations in the Middle East and North Africa, the Internet has played a key role in mobilizing

Cyber security in Algeria: A Strategic Approach to Address Regional Challenges and Strengthen National Sovereignty

populations to call for justice, equality, accountability, and better respect for human rights. The report calls on all states to avoid adopting laws that prohibit access to the Internet under false pretexts, such as the need to protect individual privacy, national security, or counter-terrorism" (Gawad, 2020, p. 464)

Accordingly, cyber attacks can be considered hostile acts against state institutions, necessitating cyber defense and deterrence to protect sovereignty. In this context, it is also important to note that cyber attacks should be countered through effective measures to seize the proceeds of crime and prosecute criminals. This will enhance international efforts to prevent, disrupt, and deter attackers, which requires close cooperation between law enforcement agencies and national authorities responsible for critical infrastructure. Since hackers do not recognize borders, combating global crime requires the global enforcement of agreed-upon laws (Jennifer Elliott, 2020, p. 2)

Findings and Recommendations:

Through this study, we have reached several key findings, including:

- The evolution of security from the field dimension to the cyber dimension;
- Security encompasses several branches: national security, economic security, and computer security;
- Cyber security relies on the preparation of subsystems for protection and deterrence;
- The emergence of the concept of cyber terrorism alongside the spread of cyber attacks;
- The term "cyber warfare" includes actions taken by a state to infiltrate the computers or networks of another country with the aim of causing damage or disruption;
- Ensuring Cyber security requires a set of policies and mechanisms;
- Algeria, with its economic diversity, is vulnerable to blackmail and external interference;
- The National People's Army includes an organic command represented by the command of the forces and an operational command formed by the commands of military regions;
- Algeria possesses several institutions and bodies responsible for ensuring its information security;
- Both the World Bank and the United Nations are working to develop models and propose solutions to ensure Cyber security for all countries and entities;

- Most targeted attacks involve intelligence gathering, espionage, and the collection of information for military, political, industrial, and financial purposes;
- International legislation allows for the defense of borders and state sovereignty in the event of an attack;
- Cyber attacks can be considered hostile acts against state institutions.

Bibliographie:

- ✓ Al-Sheikh, K. Y. (2015). Information Systems Security and Control. Syria: University of Damascus.
- ✓ Army, N. P. (2021). National People's Army Website. Récupéré sur mdn: www.mdn.dz/site_principal/sommaire/presentation/ministere_ar.php](https://www.mdn.dz/site_principal/sommaire/presentation/ministere_ar.php)
- ✓ Beqqa, A. (2019). The Risks of Cyber (Electronic) Attacks and Their Economic Impacts. Journal of Development Studies, Arab Planning Institute.
- ✓ Bouazidia, J. (2019). The Algerian Strategy in Combating Cybercrimes: Challenges and Future Prospects.
- ✓ Farhat, A. E. (2019). Cyberspace: Shaping the Battlefield in the 21st Century. Journal of Legal and Political Sciences.
- ✓ Gawad, A. A. (2020). Cyber Risks and Means of Addressing Them in Public International Law. Journal of Sharia and Law.
- ✓ Hamida Lahmar, F. H. (2021). Security Cooperation in Southeast Asia to Face Cybersecurity Threats. Tabnah Journal for Academic Scientific Studies.
- ✓ Hjira, A. (2017). Factors Affecting the Competitiveness of the Algerian Economy. Doctoral Thesis. University of Tlemcen, Algeria: University of Tlemcen.
- ✓ Jennifer Elliott, N. J. (2020, August 12). Cyber Risks: The New Threat to Financial Stability. Récupéré sur International Monetary Fund: 10. Jennifer Elliott, Nigel Jenkinson (2020). Cyber Risks: The New Threat to Financial Stability, International Monetary Fund, Accessed: August 12, 2021, Link: [<https://www.imf.org/ar/News/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial>
- ✓ Ouarda, K. (2021). The Problem of Citizenship in Light of Modern Technological Values: Between Citizen Freedom and Cybersecurity. Algiers: University of Algiers 1.
- ✓ Qouadra, H. (2020). Cyber Deterrence: Between Theory and Practice. Algerian Journal