

Cybersecurity Challenges in Algeria: A Comparative Study with Morocco

تحديات الأمن السيبراني في الجزائر "دراسة مقارنة مع المغرب"

Menasri ahmed ^{1*}

University of blida2. Algeria

Received: 2023/05/28; Accepted: 2023/06/06

Abstract: The issue of cybersecurity is urgent and faces many obstacles, particularly for countries. Despite this, it has captured the interest of the academic community, leading to the development of a knowledge-based framework that facilitates decision-making for finding solutions and opportunities at an empirical level. Algeria has adopted the use of electronic management and cyberspace, necessitating the adoption of security reforms and strategies to ensure its cybersecurity, particularly given Morocco's development in this field. To keep up, Algeria can take several actions, such as developing a comprehensive strategy, investing in infrastructure, providing vocational training, establishing partnerships, implementing laws, testing measures, and updating them regularly.

Keywords: , Cybersecurity ,Algerian strategy, Contemporary security challenges, Comprehensive strategy.

Résumé : La question de la cybersécurité est urgente et fait face à de nombreux obstacles, en particulier pour les pays. Malgré cela, elle a captivé l'intérêt de la communauté universitaire, ce qui a conduit au développement d'un cadre basé sur les connaissances facilitant la prise de décision pour trouver des solutions et des opportunités à un niveau empirique. L'Algérie a adopté l'utilisation de la gestion électronique et du cyberspace, ce qui rend nécessaire l'adoption de réformes et de stratégies de sécurité pour garantir sa cybersécurité, notamment compte tenu du développement du Maroc dans ce domaine. Pour suivre le rythme, l'Algérie peut entreprendre plusieurs actions, telles que l'élaboration d'une stratégie globale, l'investissement dans les infrastructures, la formation professionnelle, l'établissement de partenariats, la mise en œuvre de lois, la mise à l'essai de mesures et leur mise à jour régulière.

Mots clés : Cybersécurité, Stratégie algérienne, Défis contemporains de sécurité, Stratégie globale..

ملخص: واجهة العديد من الدول تحديات في مجال الأمن السيبراني الذي يعتبر أمرا مهما في الوقت الراهن. إذ يولي المجتمع الأكاديمي اهتماما كبيرا لهذه المسألة وقام بتطوير إطار معرفي يساعد في اتخاذ القرارات والبحث عن حلول واقعية، حيث اعتمدت الجزائر استخدام الإدارة الإلكترونية والفضاء الإلكتروني، وتبنت استراتيجيات أمنية لحماية أمنها السيبراني خاصة بعد تقدم المغرب في هذا المجال. ولمواكبة هذا التطور والتحديات، يمكن للجزائر اتخاذ العديد من الإجراءات توصلنا لها في هذه الدراسة مثل تطوير استراتيجية شاملة للأمن السيبراني، والاستثمار في البنية التحتية وتوفير التدريب المهني وإقامة الشراكات وتنفيذ القوانين والتدابير التكنولوجية وتحديثها بشكل مستمر ومنظم.

الكلمات المفتاحية : الأمن السيبراني ، الاستراتيجية الجزائرية، التحديات الأمنية المعاصرة ،الاستراتيجية الشاملة.

¹ Corresponding Author : Menasri ahmed

INTRODUCTION:

Cybersecurity encompasses a wide range of technical, organizational, and governance issues that must be considered to protect networked information systems from accidental and deliberate threats. It extends beyond the use of encryption, firewalls, anti-virus software, and other technical security tools. With the increasing prevalence of online government, business, and daily activities worldwide, the importance of cybersecurity has become more prominent. However, many organizations in emerging economies lack the organizational, technological, human resources, and other fundamental ingredients necessary to secure their systems, which is crucial for long-term success. As Algeria pursues digitization of administration and electronic money, it must also strive to achieve strong cybersecurity. In this context, the following problem arises:

The study aims to analyze and explain the experience of cybersecurity in the US and Britain, with the objective of drawing insights that.

- 1) **Problem:** Algeria is vulnerable to cyber attacks due to its increasing reliance on electronic management and cyberspace, but it lacks a comprehensive cybersecurity strategy to protect its critical infrastructure and sensitive data.
- 2) **Hypothesis:** Developing a comprehensive cybersecurity strategy that includes risk assessments, incident response plans, and regular testing and updating of measures will enhance Algeria's cybersecurity and protect its critical infrastructure and sensitive data from cyber attacks.

To address this problem and test the hypothesis, we will follow these steps:

- **The Basics of Cybersecurity Concepts**
- **Information about cybersecurity in Algeria**
- **Cybersecurity in Morocco and Algeria: A Comparative Analysis of Capabilities and Challenges"**

As views, our main goal is to develop a strategy A cyber security plan that is applicable at the national level and any Complies with international standards, with the ultimate goal is Defining a national cybersecurity strategy for its development

I THE BASICS OF CYBERSECURITY CONCEPTS:

A. Definition of cybersecurity:

- 1) Cybersecurity is the practice of protecting electronic devices, networks, and sensitive information from unauthorized access, theft, damage, or disruption. It involves using a

combination of technical, administrative, and physical controls to safeguard digital assets and ensure the confidentiality, integrity, and availability of data.

- 2) Cybersecurity refers to the practice of protecting computer systems, networks, and sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction, as well as from other cyber threats such as viruses, malware, and hacking. It involves implementing various technologies, processes, and policies to safeguard against cyber attacks and to ensure the confidentiality, integrity, and availability of digital assets. The National Institute of Standards and Technology (NIST)
- 3) The American mathematician Professor Norbert Wiener is widely regarded as the spiritual father and founder of a field known as "cybernetics", which deals with the control and communication of animal and machine systems. Wiener's seminal work involved defining this field as the science of command and control, including the transmission of messages between human-machine and machine-machine interactions. In essence, cybernetics is concerned with the ability to regulate and direct the behavior of various systems. (Norbert Wiener 1947)
- 4) The Information Security Agency (ANSSI) describes the cybersecurity as a “desirable state for an information system enable to resist to cyberspace events, whose objective is to ensure information confidentiality, integrity and availability”.

B. The Importance of Cybersecurity :

- 1) Safeguarding sensitive data in cyberspace should be a top priority for governments and societies to ensure continued use.
- 2) Cybersecurity is necessary on an individual level to protect personal data, accounts, and passwords. (Asaad, R 2021).
- 3) Community-level data protection helps prevent social engineering and target social behavior.(Hamad Al-Sayed Al-Najjar 2015)
- 4) Corporate-level cybersecurity is essential to protect electronic assets, data, and information. (Jubair, M. A., Mostafa...and others; 2022).
- 5) State-level cybersecurity defends financial, economic, military, television, and radio networks from electronic attacks, piracy, and interruption.
- 6) Cyberattacks cost businesses and whole nations tens of billions of dollars each year, and hundreds of thousands of electronic attacks occur daily. (Saini, D. K., & Yousif, J. H. 2021).
- 7) Governments and large companies have created departments specializing in cybersecurity, information security, and network security. (Asaad, R. 2021)
- 8) The cyber power of a state, as well as its capacity to protect itself and its electronic security, is an important factor in national strength.(Mondal, A., Paul, S., Goswami, R. T., & Nath 2020).

C. the development of interest in cybersecurity:

As with any technological advance throughout history, whenever new opportunities are created, there will always be those that exploit them for their own gain; Here's a diagram and some information on the development of interest in cybersecurity:

Early Days --> Hacking Culture --> Digitalization --> Cyber Attacks --> Cybersecurity Awareness.

- 1) **Early Days:** In the early days of computing, there wasn't much concern for cybersecurity. This was due to a lack of awareness about the potential dangers of hacking and cyber attacks.
- 2) **Hacking Culture:** In the 1980s and 1990s, the hacking culture emerged. Hackers became interested in exploring the limits of computer systems and breaking into them for fun or profit. This culture helped to raise awareness of cybersecurity issues.
- 3) **Digitalization:** As technology advanced and became more ubiquitous in the 2000s, the need for cybersecurity increased. With more people and organizations relying on digital systems to store and transmit sensitive information, the potential for cyber attacks became much greater.
- 4) **Cyber Attacks:** In the late 2000s and early 2010s, there were a number of high-profile cyber attacks that made headlines around the world. These attacks demonstrated the serious consequences that can result from a successful cyber attack, such as data breaches, financial losses, and reputational damage.
- 5) **Cybersecurity Awareness:** As a result of these high-profile cyber attacks, there has been a growing awareness of the importance of cybersecurity. Organizations have started investing more in cybersecurity measures, and there has been a surge in interest in cybersecurity as a career path. (Forbes 2020)

D. Cybersecurity Fields :

- 1) Cyber Security Fields are in high demand globally due to the increasing need for digital protection. The Arab world is also recognizing the importance of cybersecurity, and it is expected to become a sought-after discipline in the near future. This field includes various specializations and sub-specialties, such as network security, cloud security, cryptography, and ethical hacking. Job titles in this field can range from cybersecurity analyst to chief information security officer, and they offer high-paying salaries and job stability ,The cybersecurity specialization is divided into several sections, sub-specialties, and job titles, including (Syed, A., Purushotham, K., and Shidaganti, G 2020).
- 2) **Network Security:** This type of security protects computer networks from attacks, both from within and outside the network, using modern technologies and protocols to prevent malicious programs from infiltrating the network. Network security is like a firewall that prevents untrusted third parties from accessing electronic networks through various security settings.
- 3) **Application Security:** It is the process of protecting sensitive information at the application level, represented by a set of security measures that users must take before

using the application, such as setting strong passwords, answering security questions, or using two-stage authentication.

- 4) Cloud Security: It is a means of protecting personal information and data stored in electronic clouds, such as Google Drive, Microsoft OneDrive, and Apple iCloud. These cloud storage systems are highly efficient and capable of safeguarding data.
- 5) Operational Security: This type of security is used by risk management officials in companies and organizations to find alternative plans in case data is exposed to a breach. It includes educating employees and workers in best practices for preserving various types of data and information, whether personal or commercial.
- 6) Recommendations from the National Cyber Security Center (NCSC): The Recommendations outlines several important guidelines recommended by the National Cyber Security Center (NCSC) to maintain privacy and security when using the internet. These guidelines include keeping frequent backups of important data, updating operating systems and software with the latest security patches, installing antivirus and anti-malware software, using secure passwords and two-factor authentication, encrypting sensitive information, being cautious of clicking on links, using firewalls and VPNs, and securing Wi-Fi networks. Following these guidelines can help protect individuals against cyber threats such as phishing, ransomware, and hacking. (Asaad, R. 2021)

E. Measure Cybersecurity Risk:

There are different approaches to measuring cybersecurity risk, but some common methods include:

- 1) Risk Assessment: This involves identifying potential threats and vulnerabilities, evaluating the likelihood and impact of each threat, and determining the level of risk associated with each threat. Risk assessment can be qualitative or quantitative, depending on the level of detail and data available. (NIST)
- 2) Risk Scoring: This involves assigning a score to each risk based on its likelihood and impact. The score can be used to prioritize risks and allocate resources accordingly. There are various risk scoring frameworks, such as the Common Vulnerability Scoring System (CVSS) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
- 3) Risk Modeling: This involves simulating potential cyber attacks and evaluating their impact on the organization. Risk modeling can help organizations identify and prioritize the most critical assets and systems and develop effective mitigation strategies. (JOINT TASK FORCE 2018)
- 4) Compliance Assessment: This involves evaluating the organization's compliance with relevant regulations and standards, such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). Compliance assessment can help organizations identify gaps in their security controls and prioritize remediation efforts.

- 5) ISO cybersecurity standards: ISO cybersecurity standards are used by many organizations for compliance. However, there are some concerns with ISO 27001 standards that should be noted.
- 6) Firstly, Management Standard Framework:ISO 27001 is a management standard framework, not a security-specific standard.
- 7) Secondly, Framework for Managing Security: it provides a framework for managing security within an organization but does not offer a step-by-step guide for implementing security measures.
- 8) Thirdly, Compliance vs Security :compliance or certification to ISO 27001 does not guarantee complete security. It only means that an organization is managing security according to the standard and at a risk level deemed appropriate.
- 9) Fourthly, Limited Guidance on Controls :although ISO 27002 offers some guidance on controls, it does not provide detailed guidance for specific organizations, the information they handle, or the systems they use.
- 10) Lastly, Security Expertise Required :implementing an information security risk assessment and defining necessary security controls requires security expertise.

Table 1: Security Vulnerability Assessment

Asset ID	Asset ID Information	Possible security threats
1	User credentials	User Impersonation
2	Personal data and mobile applications Information Collected by Devices	Identity and credential theft. Malicious code injected into apps installed on a phone
3	Smart home status information Structure of the smart home	Editing information. Denial of Service (DoS) Attacks .Compromises of devices or sensors./Disclosure of information Function interrupt
4	Inventory Information	Access inventory information to find a specific device.with known vulnerabilities to attack smart homes
5	Newspaper information	Access log data and get useful insights.enabling possible attacks on a smart home system
6	The information is transmitted via a gateway	Steal information from packets transmitted through a gateway
7	Smart Home Setup Information	Editing Information
8	Video feeds from surveillance cameras	Control cameras to monitor and spy on users

9	Location information	Observation of location data traffic
10	Information Resources. (for example, images, documents and music)	Steal private information. Make stored media inaccessible due to hardware failure

II Information about cybersecurity in Algeria:

Algeria is a country in North Africa with a growing economy and an expanding digital infrastructure. However, like many countries, Algeria is also vulnerable to cyber threats and faces challenges in ensuring the security of its networks and information systems.

A. Key Points on Cybersecurity in Algeria: Here are some key points about cybersecurity in Algeria:

- 1) **National Cybersecurity Strategy:** In 2016, Algeria launched a National Cybersecurity Strategy, which aims to strengthen the country's cybersecurity posture and protect critical infrastructure. The strategy includes measures such as increasing awareness of cybersecurity threats, enhancing the legal framework for cybersecurity, and developing a national cybersecurity center.
- 2) **Cybercrime:** Algeria has seen a rise in cybercrime in recent years, with attacks ranging from phishing scams to ransomware attacks. In 2020, the Algerian police reported a significant increase in cybercrime cases, with many of the attacks targeting financial institutions and government agencies.
- 3) **Infrastructure:** Algeria has invested heavily in its digital infrastructure, with the country's internet penetration rate increasing from just 4% in 2007 to over 42% in 2021. However, the rapid growth of digital services has also created vulnerabilities in the country's networks and information systems.
- 4) **Education and Training:** Algeria has taken steps to address the shortage of skilled cybersecurity professionals in the country by developing educational and training programs. For example, in 2020, the National Cybersecurity Center launched a training program for cybersecurity professionals.
- 5) **Regional Cooperation:** Algeria is a member of the African Union's African Union Convention on Cyber Security and Personal Data Protection, which aims to promote cooperation and coordination among African countries in addressing cybersecurity challenges.

Overall, while Algeria has made progress in developing its cybersecurity capabilities, the country still faces significant challenges in protecting its networks and information systems from cyber threats.

B. Cybersecurity Indicators in Algeria :

The following points summarize the indicators of cybersecurity in Algeria:

- 1) According to the latest report by the specialized platform "Data Portal" on internet and mobile phone statistics worldwide, the number of internet users worldwide reached 4.6 billion people, representing 59.5% of the estimated global population of 7.8 billion people.
- 2) As for Algeria, the same source indicates that the number of internet users in January 2021 was about 26.35 million people, an increase of 3.6 million new subscribers compared to the same period last year.
- 3) The source also explains that the percentage of internet usage in Algeria reached 59.6% of the total population, estimated at 44.23 million; These numbers have a positive implication for the reality of the internet in Algeria, and represent an important step towards building a more inclusive information society. However, they also highlight the urgent need to increase electronic protection at the national level to enhance cybersecurity in Algeria.

C. The most important indicators of electronic fragility in the field of cybersecurity in Algeria are as follows:

- 1) Preparedness for electronic attacks: 0.262 out of 1, for example, Egypt scored 0.8.
- 2) Latest legislation in 2020: only one law was enacted (01).
- 3) Percentage of mobile phones infected with malware: 26.47%, currently at least one out of every four phones in Algeria has malware, with Finland having the lowest infection rate for mobile devices at 0.87% of users.
- 4) Percentage of computers infected with malware: 19.75%.
- 5) Percentage of users who have been targeted by financial malware attacks: 0.5%, with Belarus having the highest rate at 2.9%, and Denmark having the lowest rate at 0.1%. The reason Algeria's rate is considered acceptable compared to the best rate is due to the fact that Algeria does not yet have an extensive electronic payment system, and these types of malware are often distributed through hacked or fraudulent websites or unwanted emails. The latter, once they infect users, simulate login pages for official banking services and steal personal user information, such as bank account information, passwords, or payment card data.(Ali Majdi2021)

This low ranking for Algeria can be attributed to the Algerian societal culture in cyberspace in general, where Algerians often do not distinguish between licensed and malicious applications, and download applications or programs from untrusted sources that may contain spyware and data theft programs. Even globally, statistics show that 95% of breaches occur due to human error."

- Example: Most Algerians use the word processing program Word, developed by Microsoft, on their devices. Originally, this program is not free and costs \$60 for an annual home subscription. However, Algerians resort to downloading modified copies of the program, known as "cracked" software. A "crack" is a computer program designed to modify the behavior of software and break its protection to remove usage restrictions. These modifications aim to use paid software as if the hacker had paid for the license.

Interestingly, some sensitive public administrations in Algeria use these pirated programs without taking into account their security risks in the electronic field.

D. The Use of Social Media to Undermine Stability (Risks and Challenges in Algeria):

Exploiting social media to undermine the stability of countries. The number of subscribers on social media platforms in Algeria is estimated to be 25 million people, representing 56% of the population, with Facebook being the largest platform with 23 million Algerians registered. However, this network has become a means to spread fake news, rumors, and incitement, and was heavily used during what was called the "Arab Spring". Looking at the list of the most visited websites by Algerians on a daily basis, we can estimate the risks that an Algerian individual may be exposed to in an unmonitored environment, allowing the dissemination of any news content without verifying its accuracy. The most visited websites by Algerians in 2020 were found to be spending 18 minutes daily on Facebook, 18 minutes on YouTube, and 15 minutes on Google, all of which are American websites, meaning that Algerians spend a total of 51 minutes daily on these websites. The challenges facing Algeria in this context are not about hacking and espionage, but rather about the ability to influence people's opinions or impact them through various forms of political propaganda.

E. Cybersecurity in Algeria: A Priority for National Development:

A Priority for Decision-Makers in Algeria's Digital Government Era ; The need for a national workforce to enhance cybersecurity in Algeria, especially as the government promotes electronic transactions, both administrative and financial, cannot be overlooked. Establishing a national base to provide accurate statistics on Algeria's cybersecurity status is essential, as relying on foreign sources as a reference for evaluating Algeria's cybersecurity is insufficient. (Ali Majdi2021)

III Cybersecurity in Morocco and Algeria: A Comparative Analysis of Capabilities and Challenges:

A. Information about cybersecurity in Morocco:

The collection and processing of personal data in Morocco is governed by the Data Protection Law (Law no. 09-08) and its implementing Decree (No. 1-09-15), which regulate automatic and manual processing of personal and sensitive data. The Law applies to individuals (referred to as "data subjects") and not to legal persons such as limited liability companies or private limited companies. Personal data processing includes any operation performed by automatic or non-automatic means that is part of a filing system. The National Control Commission for the Protection of Personal Data (CNDP) enforces the Data Protection Law and has issued several binding decisions on personal data processing. No announced changes have been made to the data protection and privacy law yet. However, it is possible that a reform may occur in the future to implement GDPR-like regulations (Mehdi Kettani 2009)

- 1) following laws :In terms of cyber security investigations in Morocco, the legal situation is governed by several laws, including Law no. 09-08 on personal data protection and its implementing Decree no. 1-09-15, Law no. 31-08 on consumer protection (related to online advertising and spamming), Law No. 07-03 supplementing the penal code regarding the repression of offenses relating to automated data processing systems, Law no. 34-05 amending and supplementing Law 2-00 relating to copyright and neighboring rights, and Law no. 05-20 on cybersecurity.

- 2) Practical side: To address cybersecurity challenges and harmonize with partner countries, it's important to upgrade and update the legal and regulatory framework. Necessary entities should be established to implement the national cybersecurity policy and promote the development of security capabilities. Additionally, awareness among citizens, enterprises, and administrations on cybersecurity and cyber confidence issues should be raised. By taking these practical steps, Morocco can improve its cybersecurity investigations and better protect personal data. (Taieb EBBAGH 2009)

B. Information about cybersecurity in Algeria:

- 1) following laws :In Algeria, cybercrime was legally defined and deemed punishable under Article 02 of Law No. 04-09, enacted on 09.05.2009. The law was aimed at regulating media, communication, and messaging (Samir Bara2020)
- 2) while the electronic guide was provided in the third item of Law 10-05, issued on 2005.06.20. The articles in the Code of Criminal Procedure (720.238.212.156.143.79.65) were also amended (396.394.333.303). Algeria's internal legislation has been aligned with international laws and agreements, particularly the one signed in Budapest, Hungary, on November 23, 2001, which covers cybercrimes. This agreement is considered the legal reference for all international legislation in this field. (Sherif Bassam2016)
- 3) Practical side: The paragraph discusses the measures taken in Algeria to achieve cyber security. The higher authorities of the state have entrusted specialized bodies within the security services with the task of implementing these measures. The authorities have recommended respecting freedoms within the framework of constitutional legitimacy and international covenants. The paragraph mentions three bodies responsible for achieving cyber security:
 - The Central Department for Combating Information Crime (SCLC), affiliated to the National Security Directorate. This body has human resources that have professional competence to carry out their tasks at the international and national levels. They communicate with the scientific police and decentralized offices specialized in crime.
 - The Center for Prevention of Computer and Information Crime Crimes (CPLCIC), affiliated to the General Command of the National Gendarmerie. It has similar tasks to its counterparts affiliated with the National Security, and coordination takes place under the direct responsibility of the Attorney General.
 - The National Institute of Criminal Evidence and Criminology of the National Gendarmerie (INCC), also affiliated to the General Command of the National Gendarmerie. The institute relies on scientific expertise and accurate laboratory experiments to investigate crimes committed using electronic devices.

Table 2: secure internet servers in Algeria and Morocco from 2010 to 2020.

yaers	Secure internet servers/algeria	Secure internet servers/Morocco
2010	13	51
2011	18	76

2012	46	113
2013	68	182
2014	94	244
2015	152	328
2016	309	859
2017	2621	10115
2018	2855	10655
2019	2154	13479
2020	2106	16219

Source: World Bank

secure internet servers in Algeria and Morocco from 2010 to 2020.

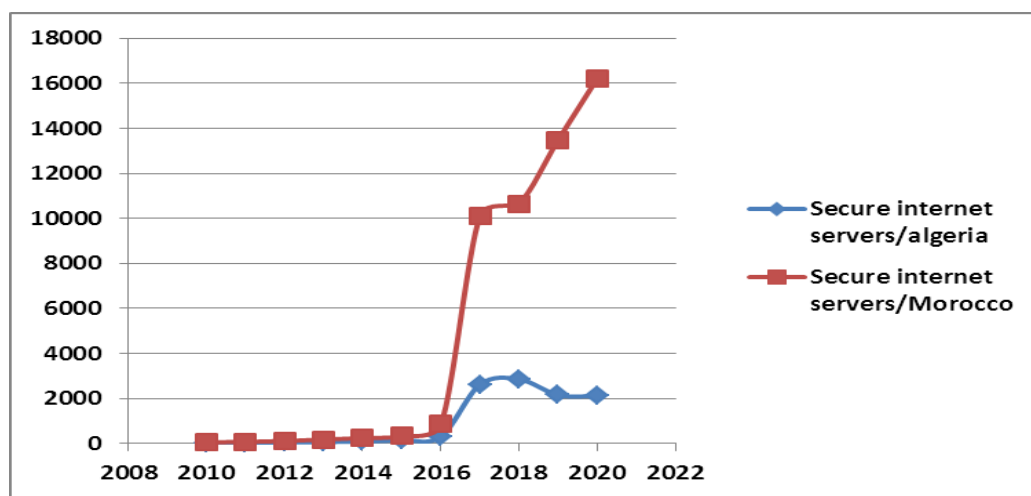


Figure 1: Secure Internet Servers in Algeria and morocco

Through the previous table and Figure 1 :

- 1) The data provided shows the number of secure internet servers in Algeria and Morocco from 2010 to 2020. Here are some observations and analyses:
- 2) The number of secure internet servers in both Algeria and Morocco has been increasing steadily over the years.
- 3) In 2010, Algeria had only 13 secure internet servers, while Morocco had 51. However, the gap between the two countries has been narrowing over the years.
- 4) In 2017, there was a significant spike in the number of secure internet servers in Morocco, with the number jumping from 182 in 2013 to 10,115 in 2017. This represents a nearly 55-fold increase in just four years.
- 5) Algeria, on the other hand, experienced a more gradual increase in the number of secure internet servers during the same period, with the number increasing from 68 in 2013 to 2,621 in 2017, which is still a significant increase.
- 6) Despite Morocco's huge increase in the number of secure internet servers in 2017, both countries had a similar number of servers in 2018 and 2019. However, in 2020, Morocco once again surpassed Algeria in the number of secure internet servers.

- 7) Overall, the data suggests that both Algeria and Morocco are investing in the development of their digital infrastructure and are increasing their capacity for secure online transactions and communication

C. Comparing Morocco and Algeria's Cybersecurity Capabilities and Challenges:

In recent years, Morocco and Algeria have demonstrated recognition of the significance of cybersecurity, and both countries have implemented national cybersecurity strategies and established dedicated institutions to monitor and coordinate their cybersecurity efforts. Despite these similarities, there are notable differences in their respective cybersecurity capabilities and challenges. The Global Cybersecurity Index (GCI) 2020 reported that Morocco outranked Algeria, with Morocco ranking 46th and Algeria ranking 92nd. The GCI measures countries' commitment to cybersecurity based on five pillars: legal, technical, organizational, capacity building, and cooperation (Samir Bennis2018). Furthermore, Morocco's IT industry is more developed, and it has a larger pool of skilled cybersecurity professionals than Algeria. Additionally, Morocco has formed partnerships with international organizations such as the European Union and the United Nations to enhance its cybersecurity capabilities. However, both countries face similar cybersecurity challenges, including an increase in cybercrime, low levels of cybersecurity awareness among their citizens, and criticisms of surveillance practices and alleged human rights violations (Prof. Dr. Juliane Brach and others2020) To address these challenges effectively, both Morocco and Algeria must continue investing in their cybersecurity capabilities.

IV CONCLUSION :

Effective cybersecurity is a crucial aspect of any organization's risk management strategy. As cyber threats become more sophisticated, it's essential for organizations to stay informed about the latest threats and best practices for cybersecurity. By adopting proactive measures, including risk management, employee training, and incident response planning, organizations can better safeguard against cyber threats and minimize the potential damage of a cyber attack.

In Algeria, the government launched a National Cybersecurity Strategy in 2016, aimed at protecting critical infrastructure, raising cybersecurity awareness, and establishing a national cybersecurity center. However, cybercrime incidents targeting financial institutions and government agencies have increased in the country. Algeria has invested heavily in digital infrastructure, resulting in a higher internet penetration rate, but this has also made its networks and information systems more vulnerable. To tackle the shortage of skilled cybersecurity professionals, Algeria has created training programs and is part of the African Union's convention on Cyber Security and Personal Data Protection to promote regional cooperation.

Morocco has implemented a comprehensive national cybersecurity strategy and established partnerships with international organizations. In comparison, Algeria has developed its own strategy to address modern security challenges. Both countries face similar cybersecurity issues, emphasizing the need for ongoing investment in their cybersecurity capabilities to effectively address these challenges.

VI Bibliography:

A- Books:

- NORBERT WIENER, Cybernetics or control and communication in the Animal and the machine, published in, UK,1947
- Mondal, A., Paul, S., Goswami, R. T., & Nath, S. Cloud computing security issues & challenges: A Review. 2020.
- Mehdi Kettani ; Data Protection & Cyber Security Law: Morocco; COUNTRY COMPARATIVE GUIDES 2022.
- ndré Lucas, Jean Devrèze, Jean Frayssinet, Computer and Internet Law, Dalloz edition, Thémis collection (Private Law), , (France), November 2001.

B - Newspaper articles:

- Asaad, R. Penetration Testing: Wireless Network Attacks Method on Kali Linux OS. Academic Journal of Nawroz University, 10(1),p 7–12. 2021.
- Hamad Al-Sayed Al-Najjar, Muhammad Abd Al-Hadi Allam, Information Wars: Who Faces It? Al-Ahram Magazine, Issue 13 (139, July), 2015.
- Jubair, M. A., Mostafa...and others Cryptography Routing Protocol for Enhancing Efficiency and Security of VANETs. IEEE Access, date of publication 24 November 2022.
- Saini, D. K., & Yousif, J. H. Vulnerability and Attack Detection Techniques: Intrusion Detection System. In Cybersecurity Applied computing Journal; Volume 2, Issue 4, October 2022.
- JOINT TASK FORCE ;Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy; This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-37r2>. December 2018.
- Ali Majdi, The Reality of Cybersecurity in Algeria, Al-Shaab Newspaper, published on 05/19/2021.
- Sherif Bassam, “The Reality of Electronic Governance in the Arab Countries,” Journal of Social and Human Sciences, University of Algiers, 3, No. 6, June, 2016.
- Samir Bennis. The Cybersecurity Challenge in North Africa: The Case of Morocco Available at: <https://www.atlanticcouncil.org/wp-content/uploads/2018/06/The-Cybersecurity-Challenge-in-North-Africa-The-Case-of-Morocco.2018>.
- Prof. Dr. Juliane Brach and others ,Security Implications of Emerging Technological Challenges in North Africa. PEN Publications – Security Implications of Emerging Technological Challenges in North Africa; Volume 4 | Number 1 | Spring 2020.

C - Seminar papers:

- Syed, A., Purushotham, K., and Shidaganti, G. (2020). Cloud Storage Security Risks, Practices and Measures: A Review. 2020 IEEE International Conference for Innovation in Technology (INOCON), Innovation in Technology (INOCON), 2020.
- Taieb DEBBAGH; Secretary–General Ministry of Industry, Trade and New Technologies, Morocco; ITU Regional Cybersecurity Forum for Africa and Arab States Tunis, Tunisia; 4-5 June 2009.

D - Websites:

- The National Institute of Standards and Technology (NIST), <https://www.nist.gov/topics/cybersecurity>
- <http://www.ssi.gouv.fr/>
- Forbes ; The Evolution of Cybersecurity: A Brief History; <https://www.forbes.com/sites/forbestechcouncil/2020/02/04>
- National Institute of Standards and Technology (NIST) Cybersecurity Framework: <https://www.nist.gov/cyberframework> 2023.
- Common Vulnerability Scoring System (CVSS): <https://www.first.org/cvss/.2023>
- "Cybersecurity Risk Management" by the International Organization for Standardization (ISO): <https://www.iso.org/standard/54534.html>.
- "Algeria's Cybersecurity Challenges." Carnegie Endowment for International Peace. Available at: <https://carnegieendowment.org/2017/04/20/algeria-s-cybersecurity-challenges-pub-68668>.2023
- "Algeria: Cybersecurity Law." Library of Congress - Global Legal Monitor. Available at: <https://www.loc.gov/law/foreign-news/article/algeria-cybersecurity-law..2023>
- "Algeria: Cybersecurity Law Aims to Protect National Security, But Raises Privacy Concerns." Global Voices. Available at: <https://globalvoices.org/2016/08/24/algeria-cybersecurity-law-aims-to-protect-national-security-but-raises-privacy-concerns/.2023>
- "Algeria Takes Steps to Improve Cybersecurity." Inside Arabia. Available at: <https://insidearabia.com/algeria-takes-steps-to-improve-cybersecurity/.2023>
- "Algeria Takes Steps to Improve Cybersecurity." Inside Arabia. Available at: <https://insidearabia.com/algeria-takes-steps-to-improve-cybersecurity/.2023>