مجلة أبعاد إقتصادية
REVUE ABAAD IKTISSADIA
جامعة امحمد بوقرة بومرداس
Abaad Iktissadia Review Vol: (14) N°(01) year: 2024 pages(368-390)

Cybersecurity as a Fundamental Element of The Digital Economy in Algeria

Sereir El Hirsti Hayet *
Laboratory of Economic and Human Development in Algeria.
University of Blida 2, Algeria
Email: h.sereir-elhirtsi@univ-blida2.dz

Benine Abderrahmane
Laboratory of the Management of Local Communities and their Role in Achieving Development,
University of Blida 2
Algeria
Email : a.benine@univ-blida2.dz

submitted:04/03/2024 Accepted:25/05/2024 published:30/06/2024

Abstract:

The digital economy is an extremely fast-paced industry with an evolving environment prone to innovation. Such a circumstance encourages companies to favor a rapid route to market, sometimes at the expense of data security. The balance between data security and digital innovation is pivotal and should be considered in the highest regard in growing the digital economy. For that, there is a need for secure cyberspace which is the essence of cybersecurity. This work addressed the importance of cybersecurity and its requirements in protecting the digital economy and the efforts made by Algeria to achieve this. The descriptive analytical approach was used, and data was collected from primary and secondary sources and analyzed using content analysis, where objective analytical interpretations were used.

This study discovered that cybersecurity in Algeria is more vulnerable to risk and that some threats and vulnerabilities could affect its digital economy, efforts to enhance cybersecurity are insufficient. Therefore, this study recommends improving information security systems, providing high-tech technology for cybersecurity purposes, building human resources capabilities, developing the judicial and security system making it in line with international developments, and preparing for the unexpected future.

Keywords: Cybersecurity; Digital Economy; Cyberthreats, Algeria.

Jel Classification Codes: F10; O33; D8, C18.

---

* **correspondent author**

Introduction

The global economy has witnessed a massive and accelerating digital transformation, creating new business models and innovative products and services. Digital information technology has replaced devices, and data has become a valuable currency in this new digital era. However, the focus is increasingly shifting from the economic benefits to the risks arising from the use of information and communications technology (ICT), namely cybersecurity risks.

Cybersecurity is a new field of security study that is not fully understood in terms of its nature, dimensions, and trends, which explains the difficulty of dealing with it. Cybersecurity includes the protection of information, confidential data, permissions, and defense. Cybersecurity is primarily concerned with cyberattacks.

Cyberattacks continued to increase during 2020 and 2021, not only in numbers but also in terms of their impact. The COVID-19 pandemic is also expected to impact the cybersecurity threat landscape. One of the most lasting developments to emerge from the COVID-19 pandemic is the permanent shift to a hybrid office (work from home) model. As a result, we have seen a rise in cyberattacks targeting organizations and businesses through home offices.

Algeria has not been spared from cyberattacks, as Trend Micro Incorporated, the global leader in cybersecurity, blocked more than 29.7 million threats in Algeria in 2022. The company detected and blocked more than 19 million (19,552,217) threats via email, and more than 400,000 (417,156) malicious URL attacks, In addition, more than half a million (508,815) malware attacks were identified and stopped (TrendMicro, 2024).

There are ongoing efforts in Algeria towards transitioning to the digital economy, and on its way to doing so, it must take into account the importance of cybersecurity in protecting its digital economy. Accordingly, this research paper came to answer the following problem: **How does cybersecurity contribute to protecting the digital economy, and what are the efforts made by Algeria to achieve this?**

The following questions arise from this problem:

- What is meant by cybersecurity?
- What are the requirements for cybersecurity in the digital economy?
- What is the impact of cybersecurity threats on the digital economy?
- What is the level of cybersecurity in Algeria?
- -What are the measures and efforts being made to enhance cybersecurity in Algeria?

This research paper aims to:

- Explain the concept of cybersecurity and its importance in the digital economy.
- Presenting the most important cybersecurity requirements to protect the digital economy.
- Revealing the level of cyber security in Algeria.
- Shedding light on the efforts made by the Algerian state to enhance cyber security to protect its economy.
- Providing recommendations to enhance cybersecurity and protect the digital economy in Algeria.

The importance of this study lies in the importance of the issue of cybersecurity, which has become one of the most important pillars of the digital economy in the world and requires awareness of the seriousness of cyber threats, and activating the cybersecurity system in various sectors of the country, and protecting the communications and information technology infrastructure of various institutions from cyber risks.

Literature Review

In this section, we will present previous studies related to cybersecurity and the digital economy:

The (Bakri & al, 2019) study showed that Malaysia is one of the most important pioneering countries in the field of the digital economy, which made it need secure cyberspace, which is the essence of cybersecurity. Moreover, the study demonstrated the impact of secure cyberspace or the role of cyber security in promoting the digital economy in Malaysia through a reliable law for clients and companies. Where this study focused on the legal aspect only and neglected other aspects such as the

organizational aspect, the technological aspect of the human aspect, the study also found that cyber security in Malaysia is less vulnerable to cyber threats, but the study did not clarify the procedures and ways that Malaysia used to reduce these threats.

The (Chooi & Ahmad, 2017) study sought to gain insights into the relationship between the development of the NCSS National Cybersecurity Strategy and the success of the nation's digital economy based on literature from journal articles, global reports, current industry events, and market trends. Where the study attempted to analyze the National Statistics Center in nine countries on the success of the digital economy. Interestingly, it was found that the nation's willingness to foster a digital economy is not related to the development and dissemination of the nation's NCSS. Although the study demonstrated the importance of cybersecurity to protect and enable the digital economy. Moreover, the study showed that countries with high digital trust rely less on NCSS at the national level to enhance trust in the digital space, but the study completely neglected the reasons that led to this.

While, the (Babayo & al, 2021) study clarified the repercussions of cybercrime and weak defense of cybersecurity on Nigeria's national security and digital economy. To the emergence of Internet crimes. Furthermore, the study reported scholarly opinions from whistleblowers about the effects of cybercrime on national security and the digital economy in Nigeria. In theory, the study succeeded in linking the various existing proposals on issues of national security and cybersecurity and empirical evidence emerging from the study area.

Also, the study (Leahovcenco, 2021) discussed issues related to cybersecurity and cyberattacks. Interestingly, this study provided an analysis of the relationship between the share of the digital economy in GDP and the GCI index using correlation analysis; As this study is one of the few studies that used criteria specific to cybersecurity, the Global Cybersecurity Index (GCI) is a composite index produced, analyzed and published by the International Telecommunication Union (ITU) to measure countries' commitment to cybersecurity to increase

cybersecurity awareness. This study also discussed the situation in the field of cyber security in the Republic of Moldova and made suggestions for its improvement. However, it did not explain the measures taken by Moldova to strengthen its cybersecurity.

Our current study sought to emphasize the importance of cybersecurity in protecting and empowering the digital economy, in agreement with previous studies. Moreover, this study sought to reveal the level of cybersecurity in Algeria and the efforts made to enhance cybersecurity and protect the digital economy.

Methodology

This article is based on literature research. Information has been accessed from a variety of literature, based on journal articles, global reports, and current trends. After collecting the literature, the researchers screened it to determine its suitability to finalize the representative literature on the topic. Representative literature from the years 2013 - 2024 was selected. Because issues related to cybersecurity are new and rapidly changing, representative literature on this topic must be current to be relevant. Articles and reports from reliable sources have been included in this article. This research provides a review of recent practices and developments in the field of cybersecurity and the digital economy.

Firstly. Cybersecurity Concept

1. Definition

The word cyber is generally believed to originate from the Greek verb κυβερεω (kybereo) to steer, to guide, to control. At the end of the 1940s, Norbert Wiener (1894–1964), an American mathematician, began to use the word cybernetics to describe computerized control systems. According to Wiener, cybernetics deals with sciences that address the control of machines and living organisms through communication and feedback (Lehto, 2013, p01). There is no general consented definition of cybersecurity. however, The following definitions can be given:

Cybersecurity is defined as technologies and processes constructed to protect computers, networks, and sensitive information from unauthorized access by cyber criminals, and hackers. (Rajesh, 2015, p. 14). In other words, Cybersecurity is protecting information and

information systems (networks, computers, databases, data centers, and applications) with appropriate procedural and technological security measures (Luiijf & al, 2013, p. 6).

Cybersecurity is the set of technologies, processes, practices, response, and mitigation measures designed to protect networks, computers, software, and data from attack, damage, or unauthorized access to ensure confidentiality, integrity, and availability (Craigen& al, 2014, p. 15)

Cybersecurity refers to the set of processes and techniques used to protect networks, information systems, data, and users who could be affected by a cyber threat (Leahovcenco, 2021, p. 97). So, cybersecurity is the collection of tools, policies, security concepts, and risk management approaches to protect Cyberspace (Luiijf & al, 2013, p. 6).

In addition, Cybersecurity refers to the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation Craigen& al, 2014, p. 15)

Moreover, cybersecurity means the activities necessary to protect network and information systems, users, of such systems, and other persons affected by the cyber threat (Leahovcenco, 2021, p97).

From the above, we conclude that cybersecurity refers to the totality of technologies and processes used to ensure the availability and continuity of information systems and enhance data protection, confidentiality, and privacy.

2. The Importance Of Cybersecurity

The importance of cybersecurity lies in the fact that cyber-attacks cause huge losses that cost companies and countries billions of dollars annually, as countries are exposed to hundreds of thousands of cyber-attacks every day and cases of disruption or theft of systems, information. Below is an explanation of the importance of cybersecurity:

Cybersecurity is one of the fast-growing technical fields, not only in IT sectors but also in economics, health, banking, education, military, government, and public sectors as well. This is due to its great importance in all sectors (Dummanaboyina, 2024, p. 2).

Where organizations are based collect, process, and store unparalleled amounts of data on computers and other devices. Some of this information may be sensitive data and information for which unauthorized access or publicity should have poor consequences. (Singh, 2021, p. 1).

Further, most of the time governments face difficulties due to inappropriate infrastructure, lack of awareness, and insufficient funding. Government bodies need to provide reliable services to society, maintain secure citizen-to-government communications, and protect confidential information (Rajesh, 2015, p. 14).

For example, in July 2015, (Chris Valasek) and (Charlie Müller) hacked a Jeep Cherokee car while someone was driving it on a highway. Weaknesses in the car's info-entertainment system have enabled hackers to remotely control it using their smartphones. Which led the company to recall and repair 1.4 million cars (Spremić & Simunic, 2018, p. 2)

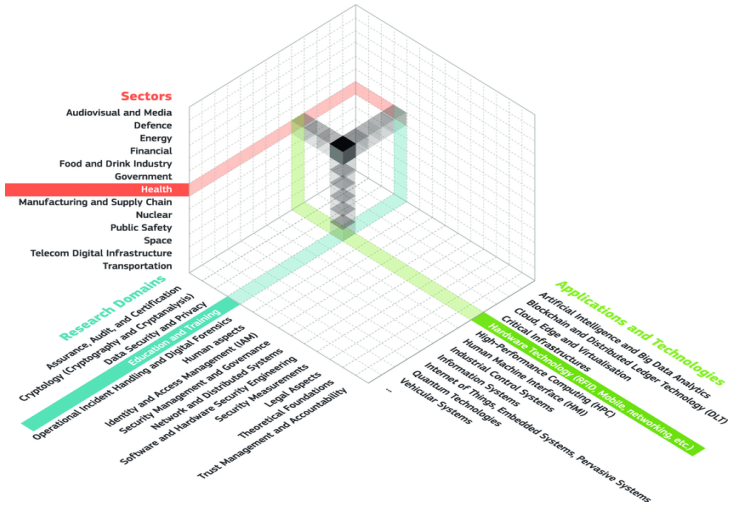
In 2001, CNA Financial was hacked by a group of hackers called 'Phoenix'. The hack affected 75,349 individuals. More than 15,000 of the company's devices were encrypted and the company's networks were disrupted, forcing CNA to temporarily close its services and pay a huge ransom of $40 million to Obtain the key to decrypt her files and data (Kartikay & William, 2023).

Based on the foregoing, it can be said that cybersecurity is important at the individual level in protecting personal data, files, and bank accounts. At the level of companies and institutions, in protecting electronic assets, data, information, employee data, servers, and websites. At the state level, it protects its electronic security and protects the financial, economic, and military systems from electronic attacks, piracy, and disruption.

3. Representation Of The Cybersecurity Realm

By combining the areas of fundamental research and the relevant sectoral domains with existing applications and technologies in the digital society, a three-dimensional representation of the cybersecurity realm can be obtained, as illustrated in Figure N°01:

Figure N°01: High-level view of the cybersecurity taxonomy.



Source: (Baldini & al, 2020, p. 17)

Cybersecurity is shown as a large, multifaceted discipline rather than a sub-area of computer science. while it is involved everywhere, each cell of this cube requires particular theoretical approaches and specific technical implementation and skills (Baldini & al, 2020, p. 17).

On the other hand, to successfully manage cyber risks, it is very important to constantly evaluate how effective security controls are. the Global Cybersecurity Status Report revealed that 97% of cyber-attacks could be prevented if institutions had effective controls. security controls are applied to detect and/or prevent unwanted events or processes in information systems (unauthorized use, inaccurate data, ineffective processes, wrong algorithms or faulty system inputs, etc.) or problems from the external environment (external attacks, faulty data transmission, natural disasters, etc.) (Spremić & Simunic, 2018, p. 3).

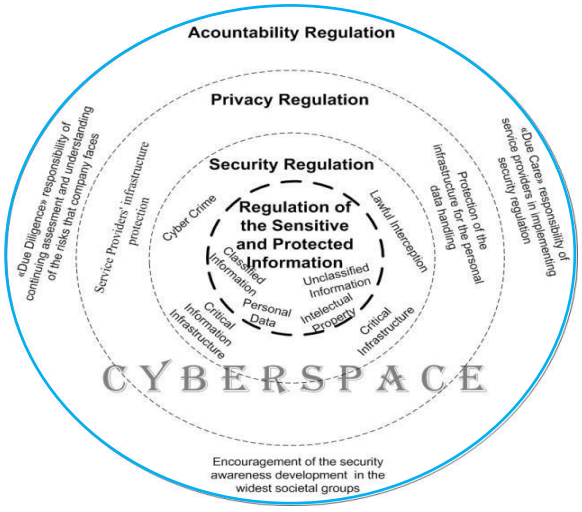
Secondly. Cybersecurity Requirements To Protect The Digital Economy

Cybersecurity is the steps to defend data and information on all electronic devices connected to the Internet from malicious attacks, hacking operations, data theft, and sabotage, accordingly, to counter cybersecurity attacks must provide the requirements listed below:

1. Identification of Organisational Prerequisites

Cybersecurity covers a vast area of society, so the organizational prerequisites are highly complex. These prerequisites are implicitly contained within some parts of the cyberspace regulation framework and can be derived from Figure 4.

Figure N°02: The Cyberspace Regulation Framework.



Source: (Klaic, 2016, p. 43)

The main organizational emphasis in a cybersecurity system should be on the policy planning bodies, not only for the system drafting process but also to harmonize particular sectoral policies with national ones. Equally important is the harmonization of the national policy with different international requirements that can come from many sources (e.g. NATO, EU, and international business sector standards). This is the area mainly covered by the responsibilities of bodies such as National Security Authorities (NSA) and National Regulatory Authorities (NRA), as well as different coordination bodies in areas such as critical infrastructure protection, crisis management, etc (Klaic, 2016, p. 44).

The National Authority responsible for National CERT/CSIRT functionality, together with other similar bodies established throughout all of the societal sectors, represents one of the main points for the successful implementation of a cybersecurity system. Other closely related and important technical bodies are Certificate Authorities (CA) which are generally responsible for the issuance of digital certificates, among others based on the relevant digital signature legislation. This field is further related to the national/international standardization

authorities and other delegated authorities for accreditation and certification processes (Klaic, 2016, p. 44).

Training employees with proper knowledge and following security policies are necessary to prevent accidental insider attacks. Recruiting cyber analysts can help not only in identifying threats but also in the incident response process. For investigating the incident and implementing countermeasures to prevent attacks, system security professionals are important (Dummanaboyina, 2024, p. 2).

Moreover, Other necessary authorities that should be identified for coordination and management come from functional areas such as cybercrime, cyberterrorism, or cyber defense. the responsible bodies for such functional areas should be clearly defined to allow two-way communication with other responsible bodies defined within a national cybersecurity system framework. In addition, should be defined the authorities are responsible for evaluating the cybersecurity system, (eg the National Cybersecurity Council).

2. Identify the Elements of Cybersecurity

There are key elements of cybersecurity, explained below:

2.1 Application security:

Applications play an essential role in business ventures; that is why every firm needs to focus on web application security. Having a secure web application is required to protect customers, their interests, and their assets. Web application weaknesses or vulnerabilities a common points of interference for a cyber thief (Roohparvar, 2019).

2.2 **Information Security**:

Information security is a collection of strategies for managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and non-digital information (Jitendra & Parashu, 2017, p. 791).

2.3 **Email Security**:

Email gateways are the number one source of security breach threats. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send

them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data (Jitendra & Parashu, 2017, p. 791).

2.4 Network Security:

Network security consists of protecting the usability and reliability of networks and data (Roohparvar, 2019).

2.5 Leadership commitment:

To have a successful cybersecurity project, it is vital to have leadership commitment. Without having the leadership in the team it is complicated to develop, implement, and maintain the processes. The top leaders or management teams of an organization should invest in cybersecurity measures to make it useful and successful. With the support of leadership for cybersecurity, an organization can improve investment in technology, resources, and skills (Roohparvar, 2019).

2.6 End-User Security:

End-user security is also known as end-point security. This is about protecting the devices that users work with and the users themselves. End-user security is vital because 91% of cyberattacks begin with a phishing email (Dynamix Solutions, 2024).

Focusing on the aforementioned elements of cybersecurity is very important in facing cyber threats, but the most difficult challenge in cybersecurity is that security risks are constantly evolving and changing faster than companies respond.

3. Providing Cybersecurity Techniques

There are many cybersecurity techniques to fight cybersecurity attacks. The next section discusses some of the suitable techniques used to maintain a security system stronger as follows: (Dummanaboyina, 2024, p. 4)

3.1 Firewall: For a system or an organization, firewalls act as the first layer of security. A firewall is used to block junk files or unauthorized packets entering from the network. This can be hardware or in-built software. Though the function of a firewall is inspecting and filtering packets, setting up suitable configurations

matters. Firewalls with incorrect configurations can be bypassed by changing the file pattern.

3.2 Honeypots: In recent years honeypots have been developed as a security alarm that helps the admin or security analyst in finding the intruder. These are used to deflect the hacker to a different path and prevent the information. Though using this technology attack can be prevented in the initial stage, false alarms can occur with improper configurations.

3.3 User credentials: For computer or web applications accessing entering users, credentials are the first step for authentication and authorization purposes. The usual way of accessing is by entering a username and password which specifies the uniqueness of every user. These can be stolen by the hacker to pretend like the user. This is known as a social engineering attack. This problem can be overcome with the latest solution, a one-time password (OTP). This is a unique password sent to the mobile or email. This is also known as 3-way authentication.

3.4 Access control lists: Maintaining ACL(Access control list) for accessing files depending on their sensitivity is trending with the growing cyber threats. ACL creates a specific list of people with privileges to access files or directories or to block a specific group of people. This is mostly used in organizations to secure highly confidential files from insiders. The list usually depends on the role and criteria of the employee.

3.5 Malware scanners : This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, Trojan horses, and worms are examples of malicious software that are often grouped and referred to as malware (Nikhita & Ugander, 2014, p. 5).

3.6 Changing to IP6 version: Internet protocol version 4, popularly known as IPV4 has been the backbone of the internet by connecting a large number of devices. Now IPV6 is changing the trend by replacing IPV4 with IPV6 which supports more number connective devices with better security capabilities. Implementing IPV6 technology can reduce the number of attacks not only in private lives but also in large-scale IT industries (Dummanaboyina, 2024, p. 3).

3.7 Encryption of the code: Encryption is the process of encrypting data in such a way that hackers cannot read it, using an encryption algorithm, and converting it into unreadable ciphertext. Encryption at the very beginning level protects data privacy and its integrity.

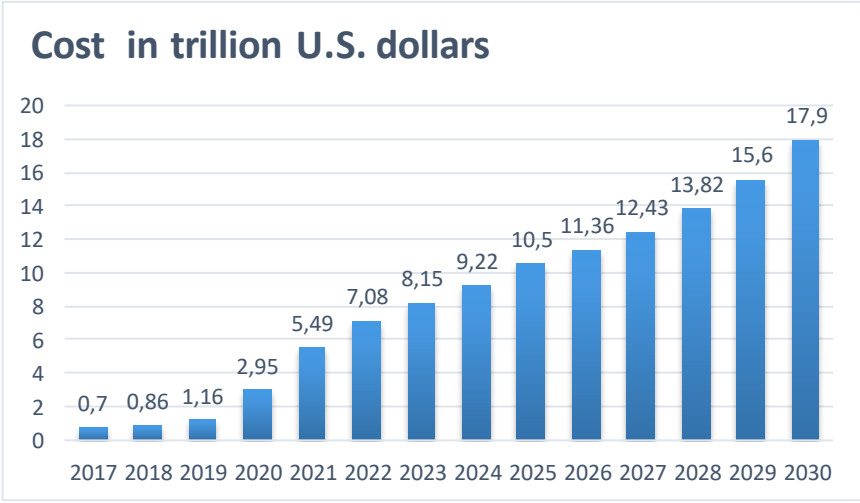
But more use of encryption brings more challenges to cybersecurity (Nikhita & Ugander, 2014, p. 3).

These aforementioned techniques are very important in facing cyberattacks and protecting governments, institutions, and individuals.

Thirdly. The impact of Cybersecurity Threats on the Digital Economy

The digital economy was valued at $14.5 trillion in 2021, but the estimated global cost of cybercrime was $6 trillion – or 41% of the digital economy. By 2025, the digital economy will be worth $20.8 trillion, but cybercrime will reach $10.5 trillion, to rise to $13.8 in 2028. (Hayat, 2024).

Figuer N°03: Estimated annual cost of cybercrime globally.



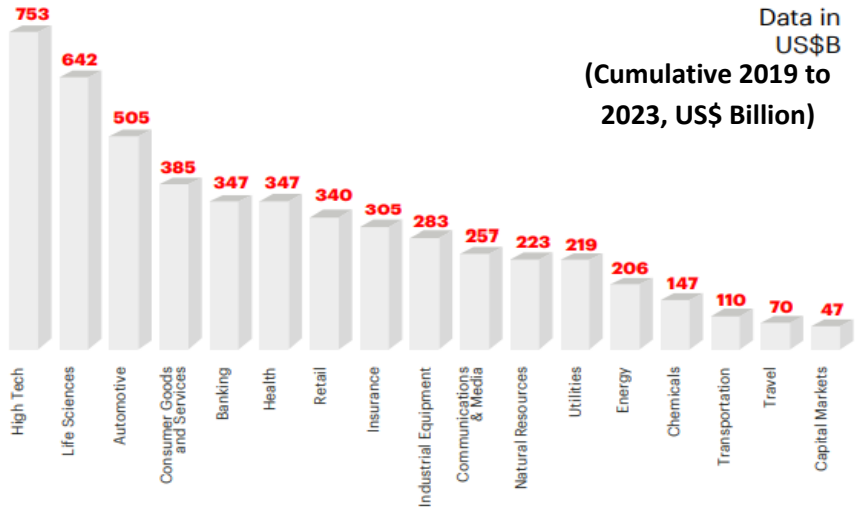
Source : (Petrosyan, 2024)

The previous figure shows the rise in the cost of cybercrime each year. The cost of cybercrime was estimated in 2024 at about 9,22 trillion US dollars, and this number is expected to rise next year to 10.5 trillion US dollars. and the growth of artificial intelligence technology is likely to lead to a rise This cost will reach 17.9 trillion US dollars by 2030.

Due to cyber attacks, companies risk losing an estimated US$5.2 trillion in value-creation opportunities from the digital economy in the next five years. High-tech industries face the highest risks (Omar &

Kelly, 2019, p. 16). The following figure shows the value at risk* by industry - direct and indirect attacks:

Figuer N°04 : Value at Risk* by Industry—Direct and Indirect Attacks.



Source : (Omar & Kelly, 2019, p. 16)**.**

The earlier figure shows that some industries are more vulnerable to cyber attacks than others, simply because of the nature of their business. While any industry can experience a data breach, those most at risk are companies that are closely involved in people's daily lives, which is why higher education institutions are the most vulnerable to cyber-attacks.

Moreover, Small and Medium Enterprises (SMEs) are prime targets for cyberattacks, as SMEs lack the budget, expertise, and technical capacity to implement effective cybersecurity measures. Worryingly, many SMEs are subcontractors to large organizations, Thus often electronically linked to the IT systems of some of the larger partner companies, they become ideal entry points for larger companies and are therefore at high risk of cyberattacks (Yadav & Gour, 2014, p. 39).

Fourthly. The reality of cybersecurity in Algeria

In this part, we will present the cyber security index in Algeria and the number of cyber-attacks it is exposed to.

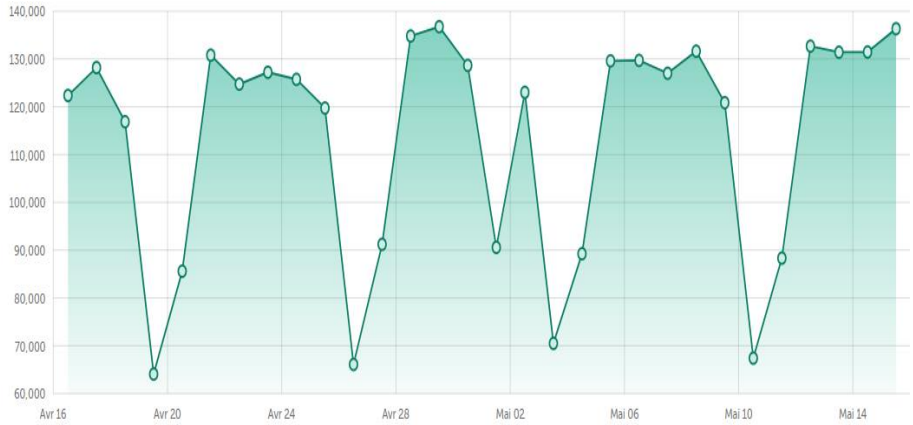
1. The level of cyber attacks in Algeria

Cybercrime is considered one of the major challenges facing Algerian society in light of technological and digital developments and economic, social, and cultural transformations. Kaspersky ranked Algeria first in

the Arab world and 14th in the world in terms of countries most vulnerable to cyber attacks in 2018. (Bashush, 2024)

In 2022, Trend Micro Incorporated, the global leader in cybersecurity, blocked more than 29.7 million threats in Algeria. The company has detected and blocked over 19 million (19,552,217) email threats, over 400,000 (417,156) malicious URL attacks, and 34,023 URL hosts. Over half a million (508,815) malware attacks were identified and stopped (TrendMicro, 2024). Despite this, the Algerian National Gendarmerie recorded 4,600 cybercrimes in 2022. The Algerian security services also recorded a record rise in cybercrimes to 14,000 crimes in 2023, including 500 crimes in the first month of the year (Bashouch, 2024). According to Kaspersky statistics, 140.000 cyber attacks were recorded daily in January 2024 (Securelist, 2024). The following figure shows statistics about the threats detected against computer users in Algeria during April and May 2024.

Figure N°05: Statistics about threats detected on users' computers.



Source : (Securelist, 2024)

The previous figure shows the daily number of cyber attacks in Algeria during April and May, ranging between 136.877 and 64.182 attacks after a slight decrease from February when attacks ranged between 140,000 and 60,000 attacks. The reasons for these attacks are due to blackmail, defamation, piracy, and the dissemination of misleading and false information, in addition to the sale of unlicensed goods over the Internet, attacks on intellectual property rights, etc.

2. Ranking of Algeria according to the level of cyber threats

To assess the number of cyber attacks to which users in different countries are exposed, Kaspersky calculated the percentage of Kaspersky users who had web antivirus software running on their computers during 2023(Kaspersky lab, 2023, p. 16). The following table shows the countries in which users encountered cyber threats:

Table N°01 : Ranking of countries where users face the greatest risk of exposure to cyber threats.

	Country	%
1	Taiwan	24.41
2	Greece	24.12
3	Belarus	22.65
4	Algeria	22.64
5	Turkey	22.54
6	Serbia	22.09
7	Tunisia	21.17
8	Moldova	21.10
9	Nepal	20.99
10	Bangladesh	20.81

Source : (Kaspersky lab, 2023, p. 16).

We note from the previous table that Taiwan occupies first place, then Greece and Belarus, and Algeria occupies fourth place in terms of the number of users exposed to cyber attacks.

Moreover, Algeria is considered the weakest country in terms of confronting cyber attacks and is ranked last on the list of information security in the world, according to what was revealed by the classification compiled by the “Comparitech” website (Bischoff, 2024). The following Table shows the types of cyber threats to which Algeria is exposed :

Table N°02 : Types of cyber threats in Algeria.

	cyber threats	%
1	% of computers facing at least one *local* malware attack	31.85
2	% of mobiles infected with malware	21.97
3	% of computers attacked by phishing (Yearly)	16.38
4	% of computers infected by at least one malware attack (web-based)	6.22
5	% of mobile users attacked via web sources	4.27
6	% of attacks by cryptominers	0.77
7	% share of users attacked by banking malware (non-mobile)	0.40
8	% share of countries targeted by malicious mailings (Yearly)	0.40
9	% of users attacked by ransomware trojans (non-mobile)	0.33
10	% of all spam emails by originating country (Yearly)	0.05
11	% of SSH-based attacks by originating country (IoT)	0.04
12	% of users attacked by mobile ransomware trojans	0.03

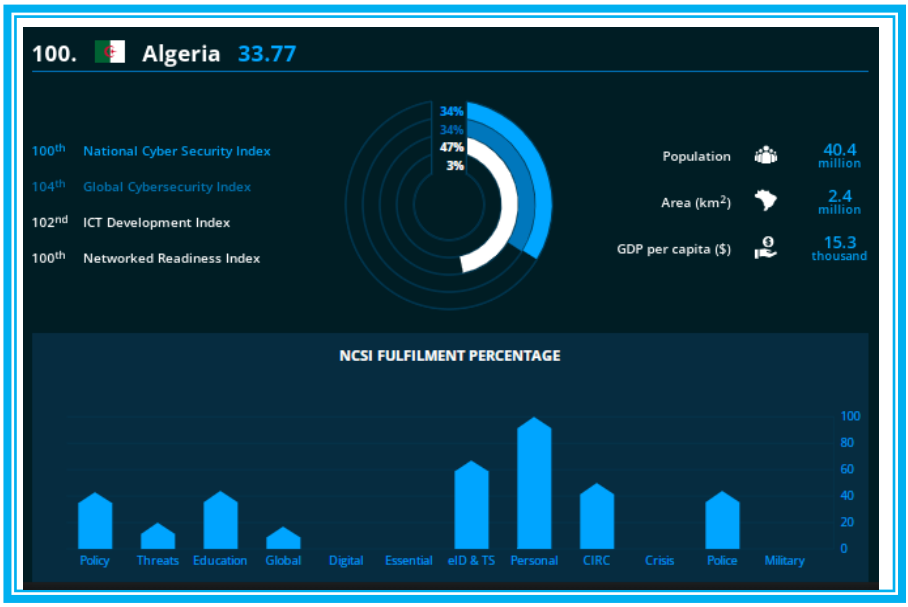
Source: (Bischoff, 2024).

Algeria is considered the least safe online country overall, being the highest-rated country in terms of lack of legislation and rates of computer malware, and also obtained a high score in the mobile malware categories at 27.97%, and the local computer malware categories at 31.85%.

3. Cybersecurity index in Algeria.

There are many indicators to measure the level of cybersecurity, the most important of which is the National Cybersecurity Index (NCSI), developed by the Academy of Electronic Governance, which measures the level of cybersecurity in countries and identifies the main priority areas that must be addressed to improve the state of cybersecurity. The index also provides an overview of countries' readiness to prevent and combat cybercrime and attacks. Analyzing these areas helps governments identify gaps in policies and strategies that should be addressed to improve the country's cyber security.

Figure N°06: Cybersecurity Indices in Algeria 2023.



Source : (e-Governance Academy, 2024).

According to the National Cybersecurity Index (NCSI), Algeria ranked 100th with an index of 33.77%. It is a late rank compared to the human and material capabilities that Algeria possesses, and to strengthen its capabilities in this field and rectify the shortcomings and gaps involved in giving utmost importance to this issue, because of its clear and dangerous impact on its economy and national security.

4. Algerian efforts made to achieve cybersecurity.

Algeria has enacted a set of laws and regulations and created bodies that regulate activities related to information technology or cybersecurity.

4. 1. The legal and legislative aspects :

Algeria issued a set of laws to protect cyberspace, the most important of which are (Zamora & Ben Issa, 2022) :

- Decree No. 09-410 of 10 December 2009 laying down the safety rules applicable to activities relating to sensitive equipment.
- The Arab Convention on Combating Information Technology Crimes, drawn up in Cairo on December 21, 2010, was ratified by Presidential Decree No. 14-252 of September 8, 2014.
- Law No. 18-07 of June 10, 2010, relates to the protection of natural persons in the field of processing data of a personal nature:

This law aims to define the rules for the protection of natural persons in the field of processing data of a personal nature.

- Law No. 18-05 of 24 Chaâbane 1439 corresponding to May 10, 2018 relating to electronic commerce (Commerce Ministry, 2024).
- Law No. 05-22 of 27/09/2022 contains special rules for combating cybercrime. (ARPCE, 2024).

4. 2. Structural and institutional aspect : The most important bodies established by Algeria in the field of cybersecurity are (Zamora & Ben Issa, 2022) **:**

- Central Authority for Combating Information Crime.
- Cyber Defense and Systems Security Monitoring Service
- Establishing the first cybersecurity center affiliated with Algeria Telecom
- Establishing a national pole specialized in combating cybercrime.

4. 3. Administrative and organizational aspect : (APS, 2024)

- The National Authority for the Prevention and Combat of Crimes Related to Information and Communication Technologies.
- The National Defense Service and the Popular Systems Security Monitoring Service.
- Establishing the first cybersecurity center affiliated with Algeria Telecom.

Despite Algeria's great efforts to achieve cybersecurity and protect its economy, it has not yet reached the level of its neighbors Morocco and Tunisia.

Conclusion:

A trustworthy digital economy is critical to the growth of organizations in the future, and this can only be achieved by strengthening cybersecurity. Algeria needs to be prepared, more than ever, to protect its national security, sovereignty, and economy. By making cybersecurity an essential factor in protecting the digital economy and society. This study reached the following results:

- Cybercrime costs US$ 9.22 trillion in 2024, and this number is expected to rise to US$17.9 trillion by 2030.
- Businesses risk missing out on an estimated $5.2 trillion in value-creation opportunities from the digital economy in the next five years.
- Higher education institutions are the most vulnerable to Cyber attacks because they possess data of an important part of society.

- SMEs are prime targets for cyber attacks, as they lack the budget, expertise, and technical capacity to implement effective cybersecurity measures.
- According to the National Cybersecurity Index (NCSI), Algeria ranked 100th with an index of 33.77%.
- Algeria expos to between 140,000 and 60,000 cyber attacks daily beginning in 2024.
- The most important cybercrimes to which Algeria is exposed are blackmail, defamation, hacking, and spreading misleading and false information.
- To enhance cybersecurity, Algeria has enacted a set of laws and legislative regulations.
- It has established several bodies in the field of cybersecurity, the most important of which is the Center for Systems Security Monitoring and Cyber Defense, and a national center specialized in combating cybercrime.

This study recommends the government Focus on improving information security systems, providing high-tech technology for cybersecurity purposes, and building human resources capabilities in this field, in addition to developing the judicial and security system and bringing it in line with. Furthermore, you should focus on the following: Improving the general public's digital literacy.

- Supporting small institutions in their digital transformation.
- Securing critical infrastructure and governmental networks.
- Keeping up with a changing technological environment.
- effective protection of information systems against cyber-attacks.
- develop and implement policies on preventive measures against cyber-attacks.
- conduct an annual cybersecurity audit to identify risks.
- Opening university majors in the field of cybersecurity.
- Encouraging cooperation between the public and private sectors in the field of cybersecurity.
- Encouraging research and development of cybersecurity.
- Strengthening international cooperation in the field of cybersecurity.

Références :

1. APS. (2024, 03 02). ***A presidential decree determines the composition of the National Authority for the Prevention of Crimes*** Related to Information and Communication

Technologies. Récupéré sur ALGERIA PRESS SERVICE: https://www.aps.dz/ar/algerie/72990-2019-06-26-12-48-47

2. ARPCE. (2024, 02 27). ***Law No. 09-04 of Shaaban 14, 1430, corresponding to August 5, 2000***. Récupéré sur Control authority: https://www.arpce.dz/ar/pub/l9d1a8
3. Babayo, S., & al. (2021). ***Cybersecurity And Cybercrime In Nigeria: The Implications On National Security And Digital Economy.*** Journal Of Intelligence And Cyber Security, Vol.04, No.01.
4. Bakri, M., & al. (2019). ***Cybersecurity And Digital Economy In Malaysia: Trusted Law For Customer And Enterprise Protection***. International Journal Of Innovative Technology And Exploring Engineering,Vol.8, No.8.
5. Baldini, G., & al. (2020). ***Cybersecurity Our Digital Anchor A European Perspective***. European Commission: Publications Office of the European Union.
6. Bashouch, N. (2024, 02 28). ***14,000 cybercrimes in 2023, and online shopping is at the forefront***. Récupéré sur echorouk: https://www.echoroukonline.com/14-
7. Bashush, N. (2024, 01 28). ***Cybercrime.. Terrifying numbers***. Récupéré sur Shorouk: https://www.echoroukonline.com
8. Bischoff, P. (2024, 02 28). ***Which countries have the worst (and best) cybersecurity? Global rankings***. Récupéré sur Comparitech Limited: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/
9. Commerce Ministry. (2024, 02 28). ***Law No. 18-05***. Récupéré sur Ministry of Trade and Export Promotion: https://translate.google.com/?hl=fr&sl=ar&tl=en&text=%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%B1%D9%82%D9%80%D9%80%D9%85%2018-05&op=translate
10. Craigen, D., & al. (2014). ***Defining Cybersecurity***. Technology Innovation Management Review, Vol.04, No.01.
11. Dummanaboyina, C. (2024, 02 10). ***Cyber security and its importance.*** Récupéré sur ResearchGate: https://www.researchgate.net/publication/347439655_CYBER_SECURITY_AND_ITS_IMPORTANCE
12. Dynamix Solutions, I. (2024, 01 25). ***What Are The Elements Of Cybersecurity And How Does It Work***. Récupéré sur Dynamix Solutions Inc: Https://Dynamixsolutions.Com/Elements-Of-Cybersecurity/

13. Hayat, Z. (2024, 01 15). **Digital trust: How to unleash the trillion-dollar opportunity for our global economy.** Récupéré sur World Economic Forum: https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/
14. Jitendra, J., & Parashu, R. (2017). ***A Recent Study Over Cyber Security And Its Elements.*** *International Journal Of Advanced Research In Computer Science, Vol.8, ume 8, No.3*.
15. Kartikay, M., & William, T. (2023, 3 3). ***CNA Financial Paid $40 Million in Ransom After March Cyberattack.*** Récupéré sur Bloomberg: https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack#xj4y7vzkg
16. Klaic, A. (2016). ***A Method For The Development Of Cyber Security Strategies.*** *Information & Security: An International Journal, Vol.34, No.1* .
17. Leahovcenco, A. (2021). ***Cybersecurity as a Fundamental Element of The Digital Economy***. *Mest Journal Vol.09 No.01*.
18. Luiijf , E., & al. (2013). ***Nineteen national cyber security strategies***. *Int. J. Critical Infrastructures, Vol.09, No.01*.
19. Lehto, M. (2013). ***The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies***. International Journal of Cyber Warfare and Terrorism, *Vol.03, No.03*.
20. *Nikhita , R., & Ugander, R. (2014).* ***A Study Of Cyber Security Challenges And Its Emergning Trends On Latest Technologies***. *International Journal Of Engineering And Technology, Vol. 4, No.1*.
21. Omar, A., & Kelly, B. (2019). ***Securing The Digital EconomyReinventing the Internet for Trust***. USA: Accenture.
22. Petrosyan, A. (2024, 02 09). ***Estimated cost of cybercrime worldwide 2017-2028***. Récupéré sur statista: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
23. Rajesh, K. (2015). ***Importance of Cyber Security. International Journal of Computer Applications****,Vol.111, No.07*.
24. Roohparvar, R. (2019, march). ***Elements of cybersecurity***. Récupéré sur INFOGUARD CYBER SECURITY: https://www.infoguardsecurity.com/elements-of-cybersecurity/
25. Securelist. (2024, 03 02). ***Democratic and People's Republic of Algeria***. Récupéré sur kaspersky:

https://statistics.securelist.com/fr/country/algeria/on-access-scan/month

26. Singh, R. (2021). **A Review On Cyber Security**. *International Journal Of Advance And Innovative Research,Vol.8, No.2*.
27. Spremić, M., & Simunic, A. (2018). ***Cyber Security Challenges In Digital Economy***. Proceedings Of The World Congress On Engineering, Vol.1,No.1.
28. TrendMicro. (2024, 02 28). ***Trend Micro Blocked over 29.7 Million Threats in Algeria:*** Reveals Annual Cybersecurity Report. Récupéré sur Trend Micro: https://www.trendmicro.com/en_ae/about/newsroom/press-releases/2023/05-06-2023.html
29. Yadav, H., & Gour, S. (2014). C***yber Attacks: An impact on Economy to an organization.*** International Journal of Information & Computation Technology, Vol. 4, No. 9.
30. Zamora, J., & Ben Issa, L. (2022). ***Importance of cybersecurity governance for ensuring a secure digital.*** Journal of Advanced Economic Research: Vol. 07,No. 02.