

Cybersecurity as a Tool for Strengthening Digital Sovereignty: Challenges and Prospects

Abderrahim Lahreche *

Laboratory of Law and Society in the Digital Space –

University of Ghardaia

lahreche.abderrahim@univ-ghardaia.edu.dz



Date of submission: 19/04/2026

- Date of acceptance: 30/05/2026

- Date of publication: 05/06/2026

ABSTRACT:

The present research focuses on the issues of cybersecurity and digital sovereignty within the framework of threats emerging in cyberspace, namely, cyber war, cybercrime, and cyberespionage. It draws attention to an expansion of the notion of security, which encompasses not only such aspects as military, economic, social, political, and legal but also informational. The focus is made on the significance of cybersecurity in terms of protection of the digital space, with particular emphasis being put on the need for a well-developed system of measures.

Key words: Cybersecurity; Digital Sovereignty; Cybercrime; Cyber Attacks, Cyberespionage.

Introduction:

Cybersecurity is not anymore a matter only for experts in information technology. It is a very significant issue in our time and affects everything in it. With the development of technology, the need to protect it against the many different threats it is subject to becomes increasingly important. Cybersecurity is not anymore something that involves only the protection of sensitive information; it has to do with the security and freedom of individuals. The targeted cyberattack can threaten the life of humans since it can take place in critical infrastructure sites, like hospitals or power plants. Furthermore, these attacks can be used to infringe on people's privacy and restrict their freedom of expression. The current interconnectedness of the digital world exposes all parts of modern life to cybersecurity threats, including the use of

* - Author Correspondent:

the Internet of Things, cloud computing, and the spread of false information via social media sites, along with the exposure of sensitive infrastructure. That being said, the necessity of cybersecurity cannot be questioned.

Moreover, cyberspace has been an important part of contemporary warfare that now poses threats to the national security of countries while causing heavy losses to the world economy. Such warfare has the potential to undermine states' cybersecurity through the various fields, including semiconductors manufacturing, digital industry, communication, information warfare, and cyber espionage. The emergence of such a geopolitical trend has enabled the utilization of information technology and cyberspace in political, military, economic, security, and social spheres in the pursuit of new generations of warfare, which has led to the emergence of new generations of warfare and its consequences on national security. These include fourth-generation warfare, amongst others, and how security and intelligence agencies respond to changes introduced by these new developments.

There are different types of cyber-attacks such as phishing, where attackers use fake websites to get sensitive data from victims. Other forms of attacks include malware attacks to infect computers, denial of service attacks which affect electronic services, and ransomware which is meant to extort the victim. All these forms of cyberattacks affect individuals, corporations and governments as well. Some effects of cyberattacks include financial losses as a result of data loss and service interruption, government loss caused by attacks on vital infrastructure, reputation losses for companies, loss of customers' trust in companies, loss of vital data and the exploitation of the stolen data for criminal and political gains, and threats to human life by disrupting essential services. As a result, there is now an urgent need to address cybersecurity in terms of the protection of digital resources, continuity of operations, and social stability amidst increasing dangers. In consideration of this situation, the following issues will be explored in the current study: What do the concepts of cybersecurity and digital sovereignty mean? What are their different aspects? What are the different kinds of cyber-attacks and methods used for intruding?

Importance of the Research

The importance of this research is related to the study of cybersecurity and digital sovereignty, as well as emphasizing the prominent role that cybersecurity must play in securing the digital world against increasingly complex cyber-attacks.

The aim of the research is also to shed light on the dangers associated with cyber-attacks and encourage actions toward increasing digital security as a national priority.

Objectives of the Research

This research will seek to:

- Define the broad term cybersecurity and digital sovereignty and identify their different facets.

- Categorize different types of cyberattacks and cyber threats.
- Examine the effect of these attacks on people, organizations, and countries.

KEY CONCEPTS

The word cyber comes from the Greek language where it means governance or control in the sense of guidance and control taken from a Greek word for one who steers a ship. Cyber can thus be interpreted as meaning remote governance or control. The suffix added to the word makes cyber mean the governance or control of that particular field, such as cybersecurity.

In relation to security, the word is antonymous with fear and means safety and protection. Security becomes an issue because of the development of technology and internet usage. Many crimes are committed in relation to cyber space, targeting information system or sensitive data. These crimes cross national borders and therefore are a danger to the information security of countries.

First Requirement: Definition of Digital Security

The Algerian legislature defines digital security as "the totality of solutions, methods, security, processes, principles, risks management techniques, measures, education, best practices, protections and technologies which may be used to secure electronic communication from any act which may undermine the availability or integrity of any stored, processed or transmitted data"¹.

It further includes all measures needed to secure information in all forms of presentation—both tangible and intangible—against several types of dangers such as cybercrime, sabotage, espionage, and accidental events. At the same time, the European Cybersecurity Declaration describes digital security as the capability of the information system to resist attacks, including data theft².

Second Requirement: Definition of Cyberspace

Frédéric Mayor defines cyberspace as a new environment of expression, information, and exchange created by people and technology. The main component of this definition is made up of people belonging to different countries, cultures, languages, ages, and occupations, who have a connection through communication technology that allows the transfer of information in digital format.

¹ Suleiman Kattaf, Abdelhalim Boutarine, Cybersecurity and Its Associated Conceptual Dimensions, Journal of Tebna for Scientific and Academic Studies, Algeria, Vol. 5, No. 2, 2022, p. 41.

² Hazem Dahhan, Nasser Al-Quraiti, Cybersecurity and Information Security Protection, Dar Al-Fikr Al-Jami'i, Alexandria, 2021, p. 7.

Thus, the word "cyber" becomes one of the most common terms used to describe the information era when used together with "space." This phenomenon has come to mean something that goes beyond the Internet as it involves all communications, networks, and databases. The idea also means the total set of information that is transmitted and organized as systems based on its uses¹.

Third Requirement: Cyber Threat

A cyber threat is another relatively recent concept that has emerged alongside cybercrime and refers to criminal activity and occurrences that are uniquely dependent on information technologies and computers². Moreover, the concept of cyber has been used to refer to electronic security, and consequently, a new term – cybersecurity – was born³.

The U.S. Strategic Command has defined a cyber threat as the operation of computer systems in order to render them useless to the adversaries, along with the intrusion into information systems and communication networks for the collection, acquisition, and analysis of information contained therein⁴. However, in a general sense, a cyber threat may be defined as any kind of attack performed over Internet networks and computer systems, which can cause damage to equipment and Internet-connected electronic networks⁵.

Third Requirement: Cybercrime

The concept of cybercrime was developed by Susan & Haston (1995). According to these researchers, cybercrime does not have an all-embracing definition because cybercrime should be viewed as an act or behavior that is performed in terms of the materiality of the act as well as the means utilized, notably in cases where computerized data or system is affected. In this regard, cybercrime consists of criminal offenses whereby computer or information system can either be the means, the object, or both in relation to the criminal offense. The use of the compound term "cybercrime" is synonymous with term like "computer crime," "electronic crime," "high-technology crime," "information-age crime," and "digital crime."⁶

¹ Mohamed Messika, Cyberspace and the Challenges of National Security of States, Journal of Legal and Social Sciences, Algeria, Vol. 7, No. 4, 2022, p. 454.

² Mohamed Karziz, Meriem Yahiaoui, The Virtual Environment and Education, Journal of Research and Studies, Algeria, No. 6, 2008, p. 238.

³ Mohamed El-Said Bouflih, Frameworks of International Cooperation to Address Cyber Threats, Journal of Applied Legal Studies, 2024, p. 3.

⁴ Abdellah Jaafari, Cyber Threats and Their Impact on Algerian National Security, African Journal of Legal and Political Studies, Vol. 6, No. 2, 2022, p. 247.

⁵ Abdelghani Chergui, Cyber Threats and the Problem of Sovereignty, Journal of Global Politics, Vol. 7, No. 2, 2023, p. 275.

⁶ Amina Bessafa, Legal Frameworks of Cybercrime in Algerian Legislation between Prevention and Enforcement, Annals of the University of Algiers 1, Vol. 37, No. 1, 2023, p. 101.

ASPECTS OF DIGITAL SECURITY

The field of cybersecurity contains numerous dimensions that not only include technical issues but also cover the military, economic, political, societal, and legal dimensions. As such, it becomes essential to take steps in order to guarantee the safety of the information from the perspective of confidentiality, integrity, and availability. Among the essential elements of information security is the formulation of proper policies and procedures as an element of the security strategy which is the backbone of the information security. The formulation of the policy offers a clear indication of the steps to be taken for the sake of protecting the information as well as the people who work with the information. For the successful implementation of information security, the policy should be enforced and supported by the entire organization.

First Requirement: The Military Aspect

This aspect copes with matters related to military defense, especially in terms of ensuring the safety of the computer networks used by the military forces. To attain this crucial part of cybersecurity, there must be strategies and capabilities for identifying any possible cyber-attack threats, as well as being ready to deal with them via technological advancement.

Second Requirement: The Political Aspect

The political aspect is anchored on the protection of the political system and the state. The release of classified documents will have dire ramifications, not only domestically but internationally, as well.

Third Requirement: The Economic Aspect

In view of the fact that knowledge plays a pivotal role in the contemporary economy and both are highly interconnected, the significance of cybersecurity in terms of protecting the economic interests of states becomes apparent. The digital economy, combined with the utilization of ICTs for conducting different economic and financial transactions, is seen as an important factor that contributes to economic development. Thus, it is crucial to provide security of this kind of information as it can be considered to be national wealth.

Fourth Requirement: The Social Aspect

The social aspect of cybersecurity is associated with the necessity to achieve the right balance between individual privacy and security. Firstly, there is a need to protect people's personal information, and secondly, it is important to provide cybersecurity and protect against any cyber threats. Cybersecurity is facilitated through the education of people about cyber risks, and at the same time, it provides protection from cybercrime conducted by networks of criminals online.

Fifth Requirement: The Legal Aspect

This aspect pertains to the rules and regulations designed for protecting and safeguarding digital information and data against any form of cyber-attacks. It is concerned not only with the safety of digital information but also the protection of the individual rights and corporate rights in relation to such things like privacy and intellectual property issues¹.

DIGITAL INVESTIGATIONS AND INFORMATION GATHERING TECHNIQUES

Efforts geared towards creation of a safe electronic environment for important and sensitive information systems regarding state infrastructure can only bear fruits through cooperation and collaboration that goes beyond any national approach alone. Only through this can the problem of cybersecurity of the information system be addressed effectively within international and regional forums².

First Requirement: Sources of Information Gathering

Without information gathering from different digital and electronic sources, cyber intelligence can hardly become a reality. Due to the fast pace of development in information technology as well as different uses of this technology, computers, mobile phones, as well as other types of portable gadgets have become common place resulting in internet-enabled devices.

The development in information technology has also been responsible for the dramatic increase in internet users, which today is in excess of 4.6 billion people. In the Middle East region, Hacking rates have continued to grow daily in most Arab countries, even exceeding the international average growth rate.

The aforementioned data demonstrates that a large number of data is produced by this substantial number of users. As most of this data is found in open sources, it is considered an invaluable source for conducting intelligence work and operations in terms of security issues. It can include criminal investigation on both traditional crime and cybercrimes in which the evidence might be gathered within cyberspace; in addition, it includes counter terrorism where terrorist acts might be carried out in

¹ Sara Yakhouch, Artificial Intelligence and Cybersecurity (Functions and Challenges), Algerian Journal of Social and Human Sciences, Vol. 9, No. 1, 2025, pp. 142–143.

² Hiba Gamal El-Din, The State and Its National Security in the Age of Artificial Intelligence and Its Intersections, Dar Al-Maaref, Egypt, 2023, p. 71.

cyberspace in terms of communication between terrorists and using the Internet for their activities¹.

Nonetheless, such data needs systematic gathering and analysis in order to have value in either discovering crime or investigating crimes. Generally, information in cyberspace in terms of intelligence can be divided into two categories according to the sources of information, namely closed and open sources.

Second Requirement: Open Sources and the Internet

There have been various sources through which information could be retrieved with the advent of the Internet; nonetheless, such sources would only prove to be valuable once the information was analyzed and used to obtain intelligence information that could help achieve some intended purpose. There are various reasons for which security agencies have understood the importance of gathering information through the Internet, as enumerated below²:

- The use of the Internet by terrorists' organizations;
- The increasing incidence of cybercrimes;
- Conflict between religions and political parties;
- Use of internet-enabled gadgets;
- Security vulnerabilities in communication infrastructures;
- Growing cyberattacks.

Open-source intelligence has proved useful in discovering the background of criminal activities through the systematic investigation and analysis of sources, including the Internet and social media.

Third Requirement: Studies Conducted on Social Networking Sites

Social media networks represent one of the most valuable open sources when it comes to gathering information on people and their different interests. Many tools, both free and paid, have been created to gather information from these sites and determine connections between people, assess their interests, or view images. Such

¹ Mohamed El-Gendy, *Cybersecurity: From Information Warfare to Cybercrime*, Dar Al-Maaref, Egypt, 2024, p. 73.

² Awad Mofeed Hassan Ali, *Cybersecurity and Its Fundamentals*, Publishing and Distribution, Sultanate of Oman, 2025, p. 40.

software can also help in predicting some events, including planning of attacks or riots in a particular area¹.

The extensive usage of the social networking sites like Facebook and Twitter has resulted in more crimes being committed through these sites. The fact of the matter is that this trend also offers an excellent chance to the security authorities, which allows them to gather and study all sorts of information that is available through these sources without having to employ any other technique or even getting judicial approval as long as the information is publicly available.

Social networking sites can also be seen as a reflection of the actual situation prevailing in life. Due to the highly social nature of such media sites, they have always had the capacity to exhibit many social and psychological issues that include not only glorifying some actions but also encouraging criminal actions that may threaten public safety and state security².

Fourth Requirement: Intelligence Gathered from Mapping Databases and Satellite Imagery

There exist many open-source databases on the Internet; some of which are free while others will require a payment or subscription. The resources in such open sources include information on geographic locations, mobile network towers' investigation, temporal satellite images of the geographic area, and information on wireless communication networks in the targeted geographic region.

The essential mapping technologies used in intelligence gathering and investigations are Google Maps, Google Earth, Bing Maps, and Google Street Views. Through comparing the different mapping technologies, investigators will be able to collect valuable intelligence regarding geographic regions, such as drawing the boundary lines of the area or determining the point where the particular photo or video was taken³.

THE CHALLENGES FACED IN THE IMPLEMENTATION OF DIGITALIZATION IN ALGERIA

In an era where nations heavily depend on the cyberspace for service delivery to its citizens, through broad Internet connections which ensure the realization of all-round development, the nation's dependency exposes it to many risks, including non-conventional threats that attack the data of the nation and result in paralyzing its operations.

¹ Abbas Mostafa Sadiq, *New Media: Concepts, Tools, and Applications*, Dar Al-Shorouk, Cairo, Egypt, 2008, p. 218.

² Abdulrahman bin Ibrahim Al-Shaer, *Social Media and Human Behavior*, Dar Safaa for Publishing and Distribution, Amman, Jordan, 2015, p. 67.

³ Mohamed El-Gendy, *op. cit.*, p. 102.

Algeria is no exception to such a reality, as the country faces challenges due to the policies put forward by the government in different sectors, notably embracing the use of e-governance as a strategy to cut down on bureaucracy, provide quality administrative services, and encourage development by ensuring the proximity of the public administration to the citizenry. This strategic move has been hindered by many factors, mainly considering the increasing number of vulnerabilities posed by cyber intrusions or propaganda which could destabilize the society. It has, therefore, led to the identification of some challenges facing Algeria in the cyberspace domain.

First Requirement: Administrative and Technical Difficulties

The following have been attempted through research to categorize administrative problems facing the adoption of digitalization. Such problems stem from a number of reasons. In terms of technical issues, the process of digitalization is hampered by poor digital infrastructure that encompasses lack of access to fast internet and poor quality of telecommunication services offered. There is also inadequate availability of data centers within the country as well as insufficient system integration evidenced by lack of a common digitalization platform at national levels. Some of the major administrative and technical difficulties include the following:

- **Inadequate information technology infrastructure:** Many of the Algerian organizations lack adequate IT infrastructure comprising networks, computers, and fast Internet access¹.
- **Human resource problem:** Although there is no shortage of human resources, their inadequate knowledge about administrative IT poses a hurdle in the implementation of IT projects².
- **Intersectoral problems in coordination:** Poor coordination between different departments in the sharing of information and adopting common information systems causes wastage of time and effort³.
- **Resistance to changes in the administration:** The reluctance of employees working in traditional administrative sectors to adopt any technological changes, often due to their fear of losing jobs or adapting to the technology, is another significant problem⁴.

¹ Chafiq Bouchair, Digital Transformation in Public Administration in Algeria: Reality and Challenges, Journal of Economic and Financial Research, No. 19, 2022, p. 34.

² Mohamed Saidi, E-Government in Algeria: Reality and Prospects for Development, Future Studies Journal, No. 12, p. 88.

³ Nadia Zarrouki, Legal Challenges of Digital Transformation in Algeria, Journal of Law and Society, No. 10, p. 66.

⁴ Karima Salhi, Change Management under E-Government: The Case of Algeria, Journal of Human Sciences, No. 16, p. 141.

Second Requirement: Financial Difficulties

The implementation of e-government faces many financial difficulties which have been a source of hindrance in the process of digitalization. In this regard, the following have been identified as some of the major financial constraints encountered during digitalization in Algeria:

- **Inadequate budget allocation to digital transformation programs:** It is common for government bodies in Algeria to have poor budget allocations to digitalization, leading to either delayed implementation or the abandonment of digital projects¹.
- **Expensive cost of building digital infrastructure:** There is a need to invest considerable resources in building an efficient digital infrastructure, including the installation of data centers, fiber optics, and advanced security systems.
- **Lack of private sector investments in digitalization:** The lack of proper financial incentives and a definite strategy for generating returns on investment discourages many investors from financing digital projects².
- **Poor financial skills for handling digitalization projects:** Despite adequate funding, many project administrators lack financial management skills for handling technology-related projects³.

Third Requirement: Human Difficulties

The shortage of human resources in the digital era poses a big problem to the organizations that aim to integrate new technologies⁴. Human threats pose one of the toughest challenges when trying to create a digital environment in an institution. This is attributed to low digital competence among the employees in terms of lack of specialized training in the digital technologies. The shortage also involves the lack of competent individuals in important fields like computer programming, networking, and management of digital projects, besides the reluctance of traditional administrative staff to embrace change.

These issues can be summed up as below⁵:

- Low level of culture towards information technology in society.

¹ Abdelkader Ben Toubal, Digital Transformation in Algeria: Reality and Challenges, Journal of the New Economy, No. 15, 2021, p. 91.

² Fatima Zahra Jaballah, The Role of the Private Sector in Supporting Digital Transformation in Algeria, Journal of Economic Studies, No. 10, 2022, p. 57.

³ Khaled Ben Aouda, Financial Governance of Digital Projects in Algeria, Journal of Administrative Sciences, No. 21, 2021, p. 48.

⁴ Samira Chettouh, The Impact of Human Competencies on the Success of Digitalization, Journal of Knowledge Economy, University of Sétif, No. 14, 2021, p. 174.

⁵ El-Yakout Arar, Scientific Research in Universities under Digitalization Requirements - Co-authoring Book entitled "Reality and Prospects, Challenges of Digitalization in Administrative Reform and Development (Higher Education Sector as a Model)", Algeria, November 2024, p. 225.

- Lack of sufficient training for advanced and new technologies.
- Little knowledge about computers, together with fear among the managers and employees about using computers.
- Reluctance to technology from employees through lack of motivation and commitment, which could be due to personal reasons like health problems.

Human resource will still remain one of the key assets that require substantial investment to ensure the smooth implementation of digitalization. Human resource forms the basis of intellectual capital, which is made up of professionals and specialists.

In this regard, the successful adoption of digitalization necessitates the readiness of technically skilled human resource that is closely associated with information infrastructure and networks¹. Such a goal can be accomplished via the development of special training courses that will help gain the necessary technical skills.

Fourth Requirement: Legal Difficulties

The advent of digitalization has ushered in a new reality in different sectors, but these changes face certain obstacles, notably those relating to legislation, regulations, and the protection of individual and institutional rights within the digital space.

- **Legislative framework is not responsive enough to meet digitalization needs:** Although there are existing legislative measures dealing with ICTs, the legislative framework does not adequately correspond with the rapid digitalization process.
- **Insufficient protection of personal data:** There is an absence of a coherent legal framework in Algeria regarding the protection of personal data despite the country having signed treaties like the Budapest Cybercrime Treaty².
- **Establishment of evidence in digital legal acts:** The matter of digital evidence is inadequately addressed despite the presence of legislation regulating electronic signatures³.
- **Inadequate implementation of digital laws in public sector institutions:** Although there are legal frameworks in place, their implementation faces some difficulties

¹ Abdelnasser Moussa, Moussa Kriche, The Contribution of E-Administration to the Development of Administrative Work in Higher Education Institutions: Case Study of the Faculty of Science and Technology, University of Biskra, Journal of the Researcher, University of Ouargla, No. 9, 2021, p. 90.

² Sabrina Ben Jelloul, Legal Challenges of Personal Data Protection in the Algerian Digital Environment, Journal of Legal Sciences, University of Annaba, No. 15, 2023, p. 67.

³ Goui Bouhenia, Electronic Evidence between Text and Practice in Algeria, Algerian Journal of Law and Technology, No. 4, 2021, p. 45.

owing to bureaucratic processes, lack of technical knowledge, and other reasons already highlighted¹.

TYPES OF VIOLATIONS AGAINST DIGITAL SOVEREIGNTY

Violation against state sovereignty through digital means is feasible through several different means, considering the various ways through which cyber warfare may be carried out using digital technologies to exert influence over nations and corporations. Such violations serve as a significant threat to digital sovereignty and demand appropriate responses from governments to enhance cybersecurity and safeguard sensitive information². The common types include the following:

First Requirement: Electronic Espionage

Electronic hacking forms one of the commonest ways of carrying out espionage operations in the modern age, owing to the growing number of entities that provide their services through the Internet. Consequently, such systems and services have become vulnerable to hacking activities and electronic espionage.

As such, any network that is linked to the Internet is automatically exposed to hacking and espionage. The level of exposure is greatly dependent upon the security policies put in place to safeguard the systems as well as the human element that directly engages these systems.

The systems heavily rest on infrastructure elements including the network, the software, the servers, the computers, and other Internet-connected devices. All these are vulnerable to hacking and cyber espionage. In actuality, all Internet-linked devices can give out significant details about themselves, the software they are running, and the entire system in which they operate unless there is sufficient security against hacking³.

For instance, considerable information regarding networking and connecting devices may be gathered through a range of electronic scanning utilities. The practice, often termed Information Gathering, is done in order to locate valuable information or security weaknesses which will allow the compromising of the device or network. Such processes might involve:

- Password theft for the purpose of obtaining information, including the exploitation of any password repositories.
- Use of social engineering tactics to trick people into revealing passwords and other confidential information.

¹ Khaled Reggad, E-Government in Algeria between Legal Texts and Practice, Journal of Economy and Society, University of Blida, No. 9, 2022, p. 134.

² Ikram Belbai, Legal Stakes of the Internet and Its Impact on Digital Sovereignty, Algerian Journal of Legal and Political Sciences, 2024, p. 234.

³ Khadidja Ben Guettat, Implications of Cyber Warfare on Digital Sovereignty, Algerian and Comparative Public Law Journal, 2024, pp. 290–293.

- Installation of malware to carry out reconnaissance of connections and communications.

Second Requirement: Cyberattack

A cyber-attack is a significant security issue that can affect persons, organizations, and countries. It can be used for various reasons, such as stealing information, fraudulent activities, and accessing confidential financial, health, military, or security data. Additionally, a cyber-attack can result in the control of electronic gadgets, which could be done for political reasons and intended to inflict physical harm like triggering an explosion.

Such attacks can also be waged using electromagnetic means or anti-radiation munitions with the purpose of weakening the fighting strength of the enemy and reducing its ability to use the electromagnetic spectrum. Such attacks involve different types of electromagnetic jamming and deception tactics. Unlike regular warfare that usually leads to losses in human lives, such attacks result in material losses and disruptions in operations. Some of the other types of cyber-attacks include those against logistics support systems for weakening the enemy's capacity and against power generation and energy control systems. They can be listed as below:

- **Defacement attacks:** In this category of attacks, attackers focus on webpages and substitute them with new pages that contain altered information. They may create fake web pages, which resemble genuine pages, in order to mislead individuals and steal confidential information like personal details and credit card data.
- **Deceptive attacks:** Deceptive attacks are based on manipulating TCP/IP to undermine security measures during the transaction between clients and servers. Transmission control and protocol are mechanisms for creating a secure connection through a combination of port and logical numbers assigned to each transaction. However, attackers can guess these ports and act as legitimate users, enabling them to hack into databases, interrupt connections, divert data packets, overload systems with messages, or even disrupt legitimate data transfer.
- **Attacks on infrastructure:** This kind of attack targets important systems, including electricity supply systems, sewage systems, hospitals, and security control systems. Some institutions have a low level of understanding when it comes to cybersecurity measures and, therefore, cannot create organizational frameworks, programs, and technologies to mitigate cyber-attacks. This leaves them vulnerable to data breach, damage to infrastructure, and insecurity generally.

Third Requirement: Electronic Hacking

The term electronic hacking is associated with any form of unapproved access into other people's computers and electronic systems with the aim of breaching confidentiality and privacy or manipulating information in any way possible. This

kind of cyber-attack goes beyond hacking personal information but also involves revealing state secrets, breaking into government organizations' website pages, and hacking the emails of politicians.

This is especially true for nations that have been embroiled in internal strife or faced economic sanctions in recent years. There have been numerous leaks of very sensitive data that involve personal details about targeted foreign personalities. This is usually done with the purpose of undermining the targeted individual or causing political turmoil in the country concerned¹.

Fourth Requirement: Cyberattack on Military System

Cyberattack against military system attacks weapon controls, satellites, and communication networks of the military to hinder its operation. Attacks against government and military activities can either be done to gain design plans for weapons, acquire confidential information, understand the strategies of the opponent during warfare, and determine the plans and movements of the military.

Therefore, all networks connected to the Internet are vulnerable to attack, including networks that are not directly linked to the Internet. Although governments and militaries depend on these networks during times of peace, their dependence does not ensure protection during times of war. On the contrary, the technological sophistication of today's military systems may end up becoming their undoing when they fall victim to cyberattack leading to their destruction or neutralization².

WAYS TO DEFEND AND PROTECT AGAINST INTELLIGENCE ACTIVITIES

Security agencies conducting intelligence operations usually encounter a myriad of obstacles as they are vulnerable to direct and indirect security risks. Conducting intelligence operations in cyberspace demands the protection of electronic gadgets used by security agencies, ensuring that their cyber accounts are secured, and making use of various tactics like anonymization and encryption. Additionally, a security agency must learn how to work with fake accounts in identifying any hostile forces against the country.

The issue of cybersecurity continues to be one of the most sophisticated fields considering the rapidly changing trends in computer technology, internet technology, and communication technology. In achieving adequate protection in cyberspace, the adoption of various methods is required.

The deployment of anti-virus programs marks the first step in the fight against malware programs that might infiltrate and harm personal computing systems. It should be understood, however, that the implementation of these tools alone does not guarantee total security for one's devices, data, and privacy.

¹ Leila Baouni, Threats in Cyberspace and Their Impact on Digital Sovereignty: Cybercrime as a Model, Journal of Studies and Defense, 2021, p. 9.

² Khadidja Ben Guettat, op. cit., p. 293.

State governments need to take a holistic strategies and policies in attaining digital sovereignty. This includes implementing numerous actions both within the state, which encompasses building digital infrastructure, localizing technologies, enacting data protection laws, safeguarding network and communication systems, fostering digital citizenship, and enhancing international digital cooperation¹.

First Requirement: Development of Digital Infrastructure and Localization of Technology

Efforts towards achieving digital sovereignty must include considerable efforts towards developing digital infrastructure. The efforts would include developing fast and secure means of communication that would give citizens a secured and stable access to the internet along with developing safe and secure localized cloud-based systems where data can be stored for purposes of processing it and offering digital services. For the sake of the sustainability and continuity of these infrastructures, proper governance is required, which is made up of three components namely, technological infrastructure, organizational arrangement, and cultural foundation. This would involve first establishing a renewable and scalable knowledge ecosystem through which the acquisition of knowledge is achieved through eliminating both material and intellectual impediments. It also involves transferring and production of technologies leading to technological empowerment which in turn involves competitiveness, innovation, adaptation, and independence from foreign technologies among others. In other words, it involves strategic resilience which refers to the ability of a state to utilize its technological capacity in producing innovations while continuously adapting to new trends and technologies.

Second Requirement: Development of Legislation and Policies for Data Protection

In order to achieve this objective, the need for the development of tougher legislation aimed at protecting personal information becomes necessary. This involves the establishment of policies that regulate the process of collecting, accessing, transmitting, and storing data according to certain standards of confidentiality and security.

Third Requirement: Monitoring and Surveillance of Networks and Communications

At this point, the state needs to have highly developed capacities for the supervision and monitoring of digital networks and communications. This is

¹ Amina Aijer, Digital Sovereignty in a Globalized World: Challenges and Stakes, Journal of Legal and Political Studies, 2024, p. 76.

necessary for identifying and responding to cyber threats. The use of hacking detection software and other methods of monitoring will be necessary here.

Fourth Requirement: Promoting Digital Citizenship

This element includes the issue of informing citizens about the dangers of using the Internet, practicing good and ethical behavior on the Internet, respecting other people's rights and engaging positively, as well as participating digitally in politics. It is important for states to develop policies that focus on building transparency and accountability in the usage of digital technology and data collection processes. This implies having systems for monitoring the usage of digital technology by government institutions and businesses, which protect the rights of citizens and preserve national sovereignty.

Fifth Requirement: Promoting Digital International Cooperation

Such an approach entails engagement in international organizations like the UN and EU, in order to create common approaches towards the digital challenges on the international stage. In such a case, the idea of a Global Digital Compact has been initiated, signed on the occasion of the 75th anniversary of the UN in September 2020, and developed further through a multistakeholder approach up until the September 2024 Summit. Such an approach would include states, the UN System, business community, civil society, local communities, academia, as well as individual members, including young people. The Global Digital Compact will outline broad principles regarding the digital world of the future.

Conclusion:

Based on the above, it is clear that digital transformation is now a matter of strategic necessity, and the cyberspace has become a space of war, where countries seek to secure their information systems from attacks on national security and stability. In Algeria, as well as in other countries, the adoption of a national cybersecurity strategy has become a means for ensuring digital sovereignty by creating different mechanisms whether by establishing specific agencies responsible for securing cyberspace or passing laws meant to counter any cyber threat and ensure the safety of users within this space.

Ultimately, technological development alone is not enough; what really counts is the willpower of politics. In cyberspace, the struggle is not only against the hacker, but also against dependency and dominance of technology. Thus, the development of a smart security system in Algeria is not only about securing the country, but also

about securing its future and ensuring the independence of its decision-making process in the digital era.

Based on the findings of this research, the following recommendations can be formulated:

- ✓ The implementation of a comprehensive national strategy at various levels involving the participation of experts and specialists in addition to other concerned parties with a view to guaranteeing digital sovereignty and cybersecurity.
- ✓ The inclusion of Algerian universities and the educational sector and vocational training within the curricula and training courses, especially in the fields of technology like cybersecurity, artificial intelligence, and digitalization.
- ✓ Developing the legal framework by enacting new laws that cover all issues concerning digital sovereignty from the individual, corporate, and governmental perspectives.
- ✓ Supporting the development of reliable cybersecurity infrastructure, which includes innovative technologies, best practices, and qualified human resources capable of coping with cyber challenges.
- ✓ Increasing public awareness about the need for data protection and privacy to support digital sovereignty and cybersecurity.
- ✓ Collaboration with other countries, especially those with developed technology, by sharing cyber threat information to ensure digital sovereignty is protected from any form of attack.

List of sources and references:

A) Books:

- Hazem Dahhan, Nasser Al-Quraiti, Cybersecurity and Information Security Protection, Dar Al-Fikr Al-Jami'i, Alexandria, 2021.
- Hiba Gamal El-Din, The State and Its National Security in the Age of Artificial Intelligence and Its Intersections, Dar Al-Maaref, Egypt, 2023.
- Mohamed El-Gendy, Cybersecurity: From Information Warfare to Cybercrime, Dar Al-Maaref, Egypt, 2024.
- Awad Mofeed Hassan Ali, Cybersecurity and Its Fundamentals, Publishing and Distribution, Sultanate of Oman, 2025.

- Abbas Mostafa Sadiq, New Media: Concepts, Tools, and Applications, Dar Al-Shorouk, Cairo, Egypt, 2008.
- Abdulrahman bin Ibrahim Al-Shaer, Social Media and Human Behavior, Dar Safaa for Publishing and Distribution, Amman, Jordan, 2015.

B) Journal article:

- Suleiman Kattaf, Abdelhalim Boutarine, Cybersecurity and Its Associated Conceptual Dimensions, Journal of Tebna for Scientific and Academic Studies, Algeria, Vol. 5, No. 2, 2022.
- Mohamed Messika, Cyberspace and the Challenges of National Security of States, Journal of Legal and Social Sciences, Algeria, Vol. 7, No. 4, 2022.
- Mohamed Karziz, Meriem Yahiaoui, The Virtual Environment and Education, Journal of Research and Studies, Algeria, No. 6, 2008.
- Mohamed El-Said Bouflih, Frameworks of International Cooperation to Address Cyber Threats, Journal of Applied Legal Studies, 2024.
- Abdellah Jaafari, Cyber Threats and Their Impact on Algerian National Security, African Journal of Legal and Political Studies, Vol. 6, No. 2, 2022.
- Abdelghani Chergui, Cyber Threats and the Problem of Sovereignty, Journal of Global Politics, Vol. 7, No. 2, 2023.
- Amina Bessafa, Legal Frameworks of Cybercrime in Algerian Legislation between Prevention and Enforcement, Annals of the University of Algiers 1, Vol. 37, No. 1, 2023.
- Sara Yakhouch, Artificial Intelligence and Cybersecurity (Functions and Challenges), Algerian Journal of Social and Human Sciences, Vol. 9, No. 1, 2025.
- Chafiq Bouchair, Digital Transformation in Public Administration in Algeria: Reality and Challenges, Journal of Economic and Financial Research, No. 19, 2022.
- Mohamed Saidi, E-Government in Algeria: Reality and Prospects for Development, Future Studies Journal, No. 12.
- Nadia Zarrouki, Legal Challenges of Digital Transformation in Algeria, Journal of Law and Society, No. 10.
- Karima Salhi, Change Management under E-Government: The Case of Algeria, Journal of Human Sciences, No. 16.
- Abdelkader Ben Toubal, Digital Transformation in Algeria: Reality and Challenges, Journal of the New Economy, No. 15, 2021.
- Fatima Zahra Jaballah, The Role of the Private Sector in Supporting Digital Transformation in Algeria, Journal of Economic Studies, No. 10, 2022.

- Khaled Ben Aouda, Financial Governance of Digital Projects in Algeria, Journal of Administrative Sciences, No. 21, 2021.
- Samira Chettouh, The Impact of Human Competencies on the Success of Digitalization, Journal of Knowledge Economy, University of Sétif, No. 14, 2021.
- Abdelnasser Moussa, Moussa Kriche, The Contribution of E-Administration to the Development of Administrative Work in Higher Education Institutions: Case Study of the Faculty of Science and Technology, University of Biskra, Journal of the Researcher, University of Ouargla, No. 9, 2021.
- Sabrina Ben Jelloul, Legal Challenges of Personal Data Protection in the Algerian Digital Environment, Journal of Legal Sciences, University of Annaba, No. 15, 2023.
- Goui Bouhenia, Electronic Evidence between Text and Practice in Algeria, Algerian Journal of Law and Technology, No. 4, 2021.
- Khaled Reggad, E-Government in Algeria between Legal Texts and Practice, Journal of Economy and Society, University of Blida, No. 9, 2022.
- Ikram Belbai, Legal Stakes of the Internet and Its Impact on Digital Sovereignty, Algerian Journal of Legal and Political Sciences, 2024.
- Khadidja Ben guettat, Implications of Cyber Warfare on Digital Sovereignty, Algerian and Comparative Public Law Journal, 2024.
- Leila Baouni, Threats in Cyberspace and Their Impact on Digital Sovereignty: Cybercrime as a Model, Journal of Studies and Defense, 2021.
- Amina Aijer, Digital Sovereignty in a Globalized World: Challenges and Stakes, Journal of Legal and Political Studies, 2024.

C) Co-authoring Book:

- El-Yakout Arar, Scientific Research in Universities under Digitalization Requirements - Co-authoring Book entitled "Reality and Prospects, Challenges of Digitalization in Administrative Reform and Development (Higher Education Sector as a Model)", Algeria, November 2024.