Contemporary Readingsin Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 17 (01), 2025
pp. 1197 – 1210

Cybersecurity and Digital Sovereignty: From Information Warfare to Cybercrime

Dr. Abderrahim Lahreche[1]*, Dr. Mabrouk Lachgueur[2]*

[1]University of Ghardaia, Faculty of Law and Political Science, Law and Society Laboratory in the Digital Space, Algeria.Email: lahreche.abderrahim@univ-ghardaia.edu.dz

[2]University of Ghardaia, Faculty of Law and Political Science, Law and Society Laboratory in the Digital Space, Algeria.Email: lachgueur.mabrouk@univ-ghardaia.edu.dz

ABSTRACT:

This researchseeks to develop a conceptual approach regarding the role of cybersecurity in promoting digital sovereignty, particularly amid technological advances in artificial intelligence systems. It focuses on effective online techniques that can be used to address these challenges and enforce digital sovereignty effectively through developing advanced security systems capable of detecting abnormal patterns and predicting security threats before they occur and raising user awareness about the risks of cybercrime while reinforcing their ability to effectively deal with electronic threats. Therefore, it is imperative to ensure proper precarious monitoring of these systems' performance in real-world environments. It is also appropriate to issue legal texts to regulate this field.

Keywords: Digital Sovereignty; Cybercrime; Cybersecurity; Artificial Intelligence

Received: 02/06/2025 **Accepted: 27/10/2025** **Published: 16/12/2025**

. INTRODUCTION

The significant technological developments in communication, digitalization, the internet, and artificial intelligence have posed new challenges to media studies concepts and research tools. Rapidly spreading web technologies have created a genuine social and communicative revolution. The cyber field has become a key part of modern warfare, targeting states' national security and inflicting substantial losses on the global economy. These conflicts have diversified, threatening state's digital sovereignty through semiconductor manufacturing, digital industries, communication technologies, information warfare, and cyber espionage. This geopolitical shift has served as a source for exploiting information technology and cyberspace in political, military, economic, security, and social spheres, leading to the evolution of warfare generations and their impact on states' national security such as the Fourth Generation Warfare, and so on. Consequently, this development has influenced how security and intelligence apparatusrespond to these changes and how they create new strategies to address threats arising from information technology integration into all aspects of life, significantly affecting national security determinants of the state.Therefore, the evolution of warfare was always related to the modern technology and communication.

As a result, these developments have influenced national sovereignty, as major technological advances have created new sovereign spheres, compelling world nations to impose security control over other states. Cybersecurity thus represents one of the most important pillars of the security system for safeguarding national security in most states, including Algeria.

This research seeks to identifyhow digital world interacts between cyberspace and sovereignty, along with Algeria's national security, recognizing that state's sovereignty has changed given new technological innovations that repudiate the international borders. States now fear for their sovereignty and consequently their national security, which has become vulnerable to new cybernetic threats.

Accordingly, the research problematic was as follows:How did Algeria succeed in protecting its digital sovereignty and national security amid cyber warfare and cybercrime?

To address this problematic, this research is divided into four main topics: beginning with the first topic: The Impact of Cyber Influence on National Digital Sovereignty and Security; then examining the second topic:Electronic Investigation and Information Gathering Methods; followed by the third topic which is:Forms of Encroachment on Digital Sovereignty; and ultimately exploring the last topicasfollows:Defense and Protection Methods Against Intelligence Operations.

1. The Impact of Cyber Influence on Digital Sovereignty and National Security

The fundamental challenge facing states today is how to take control over information technology and to avoid falling into its manipulation. Without effective countermeasures, no state can remain safe from this digital impact, whose consequences have become increasingly devastating.

Therefore, Cybersecurity represents not only a national concern but also a regional and continental one, especially with digital technologies continuing to play an increasingly key role in all aspects of daily life.

1.1 National Strategy for Achieving Digital Sovereignty and Promoting Cybersecurity

Algeria has pursued technological independence and the promotion of digital sovereignty by signing an agreement to establish the National Center for Digital Services, which will contribute to hosting and centralizing national data within national territory. This will strengthen integration among national digital solutions and enhance the country's technological infrastructure.

This significant step toward achieving technological independence and promoting digital sovereignty reflects Algeria's commitment to developing its digital infrastructure to support the digital economy and achieve technological integration. Algeria has experienceda range of phases follows:(Senoussi, 2024 , p. 9)

First Phase:

The implementation of the first national data center with all its infrastructure components, including interoperability operations, the national public service database, the interactive public services portal, and the national cloud. This was completed within the first nine months of 2024, with 14 fully digital public services deployed.

Second Phase:

Expected to deploy the second national data center with all its components, infrastructure, interoperability operations platform, national public service database, interactive public services portal, and national cloud within three months of the first center's deployment, along with 26 fully digital public services.

This implementation involves creating an infrastructure consisting of two national data centers meeting approved standards to host and centralize national data throughout national territory.

Third Phase:

Strengthening information systems throughinstitutions and bodiesincluding the National Higher School of Artificial Intelligence, an elite higher education institution tasked with training engineers specializing in artificial intelligence theory and data science. These engineers will be capable of developing and deploying practical and innovative solutions to various social and economic sector problems (such as health, energy, agriculture, transport and so on…), which contributes in the scientific and economic development in Algeria. (National Higher School of Artificial Intelligence, 2024)

In addition to the core tasks of national higher education institutions in Algeria, the school will strive to achieve the following objectives:

- **Excellence in Teaching:** Aimed at equipping engineers with a solid foundation in mathematics, a deep theoretical understanding of various artificial intelligence technologies and entrepreneurship, as well as practical and general skills that make them attractive to employers.

- **High-Quality Research:** This will be achieved by addressing the shortage of researchers and specialists in fields such as data science, artificial intelligence, the Internet of Things (IoT), computer vision, natural language processing, and speech processing.

- **Interdisciplinarity:** Focused on meeting real needs in higher education and interdisciplinary scientific research through the application and development of new AI technologies across various fields such as energy, agriculture, health, and security, among others.

- **Digitalization:** The school is established to contribute to the country's digital development.

Fourth Phase:

Creating a national higher school of cybersecurity, contributing to national efforts in scientific research and technological development in information systems security, offering high-tech innovative solutions.

Presidential Decree No. 24-181 stipulates that this school undertakes "ensuring advanced training, scientific research, and technological development for engineers and doctorate holders with high-level scientific and technical expertise, enabling them to perform development or teaching roles in cybersecurity fields."

The school is also entrusted, in collaboration with the Information Systems Security Agency*, with* "promoting the development of science and technology in the field of cybersecurity"and"participating in strengthening national technical capacities in this field."

The creation of the National School of Cybersecurity follows the directives of the Council of Ministers dated September 12, 2023, which called for the establishment of a national higher school of cybersecurity in coordination with the Ministry of National Defense, to "unify efforts and maximize efficiency in this sensitive context in order to safeguard national security."

1.2 Legal Frameworks for Promoting Digital Sovereignty in Algeria

The Algerian legislature has strengthened its legal arsenal to confront threats to Algerian national security, particularly regarding information systems security through data protection in electronic processing. The legislature has enacted several amendments, including Order 66-156 incorporating the Penal Code, under Law 04-15, Section Seven (bis), addressing threats on automated data systems processing, encompassing eight articles from Article 394 (bis) to Article 397 (bis[7]).

Law No. 04-14 related to criminal procedures also enables extending jurisdiction to systems of automated data processing crimes according to Article 37, while excluding application of search provisions stipulated in the amended Article 45 by Law No. 06-22 concerning such crimes.

The legal framework has been further strengthened through legislative rules preventing crimes related to information and communication technology via Law 09-04, which established general provisions combating attacks on personal data regardless of transmission media, whether public or private networks. This law established a national body for preventing and combating such crimes through Article 13, with its composition, organization, and management methods determined through regulations, as specified in Presidential Decree 19-172. (Taqiyya & Boubakr, 2024, p. 137)

Algeria has extended these reforms to protect individuals regarding personal data throughthe issuance of Law 18-07 concerning mechanisms protecting natural person in personal data matters, through a range of articles protecting personal information from any security threat in the digital space.

These new protection procedures have extended to the Ministry of National Defense through the National System of Information Systems Security via Presidential Decree 20-05, establishing a national system of information systems security, enacted through Article 3 that specifies: "The the National System of Information Systems Security established at the Ministry of National Defense includes:

- A National Council for Information Systems Security, referred to in the text as "the Council," charged with preparing, approving, and directing the national strategy for information systems security;
- An Information Systems Security Agency, referred to as "the Agency," tasked with coordinating the implementation of the national strategy of information systems security;
- With specialized structures from the Ministry of National Defense in this field to support the Council and Agency."

2. Electronic Investigation and Information Gathering Methods

Efforts to provide an electronically secure environment for sensitive information systems require cooperation and coordination transcending national solutions, achievable through presenting electronic security concerns at international and regional forums. (Gamal El-Din, 2023, p. 71)

2.1 Various Information Gathering Sources

Cyberspace intelligence cannot be complete without gathering information from various digital and electronic sources. The enormous advancement in information technology use and its applications has led to widespread computer, smartphone, and mobile device distribution, culminating in internet-connected modern devices.

This development has also increased the number of internet users globally to over 4.6 billion users. In the Middle East, hacking's rates increase daily among populations in most Arab countries, frequently exceeding global average growth rates.

These statistics demonstrate the vast volume of data produced by this number of users. Given that most information exists in open sources, it has become a crucial and indispensable source for gathering intelligence and security information, including criminal investigations involving traditional or cybercrimes with digital evidence in cyberspace, or terrorist operations potentially beginning in cyberspace through terrorist-communications, ending to various internet utilizations by terrorists.(El-Gendi, 2024, p. 73)

However, this informationrequiresgathering and analysis for effective use in clarifying crimes or general criminal investigations. Generally, information available in cyberspace for intelligence purposes exists either in closed or open sources.

2.2 Open Sources and the Internet

The internet has provided numerous information research sources; however, this information lacks value without analysis and transformation into useful or intelligence information usable for specific decision-making or serving particular purposes. Security agencies have recognized the importance of internet information gathering for several reasons, illustrated as follows:(Ali, 2025, p. 40)

- Internet use by terrorist groups;
- Widespreadcybercrime ;
- Political and religiousconflicts ;
- Proliferation of internet-connected devices;
- Security vulnerabilities in communication infrastructure ;
- Cyber attacks ;

The primary use of open sources involves clarifying crimes through investigating and analyzing open sources such as the internet and social media platforms.

2.3 Social Media Investigation

Social networks represent important open sources through which information about individuals and their various interests can be gathered. Numerous tools exist for compiling and analyzing information from social media to investigate suspects relationships, interests, personal images or to predict specific events such as hostile actions or riots in specific geographic areas or using specialized tools. (Sadiq, 2008, p. 218)

The extensive spread of social media and social networks such as **Facebook** and **Twitter** has led to crime spread on these platforms, possibly presenting opportunities for security apparatus to gather and analyze data from these open sources without requiring other information-gathering methods or judicial permission, given that this information and data are publicly available without restriction.

Social media serves as a reflection for real-world events and is fundamentally social; therefore, numerous social and psychological problems appear on these platforms, ranging from boasting about certain actions or phenomena supporting illegal activities threatening state security and safety.(Al-Shaer, 2015, p. 67)

2.4 Investigation Through Maps and Satellite Imagery

The internet contains numerous open-source databases, some freely available and others requiring payment or subscriptions, providing resources for investigating specific geographic locations using mobile phone towers and geographic area images during specific periods, as well as information about wireless communication networks in particular areas.

Among the most important tools for intelligence investigations are Google Maps, Google Earth, Bing Maps, and Google Street View, enabling investigators to compare these maps to gather significant information about specific geographic areas for determining boundaries or identifying published video on internet, as well as determining the location ofacapturedvideo or image in a case of no extra data. (El-Gendi, 2024, p. 102)

3. Forms of Encroachment on Digital Sovereignty

Various forms of state sovereignty encroachment in cyberspace reflect different forms of cyber warfare relying on digital technologies to influence states and organizations. These forms present genuine challenges to digital sovereignty, requiring effective government response to reinforcecybersecurity and protect sensitive information(Belbey, 2024, p. 234). Such forms are illustrated as follows:

3.1 Electronic Espionage

Electronic hacking constitutes one of the most important current espionage methods, given the numerous institutions offering services through the World Wide Web, making connected systems and their services available to either users,hackers or spies alike.

Therefore, any internet-connected system undoubtedly faces exposure to hacking and espionage, with security substantially dependent on security policies protecting these systems and the human element directly operating them.

These systems fundamentally depend on infrastructure, networks, and software on servers, computers, or internet-connected devices. All these elements are subjected to hacking and espionage. Each internet-connected device can reveal substantial information about itself, its operating programs, and its connected system unless properly secured against espionage for having access to information.(Ben Qattat , 2024, p. 290)

For instance, important information about connected networks and devices can be gathered through various electronic scanning tools through what is termed "information gathering" to obtain sensitive information or security vulnerabilities enabling device or system compromise.

3.2 Cyber Attacks

Cyber-attacks represent security threaton individuals, institutions, and states, potentially used for data theft, fraud, and illegal access to financial, medical, military, or classified security data, or manipulation of remotely controlled electronic devices directed at political objectives causing material harm, such as detonating devices remotely or disrupting systems.

This occurs through electromagnetic means or anti-radiation weapons attacking individuals and facilities to weaken enemy combat capabilities and reduce effective electromagnetic spectrum use. These attacks include various electromagnetic jamming and deception operations, typically resulting in losses unlike conventional warfare, which frequently involves human casualties. Among cyber-attack types are disrupting logistical support systems to reduce support for enemy forces and diminish effectiveness, as well as controlling electricity and power generation systems.

3.3 Hacking

This involves unauthorized access to others' devices and electronic networks, aiming to compromise institutional and individual confidentiality and privacy or affect content integrity through modification or destruction. Hacking extends beyond citizens' personal information to revealing state security secrets and compromising government institution websites and state leaders' emails and responsible officials, particularly in states experiencing civil wars or economic blockades. The past decade has experienced unprecedented secret-natured leaks with detailed precision concerning targeted international figures aimed at their removal or creating disorder and instability within their belonging states.(Baouni, 2021, p. 9)

3.4 Cyber Attacks on Military Systems

These target weapon control systems, satellites, or military communication systems to disrupt warfare operations. Attacks on military and government operations aim either to obtain weapon designs or secret information access, understand enemy thinking during war, or know military plans and troops' positions. Thus, any internet-connected network are subjected to attacks, and even disconnected ones may not escape danger. Governments and armies rely on these networks during peacetime; however, this does not guarantee wartime safety, as modern military technology advantages could transform into disaster if targeted by cyber-attacks causing disruption. (Ben Qattat , 2024, p. 293)

4. Defense and Protection Methods Against Intelligence Operations

Intelligence apparatuses sometimes face cyberspace difficulties without encountering security problems targeting them directly or indirectly. Cyberspace access requires securing electronic devices used by security agencies, securing their internet accounts, employing concealment and encryption measures, and understanding dummy account operations for tracking anti-state elements. Cybersecurity represents among the most technically complex subjects due to significant computer, internet, and communication technology advances, requiring numerous tools and methods for achieving acceptable cyberspace protection covering physical, digital, and privacy protection.

Antivirus software represents the first defense line against most computer viruses; however, recognizing that these programs alone insufficiently protect devices, data, and privacy remains essential.

4.1 Directed Policies and Strategies

States require comprehensive, multidimensional, and multilevel policies and strategies for achieving digital sovereignty, encompassing internal procedures including developing digital infrastructure, technology localization, and establishing data protection legislation, along with network and communication monitoring, promoting digital citizenship, and improving international digital cooperation.(Idjir, 2024, p. 76)

4.1.1 Developing Digital Infrastructure

For genuine and effective digital sovereignty, real investment in digital infrastructure is necessary through reliable, high-speed communication networks ensuring citizen access and network security, and local cloud storage systems. This undoubtedly improves local data processing capacity and delivers secure, reliable digital services to citizens, and ensures sustainability through proper management, with three essential elements intersecting in valuing infrastructure: technological structure, organizational structure, and cultural structure.

4.1.2 Technology Indigenization

This process involves developing a renewable knowledge system facilitating knowledge acquisition, requiring overcoming material and intellectual obstacles. It requires transferring and producing technology domestically toward technological empowerment, which is a stage of self-sufficiency and competitive capacity based on state technological capacities qualified for production, manufacturing, rapidly adapting to changes, and precariousadaptation to developments, known as strategic flexibility.

4.1.3 Establishing Legislation and Policies for Personal Data Protection

This objective requires implementing stricter legislation protecting citizens' and residents' personal data, including establishing policies controlling data use, sharing, and storage consistent with privacy and security standards.

4.1.4 Monitoring Networks and Communications

States must develop capabilities for monitoring digital networks and communications to identify and confront cyber threats, including employing advanced hacking detection techniques and regular monitoring of unauthorized activities.

4.1.5 Promoting Digital Citizenship

This encompassestheawarenessofinternet hazards, ethical and responsible online conduct, respecting others' rights, positive participation, digital political participation, and providing training programs. States must implement policies promoting transparency and accountability in digital technology and data collection use, including providing mechanisms for monitoring government and private company digital technology use, preserving citizen rights and protecting national sovereignty.

4.1.6 The EnhancementofInternational Digital Cooperation

This includes participating in international organizations such as the United Nations and European Union to establish common standards addressing digital challenges internationally. A global digital charter was announced within this framework, adopted on the UN's 75th anniversary in September 2020 and agreed upon at the September 2024 summit through a technology pathway including all stakeholders-governments, UN systems, private sector, civil society, grassroots organizations, academic circles, and individuals, including youth. The global digital charter is expected to establish broad digital principles for common future enabling open, free, and secure digital environments for all.

4.2 Algeria's Policies for Achieving Information Security

Algeria, alongside other states, has undertaken significant steps in cybersecurity to protect its digital sovereignty. Algeria's national defense leadership has prioritized cybersecurity, hastening security policy revision by incorporating new mechanisms addressing these matters. The national defense institution developed specialized programs confronting cybercrime and limiting its spread, establishing coordinated bodies consistent with technological changes in this field.(Chahrit & Kribiz, 2022, p. 310)

4.2.1 Structures Established for Investigating Cybercrime

These structures have significantly contributed to cybercrime detection across various sectors, facing numerous challenges, including advanced technologies employed in these crimes. Principal structures include:

a) The National Gendarmerie Center for Prevention of Automated Information Processing Crimes and Information Crimes

Established in 2008 in BirMouradRaïs, the capital, serving as a documentation center aimed at securing information systems serving public security. It analyzes information and data on informational crimes.

b) National Institute for Forensic Evidence and Criminology

Established in Bouchaoui (Algiers), under the General Command of the National Gendarmerie - Electronic Information and Communication Division through Presidential Decree 04-183 dated July 26, 2004, and amended through Presidential Decree 09-118 dated April 14, 2009.

This apparatus comprises 11 specialized divisions in various fields ensuring all expertise, training, and education, with numerous specialized departments and services, including fingerprint, document, automated information, and environmental services.

c) Central Unit for Combating Informational Crime (National Security Management)

National security services established the Central Unit for Electronic Crime in 2011, adapting the police judicial directorate security organization, initially forming a special security unit nucleus for electronic crime combat at the general national security management level, subsequently establishing the Central Unit for combating crimes related to information and communication technologies.

d) National Authority for Prevention and Combating Crimes Related to Information and Communication Technologies

Constituted through Presidential Decree 15-261, serving as an independent administrative authority under the Justice Minister, operating under a directorate committee supervision chaired by the Justice Minister and including government members appointed to the position, security service directors, and judges from the Supreme Court appointed by the Superior Judicial Council. The authority includes judges, officers, and agents from the judicial police of military intelligence services, the national gendarmerie, and national security.

4.2.2 National People's Army Efforts for Digital Sovereignty Defense

The National People's Army General Staff developed a cyber defense strategy covering all aspects for achieving integrated cyber defense systems, centering the army's cyber defense strategy through several principal themes:(Chahrit & Kribiz, 2022, p. 312)

a) Functional and Organizational Aspects: Cyber defense operations are directed and implemented within dedicated functions or organizations ensuring operational consistency and effectiveness.

b) Legal Aspects: Continuing to update and strengthen legal framework concerning information and communication technology use generally and information systems security specifically.

c) Human Resources Aspects: Ensuring considerable technical human resource availability and highly qualified expertise in cyber defense.

d) Technical Aspects: Strengthening and adapting protection technical capacities undoubtedly contributes to continuously detecting and responding to cyber-attacks.

e) Prevention and Awareness Aspects: Sensitizing National People's Army users to cybersecurity risks and threats and preventing them.

f) Research and Development Aspects: Utilizing National People's Army research and development structures for specialized technical means represents a decisive cyber defense strategy element.

g) Cooperation Aspects: Promoting digital security and cyber defense cooperation with partner nation militaries benefits from advanced technological expertise and means.

Conclusion

Cyberspace development has substantially enhanced intelligence and security operations among states. Algeria has undertaken significant steps protecting its digital sovereignty, as the cyberspace has established a prominent and enormoussource of various variable information such as open sources and vast date on internet which contributed in the evolution of security sciences, crime control and cybersecurity. Therefore, states, including Algeria, must strengthen their digital systems through legislation and methods protecting digital sovereignty.

Consequently, through this research, several recommendations and suggestionsshouldbe taken inconsideration:

- Establishing a comprehensive strategy at all levels encompassing all experts, specialists, and stakeholders in this field tasked with protecting state digital sovereignty and cybersecurity.

- Directly involving Algerian universities and education and professional training sectors in curricula bygivenprioritytotechnological specializations in cybersecurity, artificial intelligence, and digitalization.

- Strengthening the legislative system with laws addressing digital sovereignty questions from various perspectives affecting physical and moral persons, state institutions as well.

- Investing in developing strong, secure infrastructures ofcybersecurity including advanced technologies, best practices, and staff training for addressing security challenges across the digital space.

- Increasing societal awareness regardingtheimportance of protectingdataand privacy for promoting digital sovereignty and cybersecurity.

- Strengthening cooperation with technologically advanced states sharing information about cyber threats and preserving digital sovereignty against any kind ofhacking.

5. Bibliography List:

1. Ali, M. A. (2025). *Cybersecurity and its fundamentals.* Sultanate of Oman: Sultanate of Oman for Publishing and Distribution.

2. Al-Shaer, A. B. (2015). *Social media platforms and human behavior.* Amman, Jordan: Safaa Publishing and Distribution.

3. Baouni, L. (2021). Threats in cyberspace and their repercussions on digital sovereignty: Electronic piracy as a model. *Journal of Defense and Strategic Studies*, 9.

4. Belbey, I. (2024). The legal stakes of the internet and its impact on the digital sovereignty of states. *Algerian Journal of Legal and Political Sciences*, 234.

5. Ben Qattat , K. (2024). The implications of cyber wars on digital sovereignty. *Algerian Journal of Public and Comparative Law*, 290.

6. Chahrit, A., & Kribiz, M. (2022). Internet challenges to state sovereignty (digital sovereignty). *Journal of Legal and Economic Research*, 310.

7. El-Gendi, M. (2024). *Cybersecurity: From information wars to cybercrimes.* Cairo, Egypt: Dar Al-Maaref.

8. Gamal El-Din, H. (2023). *The state and its national security in the era of artificial intelligence and its interconnections.* Cairo, Egypt: Dar Al-Maaref.

9. Idjir, A. (2024). Digital sovereignty in a globalized world: Challenges and stakes. *Journal of Legal and Political Studies*, 76.

10. *National Higher School of Artificial Intelligence*. (2024). Retrieved from https://www.ensia.edu.dz/ar/

11. Sadiq, A. M. (2008). *New media: Concepts, tools, and applications.* Cairo, Egypt: Dar Al-Shorouk for Publishing and Printing.

12. Senoussi, A. (2024). Digital sovereignty and technological independence between the challenges of national and international circumstances. *Algerian Journal of Law and Political Science*, 9.

13. Taqiyya , T., & Boubakr, R. (2024). Legal frameworks for enhancing state digital sovereignty in confronting potential negative uses of artificial intelligence. *Voice of Law Journal*, 137.