International Journal of Law and Jurisprudence
Volume 15 · Issue 2 · 2026 · Pages 2105–2113
e-ISSN 2255-1824 (Online) · revistaidj.com/IJLJ

STRENGTHENING CYBERSECURITY TO PROTECT ALGERIAN NATIONAL SECURITY: A LEGAL ANALYTICAL STUDY

Dr. Khaled Serbah*[1], Dr. El Hosseyn Feredj[2], Dr. Hamza Ababsa[3]

[1] Comparative Private Law, Faculty of Law and Political Science, University of Chlef, Algeria, Email: k.serbah@univ-chlef.dz
[2] Comparative Private Law, Faculty of Law and Political Science, University of Chlef, Algeria, Email: e.feredj@univ-chlef.dz
[3] Comparative Private Law, Faculty of Law and Political Science, University of Chlef, Algeria, Email: h.ababsa@univ-chlef.dz

Received: 1 July 2026 | **Accepted:** 10 September 2026 | **Published:** 1 November 2026

Abstract

Strengthening cybersecurity has become one of the principal issues that consistently arises whenever the question of a State's national security is addressed. In certain circumstances, it has become an imperative that brooks neither leniency nor delay, particularly in the contemporary era, marked by the enormous expansion of the digital environment and the resulting growth of crimes whose nature poses distinctive risks to national security. Algeria, as part of this world and in view of its international and regional standing, has not been immune to deliberate cyber threats directed primarily against its national security. The more Algeria has recognised the necessity of securing its national security and the more attention it has devoted to this matter, the more it has been prompted to act to establish the overall framework required to achieve national security. The effectiveness of this framework cannot be assessed without identifying the body of legislation that provides the tools for addressing and confronting such threats in an orderly and coordinated manner commensurate with the paramount importance of the subject, together with effective institutional and organisational bodies responsible for implementation and coordination. These elements are intended to harmonise efforts to establish cybersecurity for the Algerian State.

Keywords: digital environment; cybersecurity; national security; preventive measures; intervention and response measures.

Résumé :

Le renforcement de la cybersécurité est devenu l'une des questions fondamentales qui se posent inévitablement dès lors que l'on aborde la sécurité nationale d'un État. Dans certaines circonstances, il est devenu un impératif qui ne tolère ni laxisme ni retard, en particulier à l'époque contemporaine, marquée par l'expansion considérable de l'environnement numérique et par la recrudescence qui en découle de cybercriminalités dont la nature présente des risques singuliers pour la sécurité nationale. L'Algérie, faisant partie intégrante de ce monde et au vu de sa position internationale et régionale, n'a pas été épargnée par les cybermenaces délibérées dirigées principalement contre sa sécurité nationale. Plus l'Algérie a pris conscience de la nécessité de préserver sa sécurité nationale et plus elle y a accordé d'attention, plus elle a été incitée à agir pour mettre en place le cadre global requis pour l'atteinte de la sécurité nationale. L'efficacité de ce cadre ne saurait être évaluée sans l'identification de l'arsenal législatif fournissant les instruments nécessaires pour traiter et contrer ces menaces de manière ordonnée et coordonnée, à la mesure de l'importance capitale du sujet, ainsi que des organes institutionnels et organisationnels effectifs chargés de la mise en œuvre et de la coordination. Ces éléments visent à harmoniser les efforts en vue d'instaurer la cybersécurité pour l'État algérien.

Mots-clés: environnement numérique; cybersécurité; sécurité nationale; mesures préventives; mesures d'intervention et de riposte.

Introduction:

The issue of strengthening cybersecurity and protecting national security is a product of the technological revolution and the need to adapt to transformations aimed at modernising the means and methods through which the security of peoples is maintained. This is pursued by introducing information-system technologies based on the well-known convergence between information systems and communication systems, with a view to renewing various sectors, addressing shortcomings and remedying them, and ultimately reaching a stage at which public services can be delivered at the highest possible level of quality, alongside individuals' rising expectations concerning service standards. The benefits resulting from the transition to a digital environment cannot be denied.

Although the purpose of incorporating technology in its various forms into the operation of State institutions was to serve the public interest, the digital transformation has also been accompanied by difficulties that have caused direct and indirect harm to

the national security of States. These difficulties have consequently become among the most important issues of the present age, particularly in light of the effects of the unlawful exploitation of technology and the emergence of criminal activities associated with it.

Nevertheless, States throughout the world, whether rich or poor, have recognised the need to establish a global system for confronting cyber threats to State security, especially because such threats do not recognise political borders. This recognition has made it essential to combine efforts and diplomatic initiatives in a framework of joint action under the auspices of the United Nations, while taking due account of the distinctive nature of the issue as it affects States across the world in a fair and equitable manner, regardless of their respective positions. The objective is to establish a legal framework for a global system based on a set of principles, rules, indicators and international norms that can help States protect and safeguard their national security while also monitoring conduct in cyberspace.

Accordingly, Algeria faces the task of translating international policy on cybersecurity into an effective national policy. Conversely, any neglect, lack of vigilance or failure by the competent authorities to remain alert to the various forms of cyber threats may have serious repercussions for the recognised dimensions and aspects of national security. The effects of cyber threats on public affairs are no longer hidden from anyone. Like many other countries, Algeria has therefore followed the path adopted by numerous developed States, as strengthening national security has become one of their new priorities. As evidence of the political leadership's awareness of the scale of the problem and its potential escalation, this concern has been reflected in efforts to lay the foundations and establish the basic premises for regulating and controlling the digital environment, with a view to restoring it to a secure state. Algeria has thus established the general framework for a public policy in this field, which continues to develop steadily through the adoption of specific legal protections for prevention and response. A specialist observer will note the considerable legislative activity and the breadth of provisions covering the various areas in which threats are emerging. Given the multiple dimensions of cyberspace, the legislator has sought to address them progressively, in order to raise awareness of their danger to national security, prevent the harm associated with them and deter those responsible.

Significance of the Study:

The significance of this study derives from the importance of the subject it addresses, namely the requirements for strengthening cybersecurity to protect Algerian national security. The study contributes to the continued accumulation of knowledge on this subject and to the enrichment of the emerging research agenda in legal studies by integrating various legal approaches and foundational concepts. Its aim is to develop a comprehensive understanding that leaves no room for ambiguity or doubt regarding the issue under examination. More generally, the subject derives its importance and value from its focus on a matter of paramount importance: strengthening national security against cyber threats. These threats have become a major issue and an important dimension of humanity's future, as well as a central consideration in any comprehensive development plan and a primary concern of the Algerian State when formulating public policies.

Objectives of the Study:

The study seeks to deepen understanding of the role played by the Algerian State in strengthening national security against cyber threats by highlighting its position within legislative and institutional policy, taking the current situation as its point of departure. In response to the pressing need to identify the scope and limits of the subject, the study seeks to address the key issues necessary to achieve this objective.

Research Problem:

In light of the foregoing, the research problem may be formulated as follows:

To what extent have the legal determinants established to counter cyber threats enabled Algeria to attain a position that ensures the strengthening of its national security?

This study of the requirements for strengthening cybersecurity to protect Algerian national security is divided into two main sections, each addressing two principal themes. The first concerns the legal and technical requirements for strengthening cybersecurity; the second examines the achievement of cybersecurity and the imperative of providing both preventive and deterrent institutions. Through these sections, we have sought, to the greatest extent possible, to develop and discuss the subject despite its complexity and fluidity, with a view to producing a comprehensive study with distinct inputs and outputs.

1. Legal and Technical Requirements for Strengthening Cybersecurity

Amid the growing momentum of artificial intelligence and the enormous developments taking place in the digital environment, Algeria has endeavoured to avoid the potential adverse consequences of misuse, whether deliberate or unintentional. Among the most prominent manifestations of these risks, and the one that has most concerned States, are cyberattacks involving intrusions into information systems and the network-connected infrastructure of national networks, espionage and the creation of social instability. Algeria seeks to avoid this dilemma in order to protect its sovereignty and prevent external interference within its borders.

The greater the Algerian State's awareness and understanding of this issue, the stronger the impetus for it to take carefully considered steps to strengthen national security against cyber threats. This is reflected in the extensive legislative activity

undertaken by the Algerian legislator and the legal mechanisms (first subsection) and procedural and technical mechanisms (second subsection) that it has introduced to achieve cybersecurity and national security.

1.1 Legal Requirements for Achieving Cybersecurity and National Security

Cyberattacks in their various forms have become a devastating threat to States, preventing them from fully exercising their sovereignty. Cyberspace has also become a genuine battlefield between international powers, classified as a fifth domain of conflict after land, air, sea and outer space. Given the scale of its consequences, particularly in the field of security, and in order to protect both individuals and the State, the Algerian legislator has placed this issue among its priorities at the present stage, as have other States. Security approaches have accordingly been accompanied by legal frameworks that take account of the flexibility and complexity of cyberattacks.

1.1.1 Defining the Scope of Cybersecurity

A careful reading of Law No. 18-04 laying down the general rules relating to the postal service and electronic communications shows that the Algerian legislator expressly defined cybersecurity in precise terms as follows: “the set of tools, policies, security concepts, security mechanisms, guidelines, risk-management methods, activities, training, good practices and technological safeguards that may be used to protect electronic communications against any event that may compromise the availability, integrity or confidentiality of stored, processed or transmitted data.”[1]

In light of the foregoing, it may first be observed that the Algerian legislator defined cybersecurity in a manner consistent with international policy, particularly that promoted by the International Telecommunication Union in its report on telecommunications reform trends for 2010–2011. The definition was also clearly influenced by States that took the lead in confronting cyberattacks. In this respect, particular reference may be made to the European Union, which views cybersecurity as “the ability of an information system to resist intrusion attempts targeting data”. A more detailed definition was also provided by the United States Department of Defense, which described it as “all organisational measures necessary to ensure the protection of information in all its physical and electronic forms against various offences, including attacks, sabotage, espionage and incidents”.[2]

Furthermore, from a second perspective, a legal observer may conclude that the Algerian legislator’s definition does not differ fundamentally from the approaches adopted by other legislators, particularly with regard to the basic elements on which there is broad agreement. These elements are often described in terms of cyber power, meaning the ability to control and exercise command over the environment in which violations develop and proliferate, particularly through various electronic devices, computers and mobile phones. To secure national security in this respect, Algeria should possess the sources of cyber power, which are based on building an integrated and complex system comprising digital capabilities, population, economic capabilities, military and intelligence capabilities, and the ability to control or penetrate the capabilities of others and induce them to undertake specific actions.[3]

1.1.2 The Criminal Legislator’s Efforts to Define the Boundaries of Cyber Threats

The Algerian legislator’s engagement with cybersecurity as one of the priorities of the present stage cannot be understood separately from the early phase of its adoption. The legislator’s initial response was characterised by a determination to combat cyber violations without first setting out a comprehensive conception of their boundaries. Particular attention was given to the risks of disrupting public services, destroying or altering information, systematic espionage, and damaging assets and data. In other words, the rapid development of the phenomenon did not allow the Algerian legislator sufficient time to formulate a precise definition of cybersecurity or develop its strategies; rather, its overriding concern was to intervene immediately to confront the new forms of so-called soft warfare that had become an urgent priority.

On this basis, the Algerian legislator proceeded to define cybercrime in Law No. 09-04, which lays down specific rules for the prevention of and fight against offences related to information and communication technologies, as follows: “offences involving attacks on data-processing systems as defined in the Penal Code, and any other offence committed or facilitated through an information system or an electronic communications system”.[4]

In the same context, it should be noted that, at the outset of its efforts to establish cybersecurity, the legislator criminalised activities affecting computer systems by adapting the Penal Code through Law No. 04-15 to developments in information technology. It introduced Section 7 bis, entitled “Attacks on Automated Data-Processing Systems”, comprising Articles 394 bis to 394 bis 7. These provisions address several offences, including fraudulent input, deletion or modification of data in an automated data-processing system; intentional or fraudulent designing, researching, assembling, providing, publishing or trading in data stored, processed or transmitted through an information system; targeting national defence or bodies and institutions subject to public-law rules; and participation in a group or agreement formed for the purpose of preparation or planning through one or more material acts.[5]

In this context, the Algerian criminal legislator introduced a further measure under Law No. 06-22 as part of the process of securing cyberspace, intervening to tighten penalties and impose the maximum punishments for attempts to commit the misdemeanours provided for in relation to attacks on automated data-processing systems. This approach may be attributed to the connection between such offences and the national economy, as well as their widespread commission compared with other types of crime. The legislator’s legal efforts to manage this phenomenon did not stop there. In Law No. 16-02, amending and supplementing the Penal Code, the criminal legislator also addressed the spread of the use of information and communication

technologies to commit, direct, prepare for, participate in or train for terrorist acts, with a view to preventing such conduct and punishing those responsible. The law also specifically addressed internet service providers and the technical measures required, in view of the seriousness of the offences defined by law, to remove content made available for consultation and access, thereby avoiding its undesirable consequences.[6,7]

2.1 Attempting to Establish Procedural and Technical Requirements for Cybersecurity

Achieving the desired level of cybersecurity and confronting criminal acts of a distinctive nature through a well-considered legal approach by the legislator is of great importance. However, this is insufficient unless accompanied by technical and procedural measures that ensure effectiveness and demonstrate a genuine commitment to establishing cybersecurity in Algeria.

At the outset, it is necessary to highlight the growing procedural and technical awareness demonstrated by the Algerian legislator, as well as the distinction between these measures and traditional procedures in the effort to secure cyberspace. This approach is attributable to the nature of the virtual digital environment and to the technical specificity of the means most closely associated with it, as well as to its distinctive characteristics and its separation from traditional forms of crime. Investigation and evidence-gathering in cybercrime cases require special procedural and technical operations adapted to crime scenes that vary in form and whose boundaries are not always known. Such measures are necessary to avoid what has come to be described as the “cybercrime crisis”.[8]

A review of the relevant legal framework shows that the legislator has separately established specific procedural requirements intended to prevent cyberattacks and mitigate their serious consequences for State sovereignty. These include the investigation and inquiry procedures applicable to cybercrime and the new measures introduced by Law No. 06-22. Among the foremost of these measures is the obligation of secrecy and confidentiality during preliminary inquiries and investigations, imposed on every person involved in those procedures in order to safeguard public order, subject to the applicable penalties. The Public Prosecution alone is authorised to inform public opinion, so as to prevent the dissemination of misleading information without an assessment of the accusations levelled against the persons concerned.[9]

Where necessary to preserve cybersecurity, procedural measures may be carried out under the direct supervision of the Public Prosecutor or the investigating judge, depending on whether an investigation has been opened. These measures may include intercepting correspondence through wired and wireless communications, as well as making the technical arrangements required to record sound and capture images in a confidential and specific manner, whether the persons concerned are one or several, and whether the locations are private or public.[10]

In a related context, and to address the technical aspects of the aforementioned procedural operations, the legislator authorised the Public Prosecutor or an authorised judicial police officer, as well as the investigating judge or delegated judicial police officers, to requisition any qualified officer employed by a public or private service, body or unit specialising in wired and wireless communications. It should be noted that the implementation of these technical operations may permit entry into residential premises or other places even outside the legally prescribed hours, whether or not the persons entitled to control those premises are aware of or consent to such entry.[11]

2. Achieving Cybersecurity through Institutions Operating at the National and International Levels

Legal intervention aimed at strengthening legal certainty in cyberspace is essential. Nevertheless, it is not sufficient to ensure effective cybersecurity, particularly in view of the complexity and distinctive characteristics of this field and its potentially adverse effects on national security. Legal solutions must therefore be accompanied by structural and institutional solutions, together with the pressing need for international engagement through judicial cooperation and mutual legal assistance.

2.1 Supervisory Institutions Supporting the Establishment of Cybersecurity

Whatever the reality of the manifestations that undermine national security in virtual space, the digital transformation has, on the other hand, made it possible to update and develop the means of confronting and limiting such threats. Specialised bodies have moved into this same environment in order to regulate conditions and deploy specific mechanisms to prevent or deter any unlawful conduct.

Notwithstanding the foregoing, cybersecurity has a narrower scope in terms of the protection it provides to digital activities generally, particularly offences affecting national security in cyberspace. In Algeria, responsibility for this field rests specifically with specialised bodies entrusted exclusively with its regulation. More than one actor is involved in this task, with the independent administrative authority playing the most significant role. The Algerian legislator has made considerable progress in providing a comprehensive legislative framework designed to ensure security in the conduct of various digital activities, including through the establishment of more than one independent administrative authority, each entrusted with specialised functions.

2.1.1 The Regulatory Authority for Post and Electronic Communications (ARPCE)

The Regulatory Authority for Post and Electronic Communications was first established as an independent authority under Law No. 2000-03 laying down the general rules relating to the postal service and telecommunications. That legislative framework was subsequently repealed by Law No. 18-04 laying down the general rules relating to the postal service and electronic communications, which further strengthened the role of this independent body in parallel with the technological revolution

affecting Algeria's postal and telecommunications sector. The legislator provided that: "An independent regulatory authority for post and electronic communications, enjoying legal personality and financial autonomy, is hereby established and shall be referred to in this text as the 'Regulatory Authority'. Its headquarters shall be in the city of Algiers." The administrative nature of this authority is apparent from Article 22 of the same law, which implicitly recognises that nature by providing that its decisions may be challenged before the Council of State.[12,13]

On behalf of the State, the Regulatory Authority is responsible for ensuring the proper functioning and security of the postal and electronic communications markets. To this end, it performs a number of tasks specified by the legislator in Law No. 18-04. Among the most important is ensuring effective and fair competition in the postal and electronic communications sectors through decisions intended to promote both markets and restore competition. Its responsibilities also include allocating frequencies to operators of electronic communications networks open to the public and monitoring their use in accordance with the principle of non-discrimination. In addition, it is responsible for issuing general authorisations relating to the establishment and operation of electronic communications networks and the provision of the corresponding services, as well as authorisations for private networks.[14]

Furthermore, the Regulatory Authority is responsible for approving postal and electronic communications equipment in accordance with the standards established by the applicable regulations. In order to safeguard the State's cybersecurity, it also monitors whether postal and electronic communications operators comply with the relevant legal and regulatory provisions, including those relating to cybersecurity. It additionally oversees the protection of subscribers' rights in connection with electronic communications services and handles complaints submitted by subscribers by adopting the necessary arrangements. The Authority is also required to publish useful information intended to protect subscribers' rights and to conduct awareness-raising and information campaigns whenever circumstances so require.[15,16]

2.1.2 The National Authority for the Protection of Personal Data

The Algerian legislator sought to enact Law No. 18-07 on the protection of natural persons in the processing of personal data. In the context of cybersecurity and national security, this law provides for the establishment of an independent administrative authority responsible for protecting personal data, placed under the President of the Republic and enjoying legal personality as well as financial and administrative autonomy.[17]

According to Article 23 of the same law, the National Authority consists of thirteen members appointed by presidential decree for a renewable five-year term. It comprises three experts in the Authority's field of activity, including its president, selected by the President of the Republic; three judges drawn from among the judges of the Supreme Court or the Council of State and proposed by the High Council of the Judiciary; and one member from each chamber of Parliament, selected by the relevant chamber president after consultation with the chairs of the parliamentary groups. It also includes the following representatives:[18]

a. A representative of the National Human Rights Council;
b. A representative of the Minister of National Defence;
c. A representative of the Minister of Foreign Affairs;
d. A representative of the minister responsible for the interior;
e. A representative of the Minister of Justice, Keeper of the Seals;
f. A representative of the minister responsible for post, telecommunications and digital technologies;
g. A representative of the minister responsible for health;
h. A representative of the Minister of Labour, Employment and Social Security.

The National Authority is entrusted with highly sensitive responsibilities because of their connection with the protection of public order and public morals in the field of communications and electronic transactions. Its functions include:[19]

a. Granting authorisations and receiving declarations relating to the processing of personal data;
b. Authorising the transfer of personal data abroad, subject to specified conditions;
c. Informing the data subjects and the persons responsible for processing of their rights and obligations;
d. Receiving complaints, appeals and objections relating to the application of personal-data-processing rules and informing the persons concerned of the outcome;
e. Ordering the changes necessary to protect personal data undergoing processing;
f. Ordering the removal, blocking or destruction of data;
g. Establishing the standards required in the field of personal-data processing;
h. Preparing an annual report on its activities and submitting it to the President of the Republic.

2.2 Supervisory Institutions Responsible for Ensuring Cybersecurity

Since the challenges posed by cyber threats are global in nature and are not confined by concepts associated with the recognition of geographical borders, while their point of origin lies in the virtual digital environment, States can safeguard their national security only through supervisory institutions that remain continuously vigilant in establishing cybersecurity as an

imperative rather than an optional choice.

2.2.1 Establishing Specialised Judicial and Security Bodies

In view of the limited capacity of ordinary courts and their insufficient specialisation in addressing cybercrime, which poses a serious threat to national security and exploits the rapid development of electronic means and cyberspace to modernise criminal activity, the Algerian legislator adopted the idea of judicial specialisation through the amendments to the Code of Criminal Procedure. It did so by establishing specialised criminal poles in order to activate a judicial system capable of keeping pace with the development of criminal conduct.

In this regard, moving towards specialised justice is one indicator of a sound judicial system. In an effort to keep pace with increasingly complex forms of cybercrime and to protect this vital sector, the Algerian legislator established specialised criminal judicial bodies. This approach is grounded, on the one hand, in the constitutional provision assigning Parliament the authority to legislate on rules relating to the establishment of judicial bodies and, on the other, in the President of the Republic's power to legislate by ordinance in urgent matters. Specialised criminal poles were consequently established to combat cybercrime.[20]

The establishment of courts with extended jurisdiction was one of the outcomes of the modernisation and reform of the justice system and its performance, and of the State's commitment to contain all acts affecting the national interests of society, particularly those connected with cybersecurity. In this context, reference should be made to Law No. 04/14, which introduced amendments to the Code of Criminal Procedure. Among other matters, it provides for the possibility of extending the territorial jurisdiction of the Public Prosecutor, the investigating judge and the court to the jurisdiction of other courts distributed across the eastern, western, central and southern regions of the country when certain offences are involved. These include offences affecting automated data-processing systems, which are covered as a matter of subject-matter jurisdiction.[21]

2.2.2 The Need for the Military and Security Services to Keep Pace with Cyber Threats

Starting from the constitutional framework, and particularly paragraph 21 of the Preamble to the Constitution, the leading role of the Algerian armed forces in deterring and repelling any potential threat to national sovereignty becomes evident, whatever its form, including cyberattacks. The constitutional founder emphasises the need for the People's National Army to maintain the required level of readiness and to develop its professionalism in a manner consistent with the evolution of new forms of defence, which require modernisation and adaptation to all threats affecting territorial integrity. This has prompted the military services to take these developments into account in order to achieve the readiness necessary to perform the role assigned to them by the Constitution. This involves moving towards a new level of preparedness in recruitment, training and defence of the integrity of the homeland against any potential cyber aggression. The development sought by the People's National Army is therefore based on a firm conviction that the concept of national security is evolving, alongside changes in the international, regional and domestic environment.[22]

In accordance with this constitutional context, and in order to give effect to it, a Cyber Defence and Systems Security Monitoring Service was established within the Intelligence and Preparation Directorate of the General Staff of the People's National Army. Its purpose is to ensure the protection of systems and various vital facilities through the provision of the necessary capabilities. This involves organisational integration of cyber-defence activities, the development of a technically skilled and continuously vigilant human resource base, and the preparation of an appropriate legal environment for defence, response, awareness-raising and prevention of potential threats. It also entails the need to anticipate and develop a defensive policy based primarily on research and development structures.[23]

Moreover, a careful reading of the Joint Ministerial Order concerning the departments, services and regional laboratories of the National Institute for Criminalistics and Criminology reveals its alignment with the State's policy of confronting new threats emerging in the digital sphere at the international level. Within the Institute's organisational structure, a department is specifically devoted to technical matters. It includes a service specialising in the examination of technological evidence, which, at the request of the competent judicial authorities, undertakes the analysis and preparation of reports concerning digital material evidence, computer-related offences and voice recordings, as well as image and signal processing and the examination of mobile phones. To enable it to perform these functions, three specialised laboratories have been provided for forensic audio analysis, digital evidence and computer crime, and mobile-phone examination.[24]

2.2.3 The Need for International Cyber Cooperation

At the outset, it must be recognised that a State's ability to provide the necessary protection for its own information systems independently is extremely difficult, if not impossible. This is attributable to several factors, foremost among them the enormous and flexible development of the digital environment, the growing number and expertise of individuals capable of engaging in hostile activity against a State, and the relative novelty of information technologies, together with the limited proficiency of many States in this field. It is therefore essential to apply the principal international standards for combating crime, particularly those relating to cooperation in procedural matters, in order to facilitate the efforts of other States to confront any breach of their national security. Algeria has joined this effort and has given effect to it through several forms of cooperation.

Given the adaptability of cybercrime and the ability of perpetrators to disperse or destroy evidence by exploiting advances in scientific research, criminal justice must also benefit from these developments in order to collect the relevant evidence, but through cooperation and concerted efforts. On this basis, international judicial cooperation is undertaken in accordance with the

United Nations Model Treaty on Mutual Assistance in Criminal Matters and the Model Law derived from it in 2008. These instruments provide for the exchange of information, data and evidentiary material requested by foreign judicial authorities where a natural or legal person is suspected or accused of an offence committed through a computer or computer data-storage medium in that person's possession or control. They also cover relevant information held by or available to a service provider. Given the adverse effects that such offences may have on a State's national security, urgent action may be required; in such circumstances, a sufficient amount of information and data may be disclosed to the requesting State in advance, where necessary.[25]

In light of the foregoing, international letters rogatory constitute an important and prominent link in establishing international cooperation. They involve a national court, through the national judge before whom the case is pending, issuing a commission to a foreign court, represented by a foreign judge, to conduct certain investigative operations and other judicial procedures for the purpose of obtaining evidence located abroad. This is necessary where the national court cannot undertake those measures itself because of geographical distance. To ensure the effective use of letters rogatory, States seek to intensify judicial cooperation in combating emerging forms of crime through consultation meetings, exchanges of field visits and the organisation of training courses to benefit from technical expertise. On the other hand, such cooperation may sometimes encounter the obstacle of national sovereignty, which can prevent implementation and, consequently, impede the extradition of offenders.[26]

It should also be noted that the Algerian legislator has demonstrated considerable interest in this judicial procedure, which essentially reflects judicial cooperation in support of the proper administration of justice. Algeria has joined certain relevant arrangements and concluded others. This commitment is reflected in the inclusion of letters rogatory in the Code of Civil and Administrative Procedure under Law No. 08-09, Articles 108 to 124. The legislator recognises that disputes of an international nature have distinctive characteristics that differentiate them from domestic disputes, particularly because the national court cannot, on its own, complete all investigative procedures. Ensuring cybersecurity is one such field in which recourse to judicial assistance and letters rogatory may be required.

Conclusion:

At the conclusion of this research study entitled "Strengthening Cybersecurity to Protect Algerian National Security: A Legal Analytical Study", we have reached the following findings:

1. Cyberattacks, in their various forms, have become a real threat to the national security of States, undermining their ability to exercise their sovereignty fully;
2. Cyberattacks involving intrusions into information systems and national network-connected infrastructure, espionage and the creation of social instability constitute a dilemma that Algeria has been compelled to avoid in order to protect its sovereignty and national security;
3. The Algerian legislator has engaged with cybersecurity and treated it as one of the priorities of the present stage. The digital transformation has made it possible to update and develop the means of confronting and limiting such threats;
4. The first step was the need to develop legal, procedural and technical approaches that take account of the flexibility and complexity of cyberattacks. This adaptation of concepts is attributable to the nature of the virtual digital environment, the technical characteristics that distinguish it and its relative autonomy from traditional forms of crime;
5. Legal regulation intended to establish legal certainty in cyberspace is not, by itself, sufficient to ensure effective cybersecurity, given the complexity and distinctive characteristics of this field and its adverse effects on national security. It must therefore be accompanied by specialised structural and institutional solutions;
6. The challenges posed by cyber threats are global in nature and require the adoption of international principles, particularly those relating to international judicial and security cooperation. Algeria has engaged in and implemented such cooperation.

The requirements for strengthening cybersecurity to protect Algerian national security still require further assessment and development in light of this research. Accordingly, the following proposals are put forward:

1. The issue of cyber threats to national security must receive genuine and sustained attention, particularly through the development of a forward-looking vision that enables a proper understanding of these threats, raises the necessary level of awareness, facilitates their early detection and supports an effective response;
2. The seriousness of the issue requires an effective legislative commitment that keeps pace with and matches the effects of cyber threats on national security in all its dimensions;
3. There is an imperative need to develop human capital equipped with a cybersecurity culture, particularly through education and awareness-raising, the involvement of the media in all its forms and the participation of civil society;
4. Qualitative security-enhancement efforts should be completed through specialised training in the best available technologies, effective tactical practices and rapid, secure procedures;
5. Active diplomatic engagement in the field of cybersecurity should continue, with the benefits of exchanging expertise, information and visits used to help Algeria attain the level of States that enjoy a high degree of cyber security.

3. List of Sources and References

Sources:

Presidential Decree No. 20/422 and Presidential Decree No. 20/442 relating to the 2020 constitutional amendment, Official Gazette of the People's Democratic Republic of Algeria, No. 82, 30 December 2020. The decree numbers are reproduced as stated in the source manuscript.

Law No. 18-04 of 10 May 2018 laying down the general rules relating to the postal service and electronic communications, Official Gazette of the People's Democratic Republic of Algeria, No. 27, 13 May 2018.

Law No. 09-04 of 5 August 2009 laying down specific rules for the prevention of and fight against offences related to information and communication technologies, Official Gazette of the People's Democratic Republic of Algeria, No. 47, 16 August 2009.

Law No. 04-15 of 10 November 2004 amending and supplementing Ordinance No. 66-156 containing the Penal Code, Official Gazette of the People's Democratic Republic of Algeria, No. 71, 10 November 2004; as amended and supplemented by Law No. 06-23 of 20 December 2006, Official Gazette, No. 84, 24 December 2006, and by Law No. 16-02 of 19 June 2016 supplementing Ordinance No. 66-156, Official Gazette, No. 37, 22 June 2016.

Law No. 06-22 of 20 December 2006 amending and supplementing Ordinance No. 66-155 containing the Code of Criminal Procedure, Official Gazette, No. 84, 24 December 2006.

Law No. 2000-03 of 5 August 2000 laying down the general rules relating to the postal service and telecommunications, Official Gazette, No. 45, 6 August 2000.

Law No. 18-04 of 10 May 2018 laying down the general rules relating to the postal service and electronic communications, Official Gazette, No. 27, 13 May 2018.

Law No. 18-07 of 10 June 2018 on the protection of natural persons in the processing of personal data, Official Gazette, No. 34, 10 June 2018.

Joint Ministerial Order of 14 April 2007 concerning the organisation of the departments, services and regional laboratories of the National Institute for Criminalistics and Criminology, Official Gazette, No. 36, 3 June 2007.

Academic References:

University Dissertations:

Al-Sha'ar, Khaled Ali Nazzal. Criminal Investigation in Cybercrime. PhD dissertation, Faculty of Law, Mansoura University, Egypt, n.d.

Journal Articles:

Basmaïl, Abdelkrim. "The Impact of Cyberspace on National Security." Journal of Research and Studies 19, no. 1 (2022).

Tariaa, Nouara. "The Constitutional Basis for the Role of the People's National Army in Protecting Algerian National Security." Journal of World Politics 6, no. 1 (2022).

Al-Samhan, Moni Abdullah. "Requirements for Achieving Cybersecurity for Management Information Systems at King Saud University." Journal of the Faculty of Education, no. 111 (2020).

Kamal, Soumia. "Letters Rogatory." Journal of Legal and Political Studies 1, no. 2 (2015).

Laarmani, Asia. "International Cooperation in Combating Cybercrime: Algeria as a Case Study." Algerian Journal of Political Science and International Relations 5, no. 2 (2012).

Web Sources:

United Nations Office on Drugs and Crime. Model Law on Mutual Assistance in Criminal Matters. February 2008. https://www.unodc.org/documents/corruption/Publications/Model_Law_MLA_AR.pdf.

Notes

[1] — Law No. 18-04 of 10 May 2018 laying down the general rules relating to the postal service and electronic communications, Official Gazette of the People's Democratic Republic of Algeria, No. 27, 13 May 2018, Article 10(3).

[2] — Moni Abdullah Al-Samhan, "Requirements for Achieving Cybersecurity for Management Information Systems at King Saud University," Journal of the Faculty of Education, No. 111 (2020), p. 10.

[3] — Abdelkrim Basmaïl, "The Impact of Cyberspace on National Security," Journal of Research and Studies, vol. 19, no. 1 (2022), pp. 150–151.

[4] — Law No. 09-04 of 5 August 2009 laying down specific rules for the prevention of and fight against offences related to information and communication technologies, Official Gazette of the People's Democratic Republic of Algeria, No. 47, 16 August 2009, Article 2(a).

[5] — Law No. 04-15 of 10 November 2004 amending and supplementing Ordinance No. 66-156 containing the Penal Code, Official Gazette of the People's Democratic Republic of Algeria, No. 71, 10 November 2004.

[6] — Law No. 06-23 of 20 December 2006 amending and supplementing Ordinance No. 66-156 containing the Penal Code, Official Gazette, No. 84, 24 December 2006.

[7] — Law No. 16-02 supplementing Ordinance No. 66-156 of 19 June 2016 containing the Penal Code, Official Gazette, No. 37, 22 June 2016, Articles 87 bis 11 and 394 bis 8.

[8] — Khaled Ali Nazzal Al-Sha‘ar, Criminal Investigation in Cybercrime, PhD dissertation, Faculty of Law, Mansoura University, Egypt, n.d., pp. 6–7.

[9] — Law No. 06-22 of 20 December 2006 amending and supplementing Ordinance No. 66-155 containing the Code of Criminal Procedure, Official Gazette, No. 84, 24 December 2006, Article 5.

[10] — Ibid., Article 65 bis 5, paragraphs 1–3.

[11] — Ibid., Article 65 bis 5, paragraph 4, and Article 65 bis 8.

[12] — Law No. 2000-03 of 5 August 2000 laying down the general rules relating to the postal service and telecommunications, Official Gazette, No. 45, 6 August 2000.

[13] — Law No. 18-04 of 10 May 2018 laying down the general rules relating to the postal service and electronic communications, Official Gazette, No. 27, 13 May 2018, Article 11.

[14] — Ibid., Article 13, paragraphs 1–4.

[15] — Ibid., Article 13, paragraphs 7, 9 and 10.

[16] — Ibid., Article 13, paragraphs 16–18.

[17] — Law No. 18-07 of 10 June 2018 on the protection of natural persons in the processing of personal data, Official Gazette, No. 34, 10 June 2018, Article 22.

[18] — Ibid., Article 23.

[19] — Ibid., Article 25.

[20] — Presidential Decree No. 20/422 and Presidential Decree No. 20/442 relating to the 2020 constitutional amendment, Official Gazette of the People’s Democratic Republic of Algeria, No. 82, 30 December 2020. The decree numbers are reproduced as they appear in the source manuscript.

[21] — Law No. 04/14 amending the Code of Criminal Procedure, cited in the source manuscript with reference to Articles 37, 40 and 329. The source does not provide further publication details in this footnote.

[22] — Nouara Tariaa, “The Constitutional Basis for the Role of the People’s National Army in Protecting Algerian National Security,” Journal of World Politics, vol. 6, no. 1 (2022), pp. 1082–1083.

[23] — Asia Laarmani, “International Cooperation in Combating Cybercrime: Algeria as a Case Study,” Algerian Journal of Political Science and International Relations, vol. 5, no. 2 (2012), p. 73.

[24] — Joint Ministerial Order of 14 April 2007 concerning the organisation of the departments, services and regional laboratories of the National Institute for Criminalistics and Criminology, Official Gazette, No. 36, 3 June 2007, Article 5.

[25] — United Nations Office on Drugs and Crime, Model Law on Mutual Assistance in Criminal Matters (February 2008), pp. 21–22, Articles 28–29, accessed 13 January 2025, 11:11, https://www.unodc.org/documents/corruption/Publications/Model_Law_MLA_AR.pdf.

[26] — Laarmani, “International Cooperation in Combating Cybercrime,” cited above, p. 84.