Vol. 05, No. 2, pp-281-292| december 2025
DOI: https:// DOI 10.34118/jskp.v5i02.4446

Article history (leave this part):
Submission date: 30.08-2024
Acceptance date: 15-12-2025
Available online: 27-12-2025
Keywords:
Cybercrime; Cyber Security; National Security; Algerian Legislation; Legal Strategy
;**Funding:**
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Competing interest:
The author(s) have declared that no **competing interests**exist.
Cite as (leave this part):
HananAbufaresElkhimry;. (2024).Title.Journal of Science and Knowledge Horizons: 4(1), 283-293. https://doi.org/10.34118/jskp.v2i02.2727

Journal of Science and Knowledge Horizons
ISSN 2800-1273-EISSN 2830-8379

The Algerian Legislator's Strategy in Addressing Cyber Crimes That Threaten Its Cyber Security

*1*hadfi tadjeddine*
PhD in Urban Sociology, University of El Oued - Algeria
hadfi-tadjeddine@univ-eloued.dz
2-benazza said
Benazzasaid2019@gmail.com
PhD in Educational Sociology, University of El Oued – Algeria
https://orcid.org/0009-0001-2740-8001
https://orcid.org/0009-0001-6614-9874

Abstract:

This study aims to explore the importance of the strategy developed by the Algerian legislator to confront cyber crimes that threaten its cyber Security.

Thèse crimes have had significant repercussions on national security, as Algeria's strategic location renders it an open area for various directions and a vital hub in the Maghreb, Mediterranean, and Africa. This situation has led to numerous breaches and espionage, affecting the safety of individuals, making their lives and privacy vulnerable to extortion, whether they are officials or ordinary citizens. Furthermore, espionage and threats have not spared governmental, security, and military institutions in the country, prompting urgent calls for the re-establishment of technical barriers to prevent these violations and attacks that impact national security. Therefore, we pose the following question: What is the legal strategy devised by the Algerian legislator to address the threats and risks of cybercrimes?

hadfitadjeddine

Introduction:

The international community witnessed a tremendous technological revolution in the mid-20th century, which positively impacted the lives of individuals and nations. However, on the flip side, the misuse of information systems in cyberspace has led to various crimes and threats employing advanced technical methods, affecting many individuals and institutions in all their material and electronic forms, such as espionage, sabotage, threats, and aggressive attacks in a world that is witnessing rapid digital transformation. This includes espionage against national and international security. Given Algeria's strategic location, it has also faced cyber threats from external countries aiming to undermine its security and disrupt its stability, alongside piracy related to crime, espionage, and sabotage, with alarming figures regarding the numerous threats to cyber security using advanced tools. These attacks and threats result in considerable material and moral losses. To address such violations and breaches, the Algerian government has established a strict strategy to protect its information system, ensure its security, and effectively respond to cyber incidents through investigation, assistance, and regular awareness campaigns. This involves utilizing various laws and frameworks within the cyber security strategy, which primarily focuses on erecting technical barriers and walls to prevent such attacks, thereby controlling surveillance systems to protect the information systems of institutions and individuals. This endeavor positions the Algerian state as a guardian of securing its information systems, especially critical ones. Based on this framework, we will address the issue through the following question : What is the legal strategy established by the Algerian legislator to confront cyber security threats and their risks ?

- Consequently, in this study, we will explore the topic of cyber security in general by addressing the following elements: characteristics of cybercrimes, cyber criminality, motives behind cyber criminality, dimensions of cyber security, significant means of cybercrime threats, and the prominent cybercrime threats facing Algeria. Finally, we will discuss the Algerian state's strategy in confronting cybercrimes and their threats.

1.Defining Concepts :

1.1 The Concept of Cyber Security in Brief:

Cyber security is defined as a set of technical and organizational measures used to protect electronic systems and networks from extreme cyber threats and attacks.

1.2 The Concept of Cyber Criminality:

Cyber criminality is defined as the act wherein an individual aims to sabotage and disrupt the communication networks of computing components, regardless of whether they are related to individuals or institutions, whether material or mora. (Al-Shawabkeh, 2011, p. 9)

. It is characterized as "an unlawful act committed using a computer through electronic devices, which results in harm to individuals or institutions, achieved by accessing the information systems that characterize each one." (Khal, p. 45)

Legally, it is recognized as the act of performing or omitting a deed with criminal intent to harm any legal interest protected by law, which criminalizes and penalizes it under various provisions.

The Algerian legislator defined it in Article 01 of Law No. 09-04 as "the infringement of automated data processing systems." Furthermore, the legislator has also defined it as "crimes affecting the automated data processing systems specified in the Penal Code and any other crime perpetrated or facilitated through an information system or electronic communication systems as detailed in Law No. 04-09, which includes the special provisions concerning the prevention and combating of crimes related to information and communication technologies" (raàuf, 2011, p. 42)

2,Characteristics of Cyber Crimes:

2.1 **Hidden Crimes:** These crimes are difficult to detect due to the victim's limited technical capability on one side and the advanced technical and scientific expertise of the criminal on the other.

2.2 **Fast-Executing Crimes:** They may not require significant preparation time before execution, and often, their commission occurs within a fraction of a second.

2.3 **Remote Crimes:** The perpetrator can commit the crime while being far from the victim, even in different countries.

2.4 **Soft Crimes:** These crimes do not involve violence or physical exertion, in contrast to traditional crimes. (QARAAN, 2017, p. 8)

2.5 **Transnational Crimes:** These crimes have no geographic boundaries, connected to the world through a unified internet network.

2.6 **Crimes Difficult to Prove:** These are crimes that cannot be easily proven and are challenging to confine to a specific location as they leave no trace and are not visible to the naked eye. This Is due to several reasons :

- No evidence is left by the criminal after the crime is committed.
- They rely on exceptional intelligence when carried out.
- They require technical expertise that traditional investigators may struggle to handle.
- They depend on deception in their execution, obscuring the identities of the perpetrators.
- There is considerable difficulty in preserving any technical evidence related to these crimes. (Al-Qaraan, 2017, p. 11)

3. Motivations for Cyber Crime:

Cyber criminals often exhibit high skill levels when committing cyber offenses. They rely on mental capabilities, cleverness, and an understanding of cyber methods to destroy programs and bypass security barriers. The primary motivation for many cyber criminals appears to be financial gain, often resorting to illegal methods due to unemployment. Additionally, motives may include ideological or political reasons, or personal reasons such as an employee seeking revenge against a company that dismissed them, or engaging in espionage and violating the privacy of individuals or entities. Cyber criminals often exhibit high skill levels when committing cyber offenses. They rely on mental capabilities, cleverness, and an understanding of cyber methods to destroy programs and bypass security barriers. The primary motivation for many cyber criminals appears to be financial gain, often resorting to illegal methods due to unemployment. Additionally, motives may include ideological or political reasons, or personal reasons such as an employee seeking revenge against a company that dismissed them, or engaging in espionage and violating the privacy of individuals or entities. (Al-Qaraan, 2017, p. 14)

4. Dimensions of Cyber Security:

There are various dimensions of cyber security, which we can classify as follows:

4.1 **Legal Dimension :** Laurent Gisel, a legal advisor to the International Committee of the Red Cross, emphasized that Article 36 of the 1977 Protocol requires states to manufacture new weapons in accordance with international laws. However, there are general ethical and humanitarian guidelines that must be adhered to. Leaks revealed that the U.S. government spent substantial amounts on cyber operations in 2011, and over 130 countries announced the establishment of legal departments specifically to address cyber threats. (Al-Majdoub, 2014, p. 58)

4.2 **Economic Dimension :** This involves protecting economic resources and avoiding their loss, as institutions strive to shield their economic assets from damage caused by inadequate security and the risk of attacks or breaches that could diminish the economic value of any institution or nation. (Al-Awadi, 2016, p. 6)

4.3 **Social Dimension:** A report by the Social Are We organization indicates that approximately 2.5 billion people, or 35% of the world's population, use the internet. It plays a significant role in enabling citizens to express their opinions and aspirations in various domains. However, it also poses threats such as terrorism, the spread of extremist ideologies, youth recruitment, and the promotion of illicit trafficking.

4.4 **Political Dimension:** This dimension involves the state's responsibility and sovereignty in achieving cyber security, requiring comprehensive efforts. These efforts should not be limited to supporting research and development but must also enhance security culture, implement strategies for prevention and reporting, promote information sharing, and raise awareness of best practices and risk management. (Hamdoun, 2006, p. 15)

4.5 **Military Dimension:** The early development of the internet occurred in a military environment before extending to academic and research settings that contributed to military capabilities and scientific achievements. The dangers of cyber-attacks manifest as espionage, theft, and breaches, potentially leading to tangible outcomes such as the outbreak of armed conflicts. (Jbour, 2012, p. 16)

5. Means of Cyber Crime Threats:

5.1 **Technical and Informational Espionage:** These are significant weapons in cyber warfare that threaten nations and include various forms such as spying on

information from computers, satellites, and mobile phones. (Abd El-Sadiq, 2017, p. 2)

5.2 **Electronic Hacking:** This cybercrime involves creating a system or program to seize and destroy adversarial information, corrupting the computer and automated systems to gain superiority in security, military, economic, and political aspects. (Al-Shahri, p. 2024)

5.3 **Cyber Piracy:** This is a lethal weapon in the digital domain, involving modern electronic conflict techniques, relying on recruiting skilled individual's adept in computers and technical systems to exploit technological systems, commonly referred to as "hackers." (Jaloud, 2013, p. 111)

5.4 **Silent Messages :** These are technical programs used in fourth and fifth-generation mobile phones, sent without the owner's knowledge, assisting in accurately determining their location.

6. **Social Media Networks:** These are digital platforms that connect individuals and communities across various fields such as work, religion, and more, encompassing different age, social, economic, cultural, and educational categories, playing a significant role in online technological conflicts known as cyber-crimes. (16. Jaloud, 2013, p. 116)

6.1 **Electrostatic Bags:** This military technology consists of small devices that generate powerful electromagnetic pulses used to disrupt electronic units in any system or transmission station, leading to a loss of their scientific, productive, and operational capabilities.

6.2 **Nanotechnology Weapons:** These involve the design of very precise devices in the military domain that infiltrate computer systems and technologies, used for rapidly destroying informational infrastructure, akin to the functioning of viruses through what are known as digital microbes.

7. **Major Cyber Crime Threats Facing Algeria:**

7.1 **Political Threats:** Security studies distinguish between system security and community security. Authoritarian states focus on protecting the system, while civil states seek to improve democratic principles. The system may pose a threat to society during crises, necessitating security measures that could negatively impact community safety (Al-Khalfi, 2024, p. 9)

7.2 **Social Threats:** The effects of globalization have rendered these issues a genuine criminal threat to national security. The aspirations of societal projects indeed challenge social and cultural security, where identity and nationality are

often exploited for political purposes by both ruling elites and opposition forces. Negative engagement with these components leads to the failure of societal projects and hinders efforts to modernize Algerian security and society to protect individuals, institutions, and the state from cybercrime threats.

7.3 **Economic Threats:** Economic challenges manifest in Algeria's lack of revenue diversification and high reliance on the oil sector. If Algeria continues exporting oil at this pace, there may be little left for export within a quarter of a century, highlighting a gap in the economic strategy to secure the future of upcoming generations.

7.4 **Technological Threats:** In terms of technological threats, rapid advancements pose risks to Algeria's national security, affecting both institutions and individuals. These threats include crimes related to hostile websites, particularly political sites that may serve as sources for damaging news, creating a rift between the political system and citizens.) Zayani S(2014 ،.

8. Major Cyber Crimes Experienced by Algeria:

8.1 **Cyber Terrorism:** This is considered one of the primary threats and crimes facing Algerian security in the modern technological era, where social media and websites serve as platforms for spreading extremist and violent ideologies. Cyber terrorism includes various risks such as threats of violence, sabotage, and intimidation using electronic means to harm individuals and society as a whole. (Marzouq, 2011, p. 67)

8.2 **Cyber Piracy:** Algeria recorded over 900 electronic crimes in 2017, according to the Prevention and Combat of Cyber Crime Center within the National Gendarmerie. These crimes include violations of individuals' rights, threats and extortion, terrorism-related defamation, data and computer system piracy, identity theft, and enticing minors into prostitution. The most critical electronic threats include service disruption, destruction or alteration of information, and network espionage. Consequently, Algeria reported over 900 electronic crimes in 2017 as announced by the Cyber Crime Prevention and Combat Center (Zayani & FRRD, éà&', p. 114)

9. Algeria's National Strategy for Cybercrime Prevention:

Algeria occupies an important position in combating cybercrime, having taken serious steps to address the notable increase in electronic crimes. This includes training more than 24,000 engineers and technicians specialized in cybersecurity

and initiating training for additional highly qualified individuals in this field. (Zayani Z. , 2014, p. 114)

Algeria has also contracted with global companies such as Huawei, Microsoft, and Cisco as part of its national strategy to develop the digital economy and enhance cybersecurity.

Accordingly, Algeria has made intensive efforts to protect its cybersecurity system and is working on developing its infrastructure by tightening oversight and applying appropriate legislation and technologies to confront electronic threats. The People's National Army has managed to keep pace with technological developments and secure its informational domain and cybersecurity through its active members, focusing on a rigorous strategy based on key pillars to counter cybercrime. (Zayani Z. , p. 221)

9.1 Algerian Legal Framework:

The focus has primarily been on taking legal measures to combat cybercrime, as evidenced by the issuance of Law No. 09-04 on August 5, 2009, which defines the rules for preventing information technology and communication crimes, including available procedures for monitoring electronic communications. Consequently, the Algerian legislator has organized both general and specific laws, with the general laws based on what is stated in Article 4, which mentions the following:

- Preventive measures are considered necessary to combat activities classified as terrorist or sabotage crimes, as well as to address crimes that threaten state security.
- There should be information indicating the likelihood of an informational system being attacked, posing a threat to public order, national defense, state institutions, or the national economy.
- Judicial investigation operations sometimes require the use of electronic surveillance when it is difficult to obtain results that enhance the current research efforts, within the framework of implementing mutual international legal assistance requests.
- A national authority for the prevention and combat of crimes related to information and communication technology was established according to Article 13, and Presidential Decree No. 261-15, dated October 8, 2015, was issued to organize the work of this authority. This decree defines its

formation, organization, and operational procedures, outlining the authority's tasks, as mentioned in Article 4 of the decree, which includes activities aimed at preventing and combating these crimes.

- The proposed elements of the national strategy for the prevention and combat of crimes related to information and communication technology are included. (Boualam,, 2016, p. 38)
- Enhancing and coordinating efforts to prevent and combat crimes linked to information and communication technology.
- Providing support to judicial authorities and police departments in combating crimes related to information and communication technology, including the collection and provision of information with the assistance of judiciary experts.
- Contributing to the improvement of the laws governing its field of expertise.
- Ensuring precautionary surveillance of electronic communications to detect crimes related to terrorist and sabotage activities that threaten state security, based on decisions issued by a competent judge, excluding any other national bodies.
- Strengthening the role in training investigators specialized in technical investigations related to information and communication technologies.
- Expanding the participation of new actors from outside the military establishment who can contribute to enhancing national defense doctrine, since cyberspace has become one of the most important domains, ranking fifth after land, sea, air, and space. Therefore, it constitutes a vital area for engagement and influence.
- The Directorate of Communication, Media, and Guidance organized a series of seminars in cooperation with the Army of the People’s National Army on the dissemination of information through social networks and the challenges faced by the army, emphasizing the need to enhance security awareness and control over modern technologies within the framework of the Algerian security doctrine. (Boualam, 2016, p. 39)

Additionally, the Algerian Constitution in 2016, through an emergency amendment, ensured the protection of fundamental rights and individual freedoms, emphasizing the most important constitutional principles in its articles.

- **Article 38**: Basic freedoms and human rights are guaranteed.
- **Article 44**: Freedom of intellectual innovation is guaranteed for citizens, and authors' rights are protected by law. The specific laws enacted by the Algerian legislator in the field of electronic crime, the most important of whichis:
  (Law 15-04 from Official Journal No. 14 dated March 7, 2016).

Law on Postal and Telecommunications:

The Law on Postal and Telecommunications includes several provisions related to the cyber domain. Article 87 emphasizes the ease of electronic financial transfers, while Article 84/2 addresses the use of both regular and electronic payment transfers. Article 105 stipulates the respect for correspondence, and Article 127 establishes penalties for anyone who opens or destroys mail.

Social Insurance Law

This law regulates cybercrime through social security institutions, encompassing several provisions related to electronic cards.

Law for the Prevention of Crimes Related to Information and Communication Technology

This law serves as an organization for crimes associated with information and communication technologies, as well as anything related to the informational system. The Algerian legislator has adopted the principle of punishing criminal agreements as stated in Article 394 bis, aiming to prepare for crimes affecting informational systems. The penalty for participation in the agreement is the same as that for the crime being prepared for; if multiple crimes are involved,
The punishment will be that of the gravest offense. (2018, pp. 23-24)

Conclusion:

The Algerian government has adopted cybersecurity strategies to combat criminal threats in the digital space, which pose risks to individuals, society, and internal security, especially as criminals use the latest technologies to execute their attacks. Consequently, the state has been compelled to keep pace with developments in the cyber domain and to develop the necessary laws and systems to combat these crimes and impose penalties on the perpetrators. Additionally,

there are issues of extortion, threats, defamation, and violations of personal privacy through social media platforms, which include the dissemination of false and misleading information along with hacking and cyber harassment.

Despite the efforts made to achieve this, Algeria's rankings both regionally and internationally indicate a need for further efforts to address cybercrime, whether against individuals or institutions, through activating collaborative efforts from community members. This can be summarized in the following action points :

- To eliminate cybercrime, it is necessary to raise community awareness of its dangers.
- Encourage scientific and university training specializing in the study of cybercrime to develop effective solutions.
- Promote media involvement by addressing serious topics related to these crimes and clarifying preventive mechanisms.
- Empower special military and security units to collaborate externally with organizations working to combat risks and mitigate their effects.
- Learn from leading international experiences in this field.
- Socialization plays a crucial role in combating various types of cybercrimes, both traditional and electronic, highlighting the importance of family, school, university, mosque, and civil society organizations in working together to build a community free from extremism and terrorism.

References :

1. *A. Al-Shawabkeh, M. A. (2011).* Computer and Internet Crimes. *Dar Al-Thaqafa for Publishing and Distribution.*
2. *Al-Qaraan, M. A. (2017).* Cybercrimes *(1st ed.). Dar Wael for Publishing and Distribution, Amman.*
3. *Al-Majdoub, T. (2014). "A 'Hidden' Arena for an Upcoming 'Soft' War!"* Lebanese National Defense Publications, *(89), Lebanon.*
4. *Al-Awadi, O. M. G. (2016).* Cybersecurity. *Al-Bayan Center for Studies and Planning, Beirut, Lebanon.*
5. *Hamdoun, T. (2006).* Cybersecurity in Developing Countries. *International Telecommunication Union, Algeria*
6. *Jbour, M. A. (2012).* Cybersecurity: Challenges and Requirements for Response. *Arab Center for Legal and Judicial Research.*
7. *Abd El-Sadiq, A. (2017).* Cyber Wars: Rising Capabilities and Challenges to Global Security. *Arab Center for Cyber Research, Cairo.*
8. *Al-Shahri, N. (n.d.).* Information Warfare. *Center of Excellence for Information Security, King Saud University. Retrieved March 8, 2024,*

from www.coeia.edu.sa/index.php/ar/assur_awess/data_privacy/1263_influance_warfare.html

9. *Jaloud, W. G. S. (2013).* The Role of Electronic Warfare in the Arab-Israeli Conflict. *Master's thesis in Planning and Political Development, Graduate Studies, Nablus University, Palestine*
10. *Al-Khalfi, M. (n.d.).* The Crisis of Moroccan-Algerian Relations and the Issue of Western Sahara. *Retrieved March 8, 2024, from http://www.aljazeera.net*
11. *Zayani, S. (n.d.).* Transformations of Algerian Security Doctrine in Light of Growing Globalization Threats. Thought Magazine, *(5), Algeria.*
12. *Ben Marzouq, A. (n.d.).* Cybersecurity as a New Dimension in Algerian Defense Policy. *Lecture presented to students at Mohamed Boudiaf University, M'sila, Faculty of Law and Political Science, Algeria.*
13. *Ben Marzouq, A. (n.d.).* Cybersecurity as a New Dimension in Algerian Defense Policy. *Lecture presented to students at Mohamed Boudiaf University, M'sila, Faculty of Law and Political Science, Algeria.*
14. *Al-Risail Al-Samitah. (2016).* Weapons of Covert Surveillance, *June 23. Retrieved March 7, 2024, from www.almaged.ps/3*
15. *Fadila, G. (n.d.).* Electronic Crime and the Procedures to Combat It through Algerian Legislation. *Jil Research Center. Retrieved April 7, 2024 from http://jilrc.com*
16. *Farouk, H. (1999).* Computer Viruses. *Al Arabiya for Printing and Publishing, (1st ed.), Cairo.*