RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES

Social Science Journal

Cyber Security in the Algerian National Defense System

Dr. Lehelli Abdelkader[1]

[1]Faculty of Law and Political Science, University of Ahmed DRAIA Adrar (Alegria).

Email: lehelli.abdelkader@univ-adrar.edu.dz

Abstract:

Algeria has recorded rising numbers in the field of cybercrime, especially with its orientation towards e-government, in addition to the unstable security situation in the region In general, and in Algeria's neighboring countries, and therefore national defense policies are no longer limited to Combating terrorism and protecting the sovereignty and stability of the homeland through accreditation on traditional methods only, but went beyond them to include the issue of Protecting the security of the state and society from new threats that Produced by the modern technological revolution, which requires achieving security Cyber as one of the priorities of Algerian defense policy. Where baptized Algerian security system to develop a comprehensive security strategy In order to ensure cyber security, which is considered within the security The comprehensive national of the country.

Keywords: cyber warfare, cyber espionage, cyber terrorism, information security, cybercrime, cyber security.

Introduction:

The information revolution and the emergence of the Internet have created a new environment in addition to land, sea and air, which is the cyber space, which is the new field of conflict at the international or local level, which resulted in a new form of power called cyber power, which led to sharp changes in the concept of power, its patterns and power relations in society, which made the state's ability to control questionable, and led to the ease of possession and spread of this type of power among a larger number of State, individual and group actors have a greater ability to exert this kind of soft power through cyberspace, Ease of use and cheap cost have increased the ability of actors to influence in various areas of life, whether political, economic, military, social and even ideological, and those who have this type of power become more able to achieve their goals and influence the behavior of actors using this environment, and produced new sources of threats to the state that they have never seen before, called (cyber threats), which vary and vary in their forms in terms of nature, sources and goals such as electronic espionage, electronic terrorism, information theft, cyber wars and various Cybercrime.

In light of these threats and modern patterns of wars and crimes, cyber security has become a priority and an essential pillar within the contemporary security system of each country.

In this context, rising numbers were recorded in the field of cybercrime, especially with its orientation towards e-government, and the state monitored priorities to protect the security of the state and society from the new threats that Produced by the modern technological revolution, cyber security has become one of the priorities of defense policy. Algerian.

This paper attempts to answer the following problem: To what extent have the various operational apparatuses of national defense contributed to cyber security?
To answer this problem, the study was divided into two axes:

First Theme: A Conceptual Introduction to Cyber security

In this part of the study, we try to reach a comprehensive and accurate definition of the concept of cyber security, especially in light of the confusion and great similarity between the concept and some of the concepts attached to it, in addition to knowing the most important types of cyber threats and the dimensions of cyber security.

First: Definition of cyber security:

There are many definitions that Presented to the concept of cyber security, including:

" All procedures, measures, techniques and tools used to protect the integrity of Networks, software and data from attack, corruption or non-access Authorized, and further includes device and data protection (1) "

"The sum of technical, organizational and administrative means, which are used in order to prevent unauthorized uses, and in order to prevent the misuse of these means, and to restore electronic information, as cyber security helps protect the work of information systems, and helps enhance the confidentiality and privacy of all personal data, and it also leads to the availability of all procedures and measures aimed at protecting the citizen from risks in cyberspace, as cyber security can benefit individuals and governments together"(2).

The Pentagon provided a precise definition of the term cyber security, considering it "all regulatory measures necessary to ensure that information in all its physical and electronic forms is protected from various crimes: attacks, sabotage, espionage and accidents." In sum, it can be said that cyber security is a set of mechanisms, procedures, means and frameworks that aim to protect software, computers, and cyberspace in general from various attacks, intrusions and cyber threats that may threaten the national security of countries.

Second: **Concepts related to cyber security:**

There are many concepts associated with cyber security, the most important of which are includes (3)

1- Information Security: Protecting information and information systems from unauthorized access or use, leakage, sabotage, modification or destruction and ensuring confidentiality, integrity and availability (4). Cyber security is about securing things at risk through information and communication technology.

2- Cyberspace : "It is a global field formed by various devices that represent the technological infrastructure (computers, control devices, satellites....), which are controlled by wired (cable) and wireless networks, these devices process and transmit the impact on data and information in the virtual environment by users, whether individuals, organizations or countries (5)."

3- Cyber deterrence: Cyber deterrence is defined as "preventing Malicious acts against national assets in space and assets that Supports space operations "

4- Cyber attacks: defined as": actually undermines The capabilities and functions of the computer network for a national or political purpose, By exploiting a certain weakness, the attacker was able to manipulate In order."

5- Cybercrime: "The group of illegal acts and acts Which is done through equipment, electronic devices or a network the Internet or broadcast its contents." The cybercrime is represented in All unlawful acts committed by Modern technologies and the Internet in order to obtain rights unlawful on the one hand with damage or A threat to the other party (6).

Third: Types of cyber threats :

There are many forms of cyber threats that differ in terms of nature and sources, however, there are major cyber threats throughout world that harms the national interest.Such as:(7)

1- Cyber Espionage :

It is the illegal acquisition of confidential information in order to obtain On economic, strategic or military advantage, cyber espionage It's espionage that depends on the use of technologies. Electronic access to information and cyber espionage varies In terms of type, there is espionage by individuals, through wired networks or espionage from Through Satellites .

2-Cyber Crime :

Cybercrime consists of two sections: Crime Cyber and cyber The term cyber is used to describe the idea of a part From the computer or the information age, but crime is behaviors and acts outside the law. Cybercrime is offenses committed against individu als. or groups of individuals motivated by crime with intent to harm The victim's reputation for physical or mental harm to the victim is direct Or indirectly using communication networks such as Internet (such as chat rooms, e-mail and mobile) Computer connectivity for personal purposes or financial gain or harm, including forms of crimes related to By identity, and actions related to computer contents all occur Within the broader meaning of the term cybercrime.

3- Cyber Terrorism :

Dr. (Adel Abdel Sadiq) defined it as meaning: (aggression, intimidation or threat, materially or morally, using electronic means, issued by states, groups, or individuals through cyberspace, or being the target of such aggression in a way that affects its peaceful use. As for its procedural definition, it means: (deliberate activity or attack with political motives for the purpose of influencing government decisions or public opinion using cyberspace as an auxiliary factor in the process of carrying out a terrorist act or war through direct attacks by armed force on the capabilities of the information infrastructure, or through what is considered a moral and psychological impact through incitement to spread religious hatred and war of ideas, or is done in digital form through the use of electronic weapons mechanisms. new battles in cyberspace that may have a limited impact on their digital dimension, or may exceed physical targets related to critical infrastructure) (8).

4- Cyber Warfare :

Successful cyber wars include more than one operator of "electronic wars, and rely on a team of specialists in cyber battles, where each of them is characterized by his own responsibilities and skills to establish the ability to fight, control and highlight it within cyberspace", and cyber war operators plan, manage and implement offensive and defensive activities across cyberspace.

Fourth: Dimensions of cyber security:

It includes five dimensions**:** complement each other,

1-Military dimensions: The importance of cyber security in this dimension arises from the seriousness of cyber attacks and breakthroughs that lead to the emergence of wars and armed conflicts, and breaches of nuclear facility systems, and the threats that may occur to the security of countries and governments and lead to disasters (9). Therefore, the process of securing the ability of military units to communicate through military networks, which allows securing the exchange and flow of information and orders, as well as speed, giving military orders and the ability to deliver targets remotely and destroy them, and this feature may turn into a weak point if the electronic network used in this is not well secured from any external penetration. This may result in disruption of air defense systems or electronic guidance as well as the possibility and loss of control of command units (10).

2-Political dimensions: The political dimensions of cyber security are based on protecting the state's political system and entity, where technologies can be used to broadcast information and data through which the security of states and governments may be destabilized, as they reach very quickly the largest segments of citizens, regardless of the validity of the data and information that is published (11).Russian cyber interference in the US elections is the most prominent evidence of the necessity and importance of cyber security in its political dimension, in addition to the leaks of sensitive documents that often lead to diplomatic crises between countries, and the cyberspace has become a fertile environment for election campaigns and propaganda for various international actors.

3-Economic dimensions: Cyber security is closely related to preserving the economic interests of all countries, as the economy and knowledge are closely interlinked, as most countries depend on the production and circulation of knowledge and information at all levels to strengthen and prosper their economy, which justifies the dangerous role of cyber security in protecting the economy from theft and intellectual property. Also, with the world's entry into the era of electronic money within a mobile technical environment after the launch of electronic services, the investments of banks and financial institutions in the field of digital money are increasing and companies are competing to issue applications that allow secure payment mechanisms, and some countries have developed legislation to protect their funds and the difficulties that this can raise and the legislation it requires to reduce some serious and cross-border economic and financial crimes such as money laundering and tax evasion. Cyber security ensures the provision of services provided by information and communication technologies, as well as the demand for them, which translates practically into the development of the foundations of a sound economy (12).

4-Legal dimensions: The various activities carried out by individuals and institutions are related to laws, and from the emergence of the information society, new laws have emerged, which are the regulatory and legislative environment regulating the protection of this society and the preservation of rights in it in all its dimensions, and cyber security in this dimension is based on protecting the information society and helping it in the application and implementation of these laws and legislations (13). The rapid technological developments require keeping pace with legal legislation in this field, and raise the need to activate joint international cooperation to combat them.

5-Social dimensions: Social networks in particular contribute to opening the way for individuals to express their political aspirations and social ambitions in their various forms, as well as the participation of all segments of society and its components is a means to develop society, which provides the opportunity to see ideas and information and the need of society in maintaining the stability of cyberspace and the society on which it is based (14), and therefore standing to protect our societal security from any external penetration is one of the priorities of cyber security in its social dimension, as it may lead to Any external penetration to threaten the social peace of the state, and accordingly, it is necessary to work to educate the citizen about these risks to achieve cyber security in its social dimension

The second axis: Algerian defense strategies in achieving cyber security:

This means knowing the various legislations, strategies and agencies established by the state within the national strategy to achieve cyber security, and the extent of national readiness and readiness to provide coherent measures and strategic procedures to ensure the security and protection of the presence of the state and individuals in cyberspace, protect critical information infrastructure, and build and nurture a reliable cyber community.

First: An overview of the reality of cyber threats and cyber security in Algeria:

The Algerian security arena, like other countries, is witnessing many risks and threats imposed by the modern technological revolution, especially after the spread of social media and many websites that carry destructive ideas that threaten the stability and unity of the homeland, and call for the spread of chaos, violence, extremism, hatred and division. At the forefront of the most important risks posed by the use of modern technology to Algerian security is cyberterrorism (15).

Electronic terrorism has become one of the most serious crimes targeting Algeria, through the growing manifestations of promoting all forms of violence, terrorism and extremism, using the latest technological technologies, especially social networks and electronic forums. We also point out in this context that cyber threats are not limited to the issue of cyberterrorism, but include many other risks and threats that are not only related to the security of countries, but include society as a whole, they are related to the security of individuals and organizations as well (such as inciting ethnic hatred, crimes against children, slander, cheating, theft, identity theft, destruction of information....).

This information is confirmed by the statement of the Minister of Communication, "Amar Belhimer", that Algeria is the first Arab and 14th globally among the countries most exposed to cyberattacks in 2018. In an interview with Sirmannews, Algeria with its sovereign decisions, principled positions and various geostrategic considerations is more vulnerable to these attacks. Belhimer continued that the President of the Republic In one of his press interviews, he confirmed that there are more than 80 foreign websites waging smear campaigns against Algeria (16).

As for the reality of cyber security, according to the Global Cyber security Index (GCI) for the year 2021, issued by the International Telecommunication Union (ITU), a United Nations based in Geneva, Algeria ranked 104th globally, with a score of 33.95, in the level of preparedness in the field of cyber security, while at the Arab level, Algeria ranked 12th in the Arab world according to its commitments to those measures determined by the Global Cyber security Index (17).

Despite the novelty of Algeria's approach to "**e-governance**", the number of crimes committed suggests the magnitude of the dangers that await it, which makes Algeria strive by all legal and operational means in order to achieve cyber security.

Second: The legislative framework for cyber security in Algeria

In recent years, the Algerian legislator has realized the state of legal vacuum in the field of cybercrime and cyber security, and therefore we try to list and read a set of laws and decrees in this field, including (18):

- Law No. 09-04 of August 5, 2009, containing special rules for the prevention and combating of crimes related to information and communication technologies, which defines the cases that allow the use of electronic communications surveillance based on article 4, which stipulates the following:

- To prevent acts described as crimes of terrorism, sabotage or crimes against State security.
- In the event of information about a possible attack on an information system that threatens public order, national defence, State institutions or the national economy.
- The requirements of investigations and judicial investigations when it is difficult to reach the conclusion of the charges of ongoing research without resorting to electronic surveillance.
- In the context of the implementation of requests for international mutual judicial assistance.

Article 13 provides for the establishment of a national authority to prevent and combat crimes related to information and communication technologies. This is what was done through,

- Presidential Decree No. 15-261 of October 08, 2015, which defines the composition, organization and modalities of the functioning of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies. Among the tasks exercised by the Commission is what is stated in Article 4 of the decree, which stipulates the following:(19)
- Propose elements of a national strategy for the prevention and combating of crimes related to information and communication technologies.
- Activate and coordinate the prevention and control of crimes related to information and communication technologies.
- Assist the judicial authorities and police services in combating crimes related to information and communication technologies, including through the collection and provision of information and judicial expertise.
- Ensuring preventive surveillance of electronic communications in order to detect crimes relating to terrorist and subversive acts and undermining State security under the authority of the competent judge and with the exception of any other national bodies.
- Collecting, recording and preserving digital data and determining its source and path for use in judicial proceedings.
- Ensuring the implementation of requests for assistance from foreign countries and developing the exchange of information and cooperation at the international level in their field of competence.
- Development of cooperation with national institutions and bodies dealing with crimes related to information and communication technologies.
- Contribute to the training of investigators specialized in the field of technical investigations related to information and communication technologies.
- Contribute to the modernization of legal standards in its field of competence. In addition to the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, Algeria has established other bodies that play very important roles in countering various cybercrimes, including:

-Center for the Prevention of Computer and Information Crimes of the National Gendarmerie.

- The Central Department for Combating Cybercrime of the National Directorate of Security.

-National Institute of Forensic Evidence and Criminology of the National Gendarmerie.

-Presidential Decree No. 20-05 of January 20, 2020, establishing a national system for the security of information systems, which is considered the state's tool in the field of information security, issued in issue No. 04 of January 26, 2020, of the Official Gazette (20).

This system constitutes the regulatory framework that oversees the preparation of the National Information Systems Security Strategy. This system includes a National Council for Information Systems Security, which is tasked with preparing, approving and directing the national strategy, and to exercise the functions of the Council, it has the structures of the Ministry of National Defense (21)

The National Council for Information Systems Security is chaired by the Minister of National Defense or a representative thereof, and is also composed of a representative of the Presidency of the Republic, a representative of the Prime Minister, the Minister of Foreign Affairs, the Minister of the Interior and the Minister of Finance, in addition to the Ministers of Energy, Communications and Higher Education, in addition to the possibility of using any other national person or institution (22).

This system is tasked with conducting investigations in the event of cyberattacks, as well as evaluating and collecting data, advising public bodies, in addition to other tasks related to the cyber security of public institutions (23).

Accordingly, it can be said that the Algerian legislator has tried hard to address this type of crime and combat it in various ways, through the enactment of some laws and decrees, as well as the amendment of others, such as the Penal Code as well as the Code of Criminal Procedure in that context, but it is necessary to review and develop laws every time due to the difficulty and dynamism of this phenomenon, especially since cybercrimes leave a basic problem related to terminology, which creates a conflict in the legislation of countries, as what is legitimate In one country it may not be so in another, which requires accuracy and clarity when identifying and updating patterns of criminal behavior.

Third: Operational agencies specialized in Algerian cyber security:

Algeria has established practical agencies that play very important roles in confronting various cybercrimes in an effort to achieve cyber security, namely:

1-Center for the Prevention of Computer and Information Crimes of the National Gendarmerie:

Since the National Gendarmerie is one of the security agencies charged with deterring and limiting crime, the National Gendarmerie Command has risen to establish a unique program represented in the establishment of the Center for the Prevention of Computer and Information Crimes in 2008, and it is considered the only competent agency in this regard in Algeria, and aims to secure the information system to serve public security, and was considered as a documentation center based in Bir Mourad Rais, and this center is working on analyzing the data and data of the information crimes committed, and identifying their owners, whether they are people Individually or gangs, and all this in order to secure and maintain information systems, especially those used in official institutions and banks (24).

This center also aims to help other security agencies in cooperation in order to combat information crimes, as the center is concerned with developing methods of dealing with these crimes and developing laws to regulate the field of exploitation of information through coordination with the Ministry of Justice as well as through a special institute of criminology to develop the level of dealing with crime in general and information crime in particular, Algeria is working hard to benefit from the experiences of other countries in securing the system. Informatics and its protection from crimes within a set of elements, the most important of which are:(25)

- **Prevention:** It includes an awareness campaign in coordination with the Ministry of National Security and Family, work on forums, lectures, study days and international forums, and participation in press forums , television and radio sessions and other means of publishing and publicity.

- **Control:** Raising awareness among Algerians through their use of social networks and the use of the Internet through their comments defending Algeria and knowing the dangers of suspicious behavior or attacks by publishing videos that lead to the perpetrators, thus facilitating the investigation of the gendarmerie services and the timely arrest of suspects and perpetrators of crimes.

2- National Institute of Forensic Evidence and Criminology of the National Gendarmerie:

It is a public institution of an administrative nature under the direct supervision of the Minister of National Defence entrusted with various tasks, such as conducting expertise and examinations in the framework of preliminary and judicial investigations, ensuring scientific assistance during complex investigations (26).

The Institute is one of the projects completed within the framework of the development of the National Gendarmerie «**Bouchaoui**», where it was established by Presidential Decree 04/133 of June 26, 2004, and entered into service starting from the beginning of January 2009, the period between 2004 and 2009 devoted to the formation of human resources and the acquisition of the necessary scientific and technical equipment, and the Institute performs many tasks That would meet requests received from the judiciary, judicial police officers and competent authorities , especially during the handling of complex cases (27).

It also contributes to the organization of mastery courses and post-graduation training in the specialization of criminal sciences, and to perform its tasks to the fullest, the National Institute of Forensic Evidence and Criminology contains many departments and specialized departments, the most important of which are: Fingerprint Service; Environmental Department; As for the field of cyber security, there is the Department of Computer Science; At the level of this service . Hacking and hacking are monitored, monitored and tracked, as well as the discovery of stolen information and the dismantling of computer programs (28).

3- The Central Department for Combating Cybercrime of the National Security Directorate:

The General Directorate of National Security has a key role in confronting information crimes, and this is evident through its preventive, deterrent and awareness-raising role, the preventive role is manifested through holding virtual roundabouts at the level of information networks in general and social networking sites in particular. As for the deterrent role, it is considered an extension of its preventive role in the event of a breach of public order, or in the case of destructive publications that affect public order, such as offering sensitive devices or contraband for sale through social networking sites, where intervention is carried out, the identity of the account owner is identified, and legal measures are taken. In this regard, with the completion of a judicial file against him (29).

In response to the demand for information security and combating security threats resulting from these cybercrimes, the security services established the Central Authority for Cybercrime, which worked to adapt the security formation of the Judicial Police Directorate, which was a platoon that formed the first nucleus of a special security formation to combat cybercrime and at the level of the General Directorate of National Security, which was established in 2011 to be then The Central Service for the Fight against Crimes Related to Information and Communication

Technologies was established by a decision of the Director General of National Security and added to the organizational structure of the Judicial Police Directorate in January 2015 (30).

At the international level, the Directorate of National Security has not neglected to take advantage of its effective membership in Interpol, which provides it with areas for information exchange and facilitation of judicial procedures relating to extradition, as well as the exercise of international letters rogatory and the publication of arrest warrants for those sought internationally (31).

4- National Authority for the Prevention of Crimes Related to Information and Communication Technology and combating them :

Established by Presidential Decree No. 15-261, this body is an independent administrative authority under the Minister of Justice, operating under the supervision and control of a directorate committee chaired by the Minister of Justice and comprising mainly relevant members of the Government, security service officials and two Supreme Court judges appointed by the Supreme Council of the Judiciary (32).

The Authority was tasked with proposing elements of the national strategy for the prevention and combating of crimes related to information and communication technologies, activating and coordinating prevention operations, and assisting the judicial authorities and judicial police services in combating these crimes, through the collection and provision of information and through judicial expertise, and ensuring preventive surveillance of electronic communications, in order to detect crimes related to terrorist and sabotage acts and compromising the security of State Article 13 of Law 04/09 of August containing special rules for the prevention and combating of crimes related to information and communication technology was previously stipulated in the establishment of this body through: "A national body, its organization and the modalities of its functioning shall be established through organization ."Article 14 of the same law provides for its functions:(33)

-Prevention of crimes related to information and communication technology: Prevention measures are to educate users of information and communication technologies of the seriousness of crimes that they may be victims of while browsing or using these technologies, and the most important of these crimes are: spying on communications and electronic messages, manipulating customer accounts, hacking the devices of companies, major institutions or government agencies...

- Combating crimes related to information and communication technologies: according to the text of Article 14 of the Law 04/09 There are two types of control carried out by this body:

- Assist the judicial authorities and judicial police services in their investigations of crimes related to information and communication technology, including the collection of information and the completion of judicial expertise Article 14 (b) of Law 04/09;
- Exchange of information with their counterparts abroad in order to collect all data useful in identifying and combating the perpetrators of crimes related to information and communication technologies, the draft proposes in this chapter the establishment of a competent national authority with the most important tasks of activating and coordinating the prevention of information crimes, assisting the judicial authorities and judicial police services in their investigations into such crimes, and also collecting information from their counterparts abroad in order to Fight this dangerous type of criminality.

Conclusion:

From the above, it can be said that the issue of achieving cyber security in Algeria is one of the most important new challenges to Algerian security policy, imposed by rapid technological developments, and despite the efforts made to achieve this, the ranks occupied by Algeria at the Arab and international levels indicate that it needs more efforts at all legislative and operational levels.

Among the most important conclusions and recommendations that can be drawn from this study:

- The concept of cyber security is a complex and multidimensional concept and levels, starting with achieving state security, then the security of the community, as well as the security of individuals, to then accommodate all circles that can be a source of threat, whether in the internal or external environment or overlapping between inside and outside, as the contemporary developments of the information revolution have led to the expansion of the concept of cyber security.

Despite Algeria's efforts to achieve security and confront the crime of cyberterrorism, whether legal or institutional, it still needs more participatory efforts among the various actors of society.

- Achieving cyber security requires the need to spread community awareness, involve all segments of society, sensitize it to the seriousness of the crime of electronic terrorism, and encourage scientific and university training specialized in its study.

Recommendations:

- Activating the role of civil society and the media in raising awareness of the seriousness of information crimes and the need to report them.
- Strengthening the agencies charged with investigating information crimes each time with new mechanisms, techniques, means and methods that ensure effective confrontation.
- Updating legal texts to ensure keeping pace with the speed and tremendous technological developments, to avoid any legislative deficiencies and overcome legal gaps that may prevent ensuring the goals of effectively confronting information crimes.
- Keeping abreast of technical developments in the field of information by developing criminal justice systems, holding specialized training and training for agencies in charge of investigating information crimes, and developing the skills of investigators in order to detect information crimes as an effective way to reduce organized transnational crimes.
- Benefiting from the experiences of leading countries in the field of achieving cyber security, and identifying the best international technologies adopted in combating cybercrimes such as hacking, espionage and electronic terrorism... Etcetera
- Adopting a preventive policy by spreading the culture of cyber security, raising societal awareness of the various risks and threats posed by the modern technological revolution, and immunizing community members against all destructive ideas spread by various websites and social media, by blocking those sites and prosecuting their supporters.
- Regional and international cooperation by facilitating the exchange of information in the field of combating electronic terrorism, calling for achieving international peace and security, and preventing cyberspace from turning into a field for wars and conflicts between countries.

- Modernizing and protecting the ICT infrastructure, identifying the strengths and weaknesses of legal legislation related to combating information crimes, and working to overcome obstacles to their application.

References:

1-Lamiya Tala, Cyber Threats and Crimes: Their Impact on the National Security of States and Strategies to Combat Them, Maalem Journal of Legal and Political Studies, Volume 04, Issue: 02, Year 2020, p. 60.

2-Ayman Al-Harbi, Introduction to Cyber security, study at the following link: https://drive.uqu.edu.sa/_/aarharbi/files/%D8%A7%D9%84%D8%A7%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A.pdf

3- Mona Abdullah Al-Samhan, “Requirements for Achieving Cyber security for Management Information Systems at King Saud University,” Issue 111, Journal of the College of Education, Mansoura University, September 2020.

4- Ayman Al-Harbi, previous reference.

5- Fatih Harek, Riad Hamdouche, The State between Hegemony and Achieving Security in Cyberspace, Algerian Journal of Human Security, Volume 07, Issue 01, January 2022, p. 134.

6- Hakima Djaballah, Repercussions of cybercrime on the digital environment: a study into mechanisms and strategies for combating it, Annals of the University of Algiers, Volume 35, Issue 03, September 2021, p. 652.

7- Addis Attia, The status of cyber security in the Algerian national security system,

8- Salah Mahdi Hadi Al-Shammari, Zaid Muhammad Ali Ismail. Cyber security as a new pillar in the Iraqi strategy, Political Issues Magazine, No. 62, College of Political Science, Al-Nahrain University, 2020, p. 281.

9 - Mona Abdullah Al-Samhan, previous reference, p. 15.

10- Salim Dahmani, The impact of “cyber” threats on national security, the United States of America - a model - (2001-2017), Master’s thesis, Department of Political Sciences, Faculty of Law and Political Sciences, University of Mohammed Boudiaf M’sila, 2017-2018, p. 30.

11-Mona Abdullah Al-Samhan, previous reference, p. 16.

12- Idris Attia, The Status of Cyber security in the Algerian National Security System, Maddaqa Magazine, Issue 01, p. 105.

13 - Mona Abdullah Al-Samhan, previous reference, p. 17.

14- Idris Attia, previous reference, p. 107.

15- Bin Marzouk Antara, Al-Kar Muhammad, The Electronic Dimension of the Algerian Security Policy in Combating Terrorism, Journal of Humanities and Social Sciences, Issue 38, June 2018, p. 37.

16- Article at the following link:
https://www.ennaharonline.com/%D8%A8%D9%84%D8%AD%D9%8A%D9%85%D8%B1-%D8%A7%D9%84%
D8%AC%D8%B2%D8%A7%D8%A6%D8%B1-%D8%A7%D9%84%D8%A7%D9%88%D9%84%D9%89-
%D8%B9% D8%B1%D8%A8%D9%8A%D8%A7-%D9%8814-
%D8%B9%D8%A7%D9%84%D9%85%D9%8A%D8%A7/

• (The Global Cyber security Index (GCI) is a composite index produced, analyzed and published by the International Telecommunication Union (ITU) to measure countries' commitment to cyber security in order to increase cyber security awareness. This index is rooted in the ITU's global cyber security agenda, Which was launched in 2007, and reflects its five pillars: legal, technical, regulatory, capacity building, and cooperation. The index combines 25 standards into one standard measure to monitor the cyber security commitment of the 193 ITU member states to the five pillars approved by the Global Security Agenda. cyber.)

• (The International Telecommunication Union (ITU). It is a specialized agency of the United Nations responsible for all matters related to information and communications technology. It was founded in 1865 - eighty-five years before the founding of the United Nations itself - as the International Telegraph Union, and it is one of the oldest international organizations operating Today, the headquarters of the International Telecommunication Union is located in Geneva, Switzerland, and includes 193 countries and about 900 commercial and academic institutions and international and regional organizations.)

17-International Telecommunication Union, Report on the World Cyber security Index and Cybersafety Features. Geneva: ITU Telecommunication Development Bureau, July 2021, at the following link: https://www.arab-army.com/t130137-topic

18 - Samir Bara, Cyber security in Algeria: Policies and Institutions, Algerian Journal of Cyber security, No. 04, July 2017, p. 266.

19- Hanan Mbarka Karkouri, The specificity of committing cybercrime in the information system (an analytical study in light of Algerian law), Journal of Strategic and Military Studies, Volume 02, Issue 08, September 2020, pp. 17-18.

20- People's Democratic Republic of Algeria, Presidential Decree No. 20-05 dated 24 Jumada I 1441 corresponding to January 20, 2020, regarding the establishment of a national system for information systems security, Official Gazette, No. 04, issued on January 26, 2020, p. 6.

21- Article at the following link:
https://algeriemaintenant.com/2020/01/%D8%A5%D9%86%D8%B4%D8%A7%D8%A1-%D9%85%D9%86%D8%
B8%D9%88%D9%85%D8%A9-%D9%88%D8%B7%D9%86%D9%8A%D8%A9-
%D9%84%D8%A3%D9%85%D9% 86-%D8%A7%D9%84%D8%A3%D9%86%D8%B8%D9%85%D8%A9-
%D8%A7%D9%84%D9%85%D8%B9

22 - People's Democratic Republic of Algeria, Presidential Decree No. 20-05 dated 24 Jumada al-Awwal 1441 corresponding to January 20, 2020, regarding the establishment of a national system for information systems security, Official Gazette, No. 04, issued on January 26, 2020, p. 6.

23 - Ibid., p. 07.

24- Salima Nawawi, Hoda Akoushi, The role of the National Gendarmerie in combating electronic crime: The Regional Group of the National Gendarmerie in M'sila as a model, Master's thesis, Department of Media and Communication Sciences, Faculty of Humanities and Social Sciences, University of M'sila, year 2018/2019, p. 36.

25 - Idris Attia, previous reference, p. 112.

26- Samir Bara, previous reference, p. 271.

27- Idris Attia, previous reference, p. 113.

28 - Samir Bara, previous reference, p. 272.

29 - Raja Oumdour, Privacy of investigation in the face of cybercrimes, doctoral thesis in private law, Department of Law, Faculty of Law and Political Science, University of Bordj Bou Arreridj, year 2020-2021, p. 104.

30- Samir Bara, previous reference, p. 272.

31 - Omdur Raja, op. cit., p. 106.

32- Ibid., p. 274.

33 - Idris Attia, previous reference, p. 114.