... ZAOULI N°10, Vol. 8, Août 2025, pp. 557-582 ISSN : 2788-9343

Soumission : **13/04/2025** **Acceptation : 09/06/2025** **Publication** : **25/08/2025**

Cyberespionage in the economic sphere and mechanisms for combatting it

ZÉGOUARÈNE Samia
Professor, Lecture A, Faculty of Law,
University of Algiers 1
Laboratory of Human's Rights
E.Mail : s.zegouarene@univ-alger.dz
szegouarene@yahoo.fr

Abstract:
In spite of the useful aspects of information technology in bringing people together and introducing them into the virtual world, it has negative effects that affect the rights and freedoms of individuals and even states, which led to the emergence of what is known as information crime, which affected individuals and their property, and even the security of states, and this is what It constitutes the focus of our study, as we will shed light on the most dangerous crimes to which global technology has contributed, namely "electronic economic espionage." If the geopolitical dimension is known as a fierce war that is reduced to military confrontation, the geoeconomic dimension is known as economic war to achieve economic security.
The crime of electronic economic espionage is characterized by its extreme seriousness and continuous development, especially by using modern technical methods in all fields.

keywords: *information crime, economic espionage, individual rights, state security-fields*

Résumé *:*
Malgré les aspects utiles des technologies de l'information pour rapprocher les gens et les introduire dans le monde virtuel, elles ont des effets négatifs qui affectent les droits et libertés des individus et même des États, ce qui a conduit à

l'émergence de ce que l'on appelle la criminalité informatique, qui touche les individus et leurs biens, voire la sécurité des États. C'est ce qui constitue le sujet central de notre étude, dans laquelle nous mettrons en lumière les crimes les plus dangereux auxquels la technologie mondiale a contribué, à savoir « l'espionnage économique électronique ». Si la dimension géopolitique est connue comme une guerre féroce qui se réduit à une confrontation militaire, la dimension géoéconomique est connue comme une guerre économique visant à assurer la sécurité économique.
Le crime d'espionnage économique électronique se caractérise par son extrême gravité et son développement continu, notamment par l'utilisation de méthodes techniques modernes dans tous les domaines.

***Mots-clés** : criminalité informatique, espionnage économique, droits individuels, sécurité de l'État*

Soumission : 13/01/2025 **Acceptation :** 09/06/2025 **Publication** : 25/08/2025

Introduction:

The majority of countries have recently been connected to the Internet, and with it the use of websites and computers has increased. This has led to the emergence of several challenges resulting from the digital revolution.

Despite the positive aspects of information technology in bringing people together and bringing them into the virtual world, this revolution has negative effects that influences the rightness and liberties of individuals and states, as a consequence of the exploitation of technology by individuals and various entities, which led to the emergence of what is known as information crime, which affected individuals and Their property As well as the security of countries, and this is what constitutes the focus of our study, as we will shed light on the most dangerous crimes that high technology has contributed to, namely "electronic economic espionage." If the phenomenon of espionage is ancient, the countries of the world witnessed it during their struggles to rule the world politically. And militarily, but it developed with the development of advanced technology and was carried out by experts in information technology. It took a menacing insecure as a consequence of the alteration in international's philosophy interests, like the geography of the world which becomes determined by economic data par excellence. This geoeconomic dimension became the new frame of reference for ensuring entity of the state's entity , And the degree of its abilities to confront economic competitiveness.

If the geopolitical dimension is known as the fierce war that is reduced to military confrontation, then the geoeconomic dimension is known as the economic war to

achieve economic security or continue the military-diplomatic strategy represented by economic and commercial means, as electronic economic espionage is considered one of its mechanisms.

The crime of electronic economic espionage is characterized by its extreme seriousness and continuous development, especially by using modern technical methods, due to the continuous technological development in all fields.

To address this issue, the following problem was raised:

- How does the crime of electronic economic espionage influences state's security and sovereignty?
- How can this crime be reduced in light of information technology development?
- Has the Algerian legislator kept pace in its legislation with developments in such crimes?

To address this problem, we will rely on the analytical approach as well as the descriptive approach, and this study was divided into three sections: defining terms and concepts then. (in first section).

After, we will treat the historical development of the crime of cyberespionage in economic field, its characteristics and its consequences on state's security and sovereignty (in the second section), finally we will study the different ways for combating the crime of cyberespionage in economic field and the situation of the Algerian legislator on it. (in the third section).

Section I: Define terms and concepts

This research will address defining the terms and concepts as information crime, cybercrime in the economic

Soumission : 13/01/2025 Acceptation : 09/06/2025 Publication : 25/08/2025

sphere also spyware (in the first requirement), after ,we will treat ; economic intelligence, including the economic security (in the second requirement), and finally we will study hackers and the hateful sect (in the third requirement).

A) Definition of cybercrime, electronic economic espionage, and spyware

This research will address the definition of each of the following terms: electronic crime or information crime, electronic economic espionage, and spyware.

The basis of information crime or information crime is information (data, programs), as well as legally criminalized actions that may harm the property of others, persons, or freedoms.

1- Definition of cybercrime or information crime

To define information crime we must define legal definition crime first (1-1), after the technical definition (1-2) second.

1-1 Legal definition of information crime:

In contrast with the French legislator, the Algerian legislator defined information, in Article 2, Paragraph 1, of law no. 09/04 which dated in August 5th in 2009, that includes the principles rules to prevent and to fight the crimes in relation with information and communication technologies. We notice that this description is general and incorrect, as it defines “information crime” as all crimes related to harming systems so that the other crimes are involved and assisted by cybercriminals. “They are engaged

using an information system or any category of electronic communication system."

1-2 The technical definition of information crime:

It is:

> "Every illegal act or omission carried out by means of a computer or any automated information processing device, whether the device is a tool for committing the crime or a place for committing the crime, in a closed or open electronic or information field on information networks or an environment for committing the crime, which must be the original perpetrator must have sufficient knowledge to commit it."

Information crime is named by several terms, like computer crimes, high-tech crimes, including hacker hate, cybercrime, crime in fanciful space, and crimes via a distance message system.

2- Electronic Economic Geospatialism

Economic espionage is considered one of the mechanisms of economic warfare. It also includes all methods, systems and approaches that aim to obtain confidential information owned by another, without the knowledge of the latter, that is, relying on illegal methods is sometimes done.[1]It violates the sovereignty of the state, and this work is limited to the intelligence services, but this matter has developed with the development of economic actors, as major companies have also begun to work in this field or are requested to do so from the relevant state agencies in exchange for a fee.

Soumission : 13/01/2025 **Acceptation :** 09/06/2025 **Publication** : 25/08/2025

Economic espionage is also defined as an act committed by a person or group (a company-A mafia state) obtaining important information and data of economic benefit, without the consent of the party being spied on, which inflicts losses or disabilities on the opponent in the economic market.

Economic espionage is a method that adopted inside the frame of the work of intelligence activities, the last of which commit out their work with complete secrecy. Economic espionage is not limited to searching for information, but rather to analyzing and exploiting economic information.

As for electronic economic espionage, it is closely linked to developments that occur in the digital environment. It becomes more dangerous as progress increases in the information field. Development, progress, discovery, and construction are necessarily met with demolition and espionage.

Electronic economic espionage relies on programs that track, view, and monitor the sites that the user visits, in order to steal confidential information, by introducing the program into a computer, as the program keeps itself from the system of computer so that its presence is difficult to discover.

As some experts say, electronic economic espionage has become one of the most important and dangerous weapons in the hands of many countries and governments[2]Giant companies and even individuals, all seeking control and achieving huge profits.

.

Electronic economic intelligence is a type of war aimed at controlling countries, governments, and people, the pace of which has increased significantly in light of the tremendous technical development.

3- Spyware

These are computer programs that are installed surreptitiously on computers to spy on spyware

Users, and partially take control of the individual computer outside knowledge of the users, including spare which is a secret programs that monitor users' behavior and collect various personal information,

They control the computer and steal personal and sensitive information.

B) Economic intelligence and economic security

Economic intelligence is defined as all approaches to managing and techniques for gathering and analyzing all informations with the object of reviving and improving the state's work compagnies, international organizations and non-governmental organizations that work in the economic field.

It is taught in specialized research centers, and economic intelligence is carried out through economic channels that provide information to economic actors (media, public documents, international forums, research centers). It is then analyzed by economic experts and translated into economic policy.

Economic intelligence was involved with the development of the cognizance economy and the development of informations and communications technologies, as the project group in the General Prefecture

Soumission : 13/01/2025 Acceptation : 09/06/2025 Publication : 25/08/2025

of Planning in France provided a practical definition of economic intelligence as: "a group of coordinated activities of research, processing, and disseminating useful information to economic agents and stakeholders to formulate their strategies."

The highest official for economic intelligence in France, that intelligence, Alain Juillet in When he saw:

- The aim of economics is governing to conduct and save strategic information's for all economic actor to realize competitivity in the economic field and, economic security, security of institutions, strengthening the policy of influence, and providing strategic information that allows for a best definition of the action and axis of evolution of the entity in relation to a business environment characterized by with continuous development and extreme complexity.
- Information security can relate to protecting the national economy from all forms of economic espionage and piracy of making strategies for work.
- The initial element of economic intelligence is possessing information.
- The degree of distinctness as between economic intelligence and economic espionage seems in whatever the instrument used to obtain legitimate or illegitimate informations.
- The state plays a function in determining the agreement or plan of principle structure of a country's economic and scientific potentialities for economic guarantee , which the interests of the

country being the fundamental factor , were the state alone is no longer responsible for economic security, but all institutions are obligated to participate.

C) Hackers, crackers, and hateful sects

This requirement will address the definition of hackers, crackers and the malevolent sect.

1- Hackers

He is the person who creates and modifies software, and they mean young adults associated with information technology. There are those who are called (young information geniuses), most of whom are students and young people who have knowledge in the field of technology. They are also called information pirates and their goal is sabotage and not for other purposes.

2- Crackers

The adult criminals or saboteurs in question, often between the ages of 25 and 45, are professional hackers who are among the most dangerous perpetrators of crimes.

3- The hateful sect

This sect often targets organizations, establishments, and employers, and the goal of committing the crime is revenge and obtaining material or political benefit, and it may be (Extremist, spy, or systems hacker).

Soumission : 13/01/2025 Acceptation : 09/06/2025 Publication : 25/08/2025

Section II: The historical development of the cyber espionage crime
Its characteristics and its impact on the security and sovereignty of states

This research will address three preconditions: the first precondition concerns the historical development of the crime of electronic espionage (the first requirement), the second precondition concerns the Characteristics of the spy crime Economic (The second requirement) and finally the third precondition concerns the Grimm effect of electronic economic espionage on the security and sovereignty of states (the third requirement).

A) Developing of the historical of cyber espionage crime

The director of the CIA Stansfield Turner under US President Jimmy Carter, telling :

"If we spy for causes of military security, why don't we shadow for economic security? Turner asserted out in 1992 that the United States of America must conduct more aggressive intelligence operations in order to assure America's highest economic position in the world.

It was the first economic espionage operation during the seventies and eighties, when France planted spy agents in the companies "IBM" and "Texas Instruments". They transferred the information they had obtained from a French computer company. The microphones used were placed it on located seats of Air France planes in order to capture the discussion taking place among business travelers has become a landmark in the world of intelligence.

In this regard, former French intelligence chief Pierre Marion said, “In the world of economics, we are competitors, not allies.” He added, “The United States technological information has the best material and access, making it a usual access for country to gain access to it.” The most significant attention is given by the intelligence services.

The Director of the American Central Intelligence Agency, Robert Gates, was the one who installed the fundament or basis of the concept of economic espionage in the first nineties, and this concept was adopted by American spies, as in 1995, according to the New York Times, they spied, to a large extent, on participating Japanese officials. In trade negotiations with the United States of America.

Several documents since 2007 have shown that American agents spied on the Brazilian oil company Petrobras, they also spied on the European Union official which was responsible for competition program and other issuances was aimed. The National Security Agency, depending on the New York Times, focused that “Servers owned to the big Chinese telecommunications company "Huawei" on the basis of its relationship with the Chinese army”.

In the same context, and in electronic economic espionage as a result of the tremendous development of technology, five (05) officers in the Chinese army, according to the US Department of Justice, stole data from six companies, and from American unions, they penetrated American computer networks to steal data useful to commercial competitors of the United States of America.

With the aim to direct the market’s activities of the Asian continent, the United States of America is working to recruit all its spies who are experts in advanced technology to carry

Soumission : 13/01/2025 Acceptation : 09/06/2025 Publication : 25/08/2025

out electronic economic espionage using temptation with money and advantages, and the best evidence of this is the American-Chinese economic war, and the imposition of the United States on goods. Chinese fines and high taxes amounting to billions of dollars, as well as a fine for the Chinese telecommunications giant “Huawei”.

On the other hand, China is also working in the same manner as the United States, by recruiting spies in light of electronic economic wars, in order to control and expand in all markets of the five continents.

France recently accused China of electronic economic espionage against Airbus, the European giant in the aircraft industry, by stealing information related to preparing aircraft engines for military transport of the A200M class, as well as stealing a set of electronic systems that help fly the plane. China has denied this. That was in late September 2019.

It should be noted that China has flooded Europe, America, and developing countries with its techno-economic spies.

The German intelligence agency also accused in its report that all active countries in the world (Russia, the United States, China, Britain...) of fighting and struggling to collect scientific and technological information, whether in developed countries or countries. Developing countries, and stated that everyone is spying on everyone, in all economic, agricultural, industrial, technology, etc. fields.

A Canadian national security report in 1993 also indicated that Canadian scientific secrets and technological research, which took many years to prepare and cost millions of

dollars, were stolen and transferred to factories and companies outside Canada.

As indicated in the French White Paper for the Defense of National Security in 2013, the national perception of the risks of attacks on the information system was identified in two major risks threatening France: "electronic espionage and electronic sabotage of sensitive infrastructure."

The methods and weapons of electronic economic espionage have become advanced by recruiting hackers in exchange for an open check, recruiting members of the targeted country who oppose the regime in exchange for enticing them to take them to decision-making centers.

B) Characteristics of the crime of electronic economic espionage

The crime of electronic economic espionage derives its characteristics from the characteristics of information crime, which are:

1 - The **crime of electronic economic espionage,** a global crime, that is, it is It goes beyond the borders of a single country, as it crosses continents.

2- A crime that is difficult to prove, as it does not leave a physical trace, it is also difficult for a technician to preserve its traces, if they exist, as it requires special technical expertise that is difficult for the ordinary investigator to deal with easily, due to the presence of special programs, secret words, ciphers and symbols that hinder access to the evidence, and therefore the investigator must be an expert. In technology, the same weapon used by hackers is used, which can delete

Soumission : 13/01/2025 Acceptation : 09/06/2025 Publication : 25/08/2025

information and data that could be used as evidence against him.

3- The crime of electronic economic espionage is a soft crime

Calm, it does not require muscular effort, force, violence, or the use of weapons, but rather than just intellectual effort and a significant amount of knowledge of the computer programs, the Internet and computer secrets.

4- The modernization of the laws relevant the crimes of electronic economic espionage, as they are the same as those related to information crimes. The first law stipulating them was in France under Law No. 88/19 of January 5, 1988, while the Algerian legislation was in the year 2001.

5- Judicial police officers have exceptional jurisdiction in the crime of electronic economic espionage. In Algeria, jurisdiction in combating these crimes devolves to the specialized judicial poles like in Algiers, Constantine, Oran and Ouargla.

C) The consequences of cybercrime of economic espionage on the security and sovereignty of countries

Electronic economic espionage is a crime that aimed to:

1- **Causing instability in security of countries and government's security**, as the latter become constantly concerned about their secret economic information, and become the subject of bargaining

by hackers or spies, whether they are individuals or governments of other countries, and this bargaining can be in the form of economic, military or political.

2- **The crime of electronic economic espionage can destroy the economies of countries**, whether they are large or developing countries, the latter of which do not have a firm and strong information security system.

3- **The electronic economic spy of all kinds (individuals, organizations, governments...) can exploit the citizens of developing and poor countries, by recruiting them** to serve them while luring them with financial and even political privileges, which is to reach power, which can be achieved through military coups supported by major powers. Etc., which leads to instability. In this regard, the spokesman for the Russian Kremlin, Dmitry Peskov, stated that the BRICS group considers the crime of electronic espionage as a terrorism and a danger to the security of countries.

The crime of electronic economic espionage affects international security, as a new concept of security has emerged regardless of traditional military security, we notice that the information's security of this crime is an economic nature.

4- **The consequence of the cybercrime in economic espionage field on international relations and policies,** which leads to the management of international conflicts and the pursuit of dominance in international relations.

Soumission : 13/01/2025 Acceptation : 09/06/2025 Publication : 25/08/2025

5- **The crime of electronic economic espionage affects the financial income of countries**, causing countries to lose billions of dollars.

Section III: Ways to combat the crime of electronic economic espionage and the Algerian legislator's position on it

This research will address ways for combating the crime of electronic economic espionage in the first requirement, after, the position of the Algerian legislator on the crime of electronic economic espionage in the second requirement.

A) Strategies for fighting the crime of electronic economic espionage

Counter-espionage is one of the most important and precise tasks in security work, and considering that the electronic economic espionage crime is a serious crime that affects the national security of any country, just as there is an intelligence service for espionage and hacking, there must, in return, be an intelligence service whose mission is to resist hacking.

Among the mechanisms to combat the crime of electronic economic espionage are mechanisms of a technical nature and mechanisms of an international nature.

1- Technical mechanisms to combat the crime of electronic economic espionage (information security)

They are as follows:

- Use protection programs against malicious programs (destructive viruses).
- Separating internal networks from the Internet.

- Periodic scanning to detect spy devices and jamming devices.
- Using technology to detect electronic spy devices.
- Changing applicable codes and methods.
- Allowing spyware and hacking programs to operate in a fake environment to reveal who is behind them.
- Establishing special centers to combat electronic economic espionage, and training hackers to combat intrusions.
- Since the crime of electronic economic espionage, as previously mentioned, affects the national security of countries, it is necessary to establish interests at the level of security leadership, specifically combating information crimes, combating electronic espionage, and monitoring the security of information and systems.

2- Mechanisms of an international nature

Combating cybercrime, including the crime of electronic economic espionage, has received international and regional attention, as the Budapest Convention was concluded in 2001 to combat cybercrime.

To combat or reduce this crime, cooperation must be strengthened between countries, through the exchange of information and tracking down espionage hackers, as well as strengthening and encouraging cooperation between police agencies among member states of the International Criminal Police Organization (Interpol).

- Strengthening regional and security cooperation in combating the crime of electronic economic

Soumission : **13/01/2025** **Acceptation : 09/06/2025** **Publication** : **25/08/2025**

espionage, through private organizations such as Afripol among African countries.

- Strengthening judicial cooperation between countries, by adopting bilateral or multiple judicial agreements to receive and extradite electronically hacked criminals, initiating international judicial rotatories, and publishing arrest warrants for those wanted on the international stage.

B) The attitude of the Algerian legislator on the crime of electronic economic espionage

In spite of the obstacles of checking and fighting the crime of electronic economic espionage, as it is classed the most serious information crime that impacts the security of states, the Algerian legislator tried to establish legal texts , to punish theses acts due to the constraint of technological advancement in information technology, by amending the penal code in 2004 with Law no 04/15 of 10 November 2004 under the title "Abusing Automated Data Processing Systems," and includes eight articles, from Article 394 bis 3 to Article 394 bis7.

Concerning crimes of espionage and terrorism, the Algerian legislator doubled the punishment due to their gravity according to the provisions of Article 394 bis 3, which stipulates: "The penalties stipulated in this section will be doubled if the crime aims at the national defense , bodies or institutions that are subject to public law, without affecting the application of penalties."

The Penal Code was amended in 2006 by Law No. 06/23 of December 20, 2006. Due to the seriousness of the crime of electronic economic espionage and its impact on the national

economy, the penalty prescribed for these acts was increased. The last modification of the Penal Code was at 2016.

In accordance with the Penal Code, the Algerian legislator modified the Code of Criminal's Procedure in application of Law no 06/22 of December 20, 2006. During the 37 th period thereof, the legislator increased the territorial jurisdiction of the Public Prosecutor in electronic crimes. It also extended the jurisdiction of judicial police officers, and even inspection in Such crimes have a special nature, as judicial police officers are authorized to intercept correspondence, record votes, and capture photos, take pictures, in accordance with article 65 bis 5/10 of the Q.S.C.

At last, the Algerian legislator created a specific law that aims to prevent and fight all crimes concerned the information and the communication technologies, which includes the crime of electronic economic espionage, as information systems can be searched when necessary and information data can be seized.

C) Regarding the bodies specializing in combating economic espionage crime:

Considering the gravity of the crime of economic espionage, the Algerian legislator set up a national body to prevent all crimes relative to information and communication technologies in conformity with Law no 04/09 of August 5, 2009. The presidential decree issued in 2015 came to clearly regulate it, and one of its tasks is to activate international judicial and security cooperation, and coordinating preventive operations and technical assistance to judicial and security authorities in the event of an

Soumission : 13/01/2025 **Acceptation :** 09/06/2025 **Publication** : 25/08/2025

aggression on the system of information in the manner that menaced the strategic interests of the national economy.

As well, specialized criminal judicial bodies were established pursuant to Law No. 04/14 of 10/01/2004 amending and supplementing the Code of Criminal Procedure, as they are specialized in examining information crimes targeting state institutions and the national economy and defense.

Concerning the National Institute of Criminal Evidence including Criminology, which consists of eleven (11) departments specialized in different fields, its tasks are to provide expertise and provide technical assistance, and the Department of Automated and Electronic Media is charged with processing, analyzing and presenting all digital evidence that helps justice.

Finally, the Ministry of National Defense created the "Cyber Defense and Systems Security Monitoring Service" at the level of the Information and Preparation Department, whose goal is to secure and protect the country's vital systems and installations against threats, electronic terrorism, and spying on the secrets of the Algerian state, and this will protect the security and sovereignty of Algeria. By responding quickly to intrusions and jamming spy devices, according to the latest statistics of the Ministry of National Defense, it aborts 3,500 intrusions every day into the websites of its force leaders by hackers from various parts of the world.

Conclusion:

It is clear from this study how dangerous the crime of electronic economic espionage is to the security and sovereignty of countries, as electronic wars have now become economic wars whose goal is to control the world's markets and control its wealth and national sovereignty.

These wars have become more ferocious recently, especially between the United States of America and China, as this crime has affected international relations and has become a means of sowing strife and conflicts in countries of the world.

Considering that Algeria is a country in this international community, and as a result of the tremendous technological development, it is always targeted by hackers, therefore the level of caution must be raised and information security must be controlled in an effective manner, through the training of cadres in modern technology along with the training of judicial police officers specialized in information security, and judges. We specialized in repressing this category of crime, some as is the fact in the United States of America and Britain. Legal texts must also be amended in line with technological developments taking place while strengthening judicial and security cooperation between countries.

Soumission : 13/01/2025 **Acceptation :** 09/06/2025 **Publication** : 25/08/2025

References

- Abdel Fattah Murad, Explanation of Computer and Internet Crimes, Egyptian House of Books and Documents, 2005, p. 65, reference referred to in, Fadila Aqly, previous reference, p. 6.

2- Wikipedia cyberespionage on britannica.com archived on February 20, 2023.

3- Official Gazette, Issue No. 47 issued on 08/16/2009.

4- Wikipedia cyberespionage on britannica.com archived on February 20, 2023.

5- Electronic espionage, an article published online on April 10, 2009, without mentioning the author.

6. Fouad Barami, Electronic Espionage, Its Characteristics and Objectives, an article published online on 12/13/2018 at 18:24, p. 1 and p. 2.

7- **Wikipedia,** Cyberespionage on britannica.com archived on February 20, 2023.

8- Hamdani Mohamed, the importance of economic intelligence in improving business suitability and attracting foreign investments, Algerian Enterprise Performance Journal, issue 02/2012, p. 12 and p. 13.

9- Hamdani Muhammad, the importance of economic intelligence in improving business suitability and attracting foreign investments, Algerian Enterprise Performance Journal, issue 02/2012, pp. 12 and 13.

10-. Economic espionage, previous reference, p. 2.

11- Fadila Akli, Cybercrime and measures to confront it through Algerian legislation, Proceedings of the Fourteenth International Conference, Cybercrime, Libya, Tripoli, March 24 and 25, 2017, p. 6.

12-. Abdel Fattah Murad, Explanation of Computer and Internet Crimes, Egyptian House of Books and Documents, 2005, p. 65, reference referred to in, Fadila Aqly, previous reference, p. 6.

13- Hamdani Muhammad, previous reference, p. 13.

14- Elias Grol, Swedish writer and political analyst, Economic espionage...a new intelligence goal, article published in the UAE electronic newspaper Al-Ittihad, dated 05/28/2014, without page.

15- Elias Groll, previous reference, without page.

16. A. Hamad bin Abdullah Al-Luhaidan, Economic espionage is the most important axis of economic wars, an article published in Al-Yamamah Magazine, electronic version, Bahrain, 11/25/2005, Issue No. 13668, without mentioning the page.

17-. Bashir Al-Wandi, The Importance of the Counter-Espionage Service in Protecting the National Security of the State, European Center for Counter-Terrorism and Intelligence Studies, March 16, 2018, p. 1.

Bibliography

1. Laws

1- Law No. 09-04 of August 5, 2009 containing the rules for preventing and combating crimes related to media and communication technologies (GR), No. 47, issued on August 16, 2009.

2- Law No. 40-14 dated 10-01-2004 amended and supplemented the Code of Civil Procedure regarding information crimes targeting state institutions and the economy.

Soumission : 13/01/2025 **Acceptation :** 09/06/2025 **Publication** : 25/08/2025

2. Books

- Abdel Fattah Murad, Explanation of Computer and Internet Crimes, Egyptian House of Books and Documents, 2005, p. 65, a reference referred to in the book of Fadila Akli, previous reference, p. 6.

- Bashir Al-Wandi, The Importance of the Counter-Espionage Service in Protecting the National Security of the State, European Center for Counter-Terrorism and Intelligence Studies, March 16, 2018, p. 1.

- **Wikipedia** cyberespionage on britannica.com archived on February 20, 2023

3. Articles

- Electronic espionage, an article published online on April 10, 2009, without mentioning the author

- Fouad Barami, Electronic espionage, its characteristics and goals, an article published online on 12/13/2018 at 18:24, p. 1 and p. 2.

-Hamdani Mohamed, the importance of economic intelligence in improving business suitability and attracting foreign investments, Algerian Enterprise Performance Journal, issue 02/2012, p. 12 and p. 13.

-A Hamad bin Abdullah Al-Luhaidan, Economic espionage is the most important axis of economic wars, an article published in Al-Yamamah magazine, electronic version, Bahrain, 11/25/2005, issue No. 13668, without mentioning the page.

-Elias Grol, Swedish writer and political analyst, Economic espionage...a new intelligence goal, article

published in the UAE electronic newspaper Al-Ittihad, dated 05/28/2014, without mentioning the page.

4. Forums

- Fadila Akli, Cybercrime and measures to confront it through Algerian legislation, Proceedings of the Fourteenth International Conference, Cybercrime, Libya, Tripoli, March 24 and 25, 2017, p. 6.