Contemporary Readingsin Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 18 (01), 2026
pp. 580 - 590

Electronic Economic Espionage, the New Face of Cybercrimes Affecting State Security.

Dr. Nacera Khouas[1]

[1]Faculty of Law, University of Algiers **1,** Comprehensive Development Mechanisms Laboratory in Algeria, Algeria**.**

Abstract

Economic espionage is one of the risks that companies and governments pay great attention to combating, as it poses a threat to stability and economic development.

The digital revolution and the total reliance on digital communications have doubled the emphasis of companies and officials on preserving trade secrets from robbery and theft, and have also made it easier for hackers to access the data and secrets of companies and economic institutions**.**

Keywords: espionage, electronic, cybercrime, state security.

Received: 10/08/2025 **Accepted: 18/02/2026** **Published: 24/04/2026**

Introduction:

Most countries have recently become connected to the Internet, and with it the use of websites and computers has increased, which has led to the emergence of several challenges resulting from the digital revolution.

Despite the positives of information technology in bringing people closer together and introducing them into virtual worlds, this revolution has negative effects that have affected the rights and freedoms of individuals and even countries, as a result of individuals and various parties exploiting technology, which has led to the emergence of what is known as information crime, which has affected individuals or people and their property, and even affected the security of countries. This is the focus of our study; we will shed light on the most dangerous crime that high technology has contributed to, which is "electronic economic espionage." If the phenomenon of espionage (espionage) is old, the countries of the world have witnessed it during their struggles to dominate the world politically and militarily, However, it has developed with the development of advanced technology and has become carried out by experts in technology and information technology, and it has taken a more dangerous direction as a result of the change in the international philosophy of interests, as the geography of the world has become determined by an economic given par excellence. This geo-economics dimension has become the new framework for ensuring the entity of countries and the extent of their capabilities to confront economic competitiveness.

If the geopolitical dimension is known as fierce war, which is reduced to military confrontation, then geo-economics is known as economic war to achieve economic security or continue the diplomatic military strategy represented by economic and commercial means, and electronic economic espionage is considered one of its mechanisms.

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

To address this issue, we raise the following problem:

How the crime of electronic economic espionage affected and affects the security and sovereignty of the state?

What is the way to combat or even reduce this crime in light of information madness?

Has the Algerian legislator kept pace in his legislation with the developments taking place in such crimes?

To address this problem, I will follow the analytical and descriptive approach, and I will divide this study into three (03) investigations:

The first section: Defining terms and concepts: cybercrime, electronic economic espionage, economic intelligence, economic security, hackers, crackers, and the hateful sect.

The second section: The historical development of the crime of electronic economic espionage, its characteristics and its impact on the security and sovereignty of states.

The third section: Mechanisms to combat the crime of electronic economic espionage and the position of the Algerian legislator on it.

Section One: Defining terms and concepts

First: Definition of cybercrime

The basis of cybercrime or cybercrime is information (data, programs) as well as legally criminal actions that may affect the money of others, individuals, and freedoms.

1- Legal definition of cybercrime:

The Algerian legislator defined this, unlike the French legislator, in Article 2, Paragraph 1 of Law No. 09/04 (1) of August 5, 2009, which includes special rules for preventing and combating crimes related to media and communication technologies, however, this definition was general and inaccurate, as "information crime is all crimes related to tampering with systems or other crimes that are committed or facilitated by the use of an information system or any type of electronic communication system."

2- Terminological definition of cybercrime:

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

Cybercrime is called by several terms, including computer crimes, high-tech crimes, hacker crimes, Internet crimes, crime in fictional space, and crimes via remote communication networks.

Second: Electronic economic espionage

Economic espionage is considered a mechanism of economic warfare, and it is all the methods, systems and approaches that aim to obtain secret information owned by another, without the latter's knowledge, i.e. illegal methods are relied upon, sometimes (2) in which the state's sovereignty is violated, and this work is limited to the intelligence services, However, this matter developed with the development of economic actors, as large companies also began to work in this field, or this was requested from the competent state agencies in return.

Economic espionage is also defined as the act by which a person or group is intended (Company–State-Mafia) Obtaining important information and data of economic benefit, without the consent of the spied-on party, which incurs losses or disabilities to the opponent in the economic market.

Economic espionage is a process that falls within the framework of the work of intelligence agencies, the latter of which carry out their work in 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 matched by destruction and espionage. Electronic economic espionage relies on programs that track, view, and monitors the sites that the user visits, to steal confidential information, by installing the program on the computer, as the program hides itself from the system so that it is difficult to detect its presence.

As some experts say, the process of electronic economic espionage has become one of the most important and dangerous weapons in the hands of many countries, governments (3), giant companies, and even individuals, all of whom seek to control and achieve huge profits.

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

Third: Spyware

Spyware are computer programs that are installed surreptitiously on computers to spy on Users, and partially control the personal computer without the user's knowledge and spyware are secret programs that monitor users' behavior and collect various personal information, it controls the computer and steals sensitive information (4).

Fourth: Economic intelligence

Economic intelligence is defined as: "All approaches to managing and analyzing information collection and analysis techniques with the aim of revitalizing and improving the work of the state, companies, international organizations, and non-governmental organizations working in the economic field."

Economic intelligence is taught in specialized research centers, and is carried out through economic channels that provide information to economic actors (media, public documents, international forums, research centers), which is then analyzed by economic experts and translated into economic policy (5).

Economic intelligence was coupled with the emergence of the knowledge economy and the tremendous development of media and communication technology, as the working group in the General Directorate of Planning in France presented a practical definition of economic intelligence as: "a set of coordinated activities of research, processing, and disseminating useful information to economic agents and stakeholders to formulate their strategies" (6).

The highest official in charge of economic intelligence in France, Alain Juillet, while he believes that Economic intelligence, "includes controlling and protecting strategic information for all economic agents in order to reach competition in the economic field, economic security, institutional security, strengthening the policy of influence" (7), and providing strategic information that allows for good identification of the activity and axes of development of the institution in light of a business environment characterized by continuous development and extreme complexity.

Information security can relate to protecting the national economy from all forms of economic espionage and piracy of production methods and plans. **Possession of information represents the first element of economic intelligence.**

The difference between economic espionage and economic intelligence appears in whether the means used to obtain information are legitimate or illegitimate?

Fifth: Economic security

It is the basic interests of the nation, that is, arranging the basic elements of the nation's economic and scientific energies, as the state alone is no longer responsible for economic security, but rather all institutions are obligated to participate (8).

Sixth: Hackers

He is the person who creates and modifies software, and they mean young adults associated with informatics. There are those called (young information geniuses), and most of them are students and young people who have knowledge in the field of technology. They are also called information hackers, and their goal is sabotage and not for other purposes (9).

Seventh: Crackers

They are the adult criminals or vandals involved, often between the ages of 25 and 45, and professional hackers are among the most dangerous perpetrators of crimes.

Eighth: 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) (10).

Section Two: The historical development of the crime of electronic espionage, its characteristics and its impact on the security and sovereignty of states

We will divide this research into three (03) elements

First: The historical development of the crime of electronic espionage

Stansfel dterner, director of the intelligence agency under US President Jimmy Carter, says:" If we are spying for reasons of military security, why not spy for economic security?" Turner pointed out in 1992 that the United States of America should carry out more aggressive intelligence operations with the aim of securing the leading American economic position in the world (11).

The first economic espionage operations were during the seventies and eighties, when France planted spy agents in my company, Album and Texas Instruments, and they transferred the information they obtained to a French computer company, the microphones that are installed in the seats of Air France planes to capture the debate between traveling businessmen have 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," adding, "The United States has the most relevant and easily accessible technological information, so it is natural for your country to receive the greatest amount of attention from the intelligence services" (12).

It is worth noting that the Director of the Central Intelligence Agency, Robert Gates, was the one who laid the foundations for the concept of economic espionage in the early nineties. This concept was taken by American spies, who in 1995, according to the New York Times, spied extensively on Japanese officials participating 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, a European Union official who handles competition policy and other issues was targeted, and the National Security Agency, according to the New York Times, targeted servers belonging to the Chinese telecommunications giant Huawei under the pretext of its relationship with the Chinese military.

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, by hacking into American computer networks to steal useful data for commercial competitors of the United States of America.

In an effort to control the markets of the Asian continent, the United States of America is working to recruit all its spies who are experts in advanced technology to carry out electronic economic espionage using the temptation of money and advantages, and the best evidence of this is the American-Chinese economic war and the imposition of the.M.Chinese goods are subject to high fines and taxes estimated at billions of dollars, as well as fines for the Chinese telecommunications giant Huawei.

On the other hand, China is also working in the same direction as U.S.A 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 on the European aircraft manufacturing giant Airbus of stealing information related to equipping A200M aircraft engines for military transport, as well as stealing a set of electronic systems that help fly the plane, and China denied this in late September 2019.

It is worth noting that China has flooded Europe, America and developing countries with its technical and economic spies. The German Intelligence Agency also accused in a report that all active countries in the world (Russia, U.S.A, China, Britain...) by scrambling and struggling to collect scientific and technological information, whether in developed or developing countries, she stated that everyone is spying on everyone, and in all economic, agricultural, industrial fields...Etc.

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 (13).

The French White Paper for the Defense of National Security in 2013 also referred to the national perception of the risks of an attack on the information system, which identified two major dangers threatening France: "cyber espionage and electronic sabotage of sensitive infrastructure"

The methods and weapons of electronic economic espionage have become advanced by recruiting hackers in exchange for a blank check, recruiting members of the targeted country who oppose the regime in exchange for luring them to decision-making centers, or by planting spyware in the company's devices and networks, or spying by planting malicious software in computers via emails in order to collect information, usernames and passwords Or destroy the company's business programs that were spied on and its information base.

In this context, we can point out the most famous cases of economic espionage and electronic economic espionage in various historical stages of the world. Among the forms of espionage, the following examples can be listed (14): The Byzantines broke the Chinese monopoly when Emperor Justinian sent monks to China to learn the secret of silk. They returned with silkworms hidden in their luggage.

Between 1987_1989, the FBI discovered F.b in the United States of America, French intelligence spied on a number of American electronics companies, such as "I".BM and Texas Instrument for the French state-owned computer company, Company des Machines Bull, have been different its methods range from electronic surveillance to trying to recruit individuals who are dissatisfied with American companies.

An English immigrant named Samuel Slater also established a factory, the first of its kind for water-powered textiles in America, by relying on technologies from his country. The British judiciary criminalized him and issued the death penalty against him for stealing trade secrets. The English described him as "the traitor Slater."

-In 2004, hackers in Shanghai working for the Chinese company Hawaii hacked the Canadian communications network Nortel.

- At the end of 2019, the German car manufacturer "B" was accused.Um. Vietnamese hackers attempted to hack into its networks, and Hyundai and Toyota reported similar activities.

- In February 2021, Sweden accused one of its citizens –a technical advisor – of passing trade secrets, including codes belonging to Skansa and Volvo, to a Russian diplomat in exchange for several thousand dollars.

Second: 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 is a global crime that transcends 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, and it is difficult for the technician to preserve its traces if they exist, as it requires special technical expertise that the average investigator cannot deal with easily, due to the presence of special programs, secret words, codes and symbols that hinder access to evidence Therefore, the investigator must be a technology expert and use the same weapon that the hackers relied on, which can delete information and data that could be used as evidence against him.

3-The crime of electronic economic espionage is a soft, calm crime that does not require muscular effort, force, violence, or the use of weapons, but rather intellectual effort and great knowledge of the secrets of computers, some computer programs, and the Internet.

4-The modernity of the laws related to electronic economic espionage crimes is the same as those related to information crime. The first law that stipulated them was in France under Law No. 88/19 dated January 5, 1988, while the Algerian legislation was in 2001.

5-The jurisdiction of judicial police officers is exceptional in the crime of electronic economic espionage. In Algeria, jurisdiction to combat these crimes devolves to the criminal pole specializing in crimes related to media and communication technology.

Third: The impact of the crime of electronic economic espionage on the security and sovereignty of states

The crime of electronic economic espionage aims to:

- Destabilizing the security of countries and governments, as the latter become constantly concerned about their secret economic information, and become the subject of bargaining by hackers or spies, whether individuals or governments of other countries, and this bargaining can be in an economic, military or political form.

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

- Electronic economic espionage and its various types (individuals, organizations, governments..) He can exploit citizens of developing and poor countries, by recruiting them to serve him while tempting them with financial and even political privileges, which is to reach power, which could be through military coups supported by major powers...Etc., which leads to instability. In this regard, the spokesman for the Russian Kremlin, Dmitry Pskov, stated that the BRICS group considers electronic espionage to be terrorism and a threat 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, which is information security of an economic nature.

- The impact of the crime of electronic economic espionage on international relations and policies, which leads to the management of international conflicts and the pursuit of hegemony over international relations. The crime of electronic economic espionage affects the financial revenues of countries, causing countries to lose billions of dollars.

The third topic: Mechanisms to combat the crime of electronic economic espionage and the position of the Algerian legislator on it.

First: Mechanisms to combat the crime of electronic economic espionage

Counter-espionage is one of the precise and main tasks in security work, and considering the crime of electronic economic espionage a serious crime that affects the national security of any country, just as

there must be an intelligence agency for espionage and hacking, there must be, in return, an intelligence agency whose mission is the component of hacking (15).

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

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

They are as follows:

- Using 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.

- Switching codes and applicable 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 forming hackers to combat hacking.

- 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, especially in combating information crimes, combating electronic espionage, and monitoring the security of information and systems.

2- The National Criminal Pole for Combating Crimes Related to Media and Communication Technologies as a Judicial Mechanism to Combat Economic Espionage:

The establishment of a specialized national criminal hub to combat crimes related to media and communication technologies did not come by chance, but rather was the result of the specificity of this type of crime as it is technical and committed in a digital environment and is difficult to investigate and follow up on.

In line with the widespread use of modern media and communications and the spread of cybercrimes, especially those affecting Algerian national security, the Algerian legislator intervened pursuant to Order 21-11 of August 25, 2021 amending and accusing the Code of Criminal Procedure (Order 66-156), which established a criminal pole with national jurisdiction to combat crimes related to media and communication technologies, as Article 211 bis 22 of Order 21/11 stipulated that:" A national criminal pole shall be established at the level of the court headquarters of the Algerian Judicial Council, specializing in the follow-up and investigation of crimes related to information and communication technologies and crimes related to them “referring to Article 211 bis 23 of Order 21-11, we find that it maintains the same definition of information crime mentioned in Article 2 of Law 09-04 mentioned above, as Article 211 bis 22 stipulates that crimes related to information and communication technologies are: "Any crime committed or facilitated by the use of an information system, an electronic communications system, or any other means or mechanism related to information and communication technologies."

Article 211 bis 24 of the Q.E.C The crimes stipulated in Order 21-11 that constitute misdemeanors as follows: "Taking into account the provisions of paragraph 2 of Article 211 bis 22 above, the Public Prosecutor at the National Criminal Pole for Combating Crimes Related to Information and Communication Technologies, the investigating judge and the head of the same pole shall have exclusive jurisdiction to follow up, investigate and adjudicate the crimes related to information and communication technologies mentioned below, as well as the crimes related to it.

- Crimes affecting state security or national defense.

- Crimes of publishing and promoting false news among the public that could harm security, public tranquility, or the stability of society.

- Crimes of publishing and promoting malicious news that affects public order and security of an organized or transnational nature.

- Crimes of tampering with automated data processing systems related to public administrations and institutions.

- Crimes of trafficking in persons or human organs or smuggling migrants.

- Crimes of discrimination and hate speech.

The National Criminal Pole for Combating Crimes Related to Information and Communication Technologies has exclusive jurisdiction over the most complex crimes or crimes related to them, according to the text of Article 211 bis 25 Q.E.C "Taking into account the provisions of paragraph 2 of Article 211 bis 22, The Public Prosecutor at the National Criminal Pole for Combating Crimes Related to Information and Communication Technologies, as well as the investigating judge and the head of the same pole, are exclusively responsible for following up, investigating and adjudicating crimes related to the most complex information and communication technologies and crimes related to them.

The most complex crimes related to information and communication technologies, as defined by this law, mean a crime that, given the multiplicity of actors, partners or victims, or due to the vast geographical area of the place where the crime was committed, or the seriousness of its effects or consequences, or its organized or transnational nature, or its violation of public order and security, requires the use of special investigative means and specialized technical expertise, or resorting to international judicial cooperation.

In addition to the exclusive specific jurisdiction of the National Criminal Pole to combat crimes related to information and communication technologies, there is a joint jurisdiction stipulated in Article 211 bis 27, whereby the Public Prosecutor, the investigating judge and the head of the National Criminal Pole to combat crimes related to information and communication technologies exercise joint jurisdiction with the jurisdiction resulting from the application of Articles 37, 40 and 329 of this law with regard to crimes related to information and communication technologies and crimes related to them.

3- Mechanisms of an international nature

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

Among the international agreements that aim to curb economic espionage practices is the TRIPS Agreement, which urges WTO members and those who join this agreement to protect intellectual property rights and confidential information of commercial value. This agreement allows for the application of criminal penalties in the event of infringement of intellectual property rights.

The US Economic Espionage Act, enacted in 1996, punishes anyone who spies and steals trade secrets with the aim of benefiting another government, a foreign means or agent with a fine of up to $500,000, or 15 years in prison, or both. Commercial companies that steal trade secrets are fined $5 million if their purpose is to achieve private gain and $10 million if it is for the benefit of a foreign government.

To combat or reduce this crime, cooperation between countries must be strengthened, through exchanging information and tracking down spied hackers, as well as strengthening and encouraging cooperation between police agencies between member states of the International Criminal Police Organization (Interpol), as well as Strengthening regional and security cooperation in combating the crime of electronic economic espionage, through private organizations such as Afripol among African countries.

Add to this the need to enhance judicial cooperation between countries, by adopting bilateral or multiple judicial agreements to receive and extradite electronically hacked criminals, direct international judicial delegations, and publish arrest warrants for those wanted internationally.

Second: The position of the Algerian legislator on the crime of electronic economic espionage

Despite the difficulty of controlling and combating the crime of electronic economic espionage, considering it the most serious information crime that threatens the security of countries, the Algerian legislator, as a result of the pressure of technological development in the field of information technology, tried to establish some legal texts that criminalize these acts by amending the Penal Code in 2004 by Law No. 04/15 dated November 10, 2004 under the title "Infringement of Automated Data Processing Systems", which includes eight articles from Article 394 bis to Article 394 bis7.

With regard to espionage and terrorism crimes, the Algerian legislator doubled the penalty due to their seriousness, according to the text of Article 394 bis3, which states: "The penalties stipulated in this section shall be doubled if the crime targets the national defense or bodies and institutions subject to 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 amendment to the Penal Code was in 2024.public law, without prejudice to the application of penalties."

In line with the Penal Code, the Algerian legislator amended the Code of Criminal Procedure by Law No. 06/22 of December 20, 2006. In Article 37, the legislator extended the territorial jurisdiction of the Public Prosecutor in cybercrimes, and also extended the jurisdiction of judicial police officers. Even searches in such crimes are of a special nature, as judicial police officers can intercept correspondence, record votes, and take photos, according to Article 65 bis5/10 of Q.E.C.

Finally, the Algerian legislator came up with a special law to prevent and combat crimes related to information and communication technology, including the crime of electronic economic espionage, which is Law No. 04/09 dated August 5, 2009, which includes the rules for preventing and combating crimes related to information and communication technology, as information systems can be inspected when necessary and information data seized.

To confront the seriousness of the crime of electronic economic espionage, the Algerian legislator established a national body for the prevention of crimes related to information and communication technology pursuant to Law No. 04/09 of August 5, 2009. The presidential decree issued in 2015 clearly regulated it, one of whose tasks is to activate international judicial and security cooperation, Coordinating preventive operations and technical assistance to judicial and security authorities in the event of an attack on an information system in a manner that threatens the strategic interests of the national economy.

In addition, specialized criminal judicial bodies were established pursuant to Law No. 04/14 of 10/01/2004 amending and supplementing the Code of Criminal Procedure. They are responsible for examining cybercrimes targeting state institutions, the economy, and national defense, which were replaced by the 2021 amendment to the Code of Criminal Procedure, which stipulated a specialized criminal hub for examining crimes related to media and communication technology.

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

Finally, the Ministry of National Defense, which created the "Cyberian Defense and Systems Security Monitoring Service" at the level of the Information and Preparation Department, aims to secure and protect the country's vital systems and facilities against threats, electronic terrorism, and spying on the

economic secrets of the Algerian state. This will protect Algeria's security and sovereignty, through a rapid response to breaches and interference with spy devices.

Conclusion:

This study shows the seriousness of the crime of electronic economic espionage on 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 and dominate its wealth. These wars have become fiercer recently, especially between the two U.S and China, as this crime affected international relations and became a means of sowing strife and conflicts in countries around the world. Considering that Algeria is a country in this international community and as a result of the tremendous technological development, it always remains targeted by hackers, therefore the level of caution must be raised and information security must be controlled in an effective manner, by training cadres in modern technology with the training of judicial police officers specialized in information security, And judges specialized in combating this type of crime, as is the case in U.S.A, which enacted the Economic Espionage Act in 1996, signed by US President Bill Clinton, which aims to protect the interests, information and data of American companies, in light of the presence of a number of foreign entities seeking to steal trade secrets. The legal texts must also be amended in line with the technological developments taking place while enhancing judicial and security cooperation between countries.

Bibliography:

1- Official Gazette, No. 47 issued on 08/16/2009.
2- Electronic espionage, an article published online on 04/10/2009, taken from the Moroccan newspaper Al-Ittihad Al-Ishtiraki, without mentioning the author, p. 1.
3- Fouad Barami, Electronic Espionage, Its Characteristics and Objectives, an article published online on 12/13/2018 at 18:24, pp. 1 and 2.
4- Wikipedia, the free encyclopedia, April 2019.
5- 5 and 6 – Hamdani Muhammad, The importance of economic intelligence in improving business suitability and attracting foreign investments, Algerian Institutions Performance Magazine, Issue 02/2012, pp. 12 and p. 13.

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

8- Fadhila Aqli, 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.

9- Abdel Fattah Murad, Explanation of Computer and Internet Crimes, Egyptian National Library and Archives, 2005, p. 65, reference referred to in, Fadhila Aqli, previous reference, p. 6.

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

11- Elias Grohl, Swedish writer and political analyst, economic espionage...A New Intelligence Target, an article published in the Emirati electronic newspaper Al-Ittihad, dated 05/28/2014, without a page.

12- Elias Grohl, op. cit., no page.

13- Hamad bin Abdullah Al-Luhaidan, Economic Espionage: The Most Important Axes of Economic Wars, an article published in Al-Yamamah Magazine, electronic version, Bahrain, 11/25/2005, issue 13668, without mentioning the page.

14 – Economic espionage....Stealing trade secrets to destroy competitors, Al Jazeera report dated August 1, 2022, published on the website, browsed on April 4, 2025 at 16:47 pm.www.aljazeera/net.

15- 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.

References:

1-Books:

1- Abdel Fattah Murad, Explanation of Computer and Internet Crimes, Egyptian House of Books and Documents, 2005.

2-Legal texts:

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

2-Order No. 21-11 of August 25, 2021 supplementing Order 66-156 of June 8, 1966 containing the Code of Criminal Procedure, Official Gazette No. 65 issued on 08/26/2021.

3-Articles:

1-Elias Grohl, Swedish writer and political analyst, economic espionage...A New Intelligence Target, an article published in the Emirati electronic newspaper Al-Ittihad, dated 05/28/2014, without a page.

2-Bashir Al-Wandi, The importance of the counter-espionage apparatus in protecting the national security of the state, European Center for Counter-Terrorism and Intelligence Studies, March 16, 2018.

3-Hamdani Mohamed, The importance of economic intelligence in improving business suitability and attracting foreign investments, Algerian Institutions Performance Magazine, Issue 02/2012.

4-Hamad bin Abdullah Al-Luhaidan, Economic Espionage: The Most Important Axes of Economic Wars, an article published in Al-Yamamah Magazine, electronic version, Bahrain, 11/25/2005, issue 13668, without mentioning the page.

5-Fadhila Aqli, Cybercrime and Measures to Confront It Through Algerian Legislation, Proceedings of the Fourteenth International Conference, Cybercrime, Libya, Tripoli, March 24 and 25, 2017.

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

7- Electronic espionage, an article published online on 04/10/2009 taken from the Moroccan newspaper Al-Ittihad Al-Ishtiraki, without mentioning the author.

8- Wikipedia, the free encyclopedia, April 2019