CORPS & PSYCHISME
P-ISSN: 2496-4476 E-ISSN: 2273-1571
Volume 13/ Issue 1/ 2026

Cybersecurity: Reading In Terms And Concepts

Bekkaddouri Azzedine[1]
Email. azzedine.bekkaddouri@univ-bechar.dz
Yahiaoui Sid Ahmed[2]
Email. yahiaoui.sidahmed@univ-bechar.dz
Cherrad Souhil[3]
Email. cherrad.souhil@univ-bechar.dz
[123]Tahri Mohamed University – Bechar (Algeria)

Received : 16/08/2025 ; Accepted : 27/12/2025 ; Published : 13/03/2026

Abstract:

The technological revolution currently sweeping the world has had numerous social, economic, and political repercussions, damaging international relations and embroiling many governments in conflicts and wars involving various weapons and military equipment. However, the most prominent threat facing humanity as a whole is cybersecurity, or what is known as cyberattacks, which have become the theater of electronic space, replacing traditional conflicts and wars. Powerful nations use these attacks to target other nations' information systems in an effort to compromise their networks, take control of them, and ultimately dominate global communications and information systems.

Keywords : cybersecurity, cyberwarfare, cyberattacks, cybercrime

1. Introduction

The issue of cyberwarfare and similar terms has become a burden on peoples and governments due to its negative repercussions on various sectors and fields, especially those related to the economies and defenses of countries at the regional and global levels, thus directly affecting international relations due to the damages produced by cyberspace that threaten the peace and security of countries. The development of the Internet and the ensuing technological revolutions have also had a significant impact on the stability and unity of peoples, as well as the future of individuals and groups. This is particularly true given the acceleration of electronic security threats, also known as electronic information warfare.

Far from the traditional methods that have characterized the various wars that humanity has known for decades, Algeria, like other countries around the world, has hurried to adopt a security policy that preserves its economic and military secrets. This is represented by electronic management that protects the nation's information system through numerous security and civil agencies. Modern technology is becoming an essential component of modern warfare, and the world is currently witnessing a new kind of war where the victor is the one who is adept at negotiating in cyberspace. The nature and elements of this war are extremely difficult to define, and there are corresponding criminal or civil consequences and responsibilities at the local and international levels. This is best demonstrated by the extremely high rates of cybercrime, which undermine national infrastructure, including networks, systems, and electronic data, and endanger morals and values.

In this article, we will provide a detailed explanation of concepts directly related to the term cybersecurity, by addressing the following elements :

The first axis : The concept of cyber security and cybersecurity.

The second axis : Cyberwar.

The third axis : Cybercrime.

The fourth axis : Cybercriminal.

Definition Cybernetics :

A/Linguistic Definition of Cybernetics :

The word cybernetic is derived from the Greek word (kybernetes), which was first mentioned in science fiction books, and it meant the captain of the ship; this word was previously used by the philosopher Plato during his dialogues about the art of captaining the ship.(Al-Fatlawi, 2016, p 05) Referring to the language dictionaries, the “Al-Mawrid” dictionary defines the word “cybernetics” as the science of control, i.e., controlling and dominating things.(Al-Baalabki, 2017, p 307) Le Petit Larousse defines cyber as "the science that studies the mechanisms of communication and control of machines and other living beings".(Larousse, p 104) The Oxford dictionary defines it as “The study of the effectiveness of human work by comparing it with the effectiveness of computers, and it is related to the features and characteristics of computers, information technology, and virtual reality” .(Oxford, p 299)

B/Technical definition of cybernetics :

Norbert Wiener sees the modern terminological source of cybernetics as the science of driving or controlling living things and machines and the study of the mechanisms of communication in each.(Diaa, 2017, p 56)"Bray Walter" defines it as: The science of mental machines.(Mona Abdulah, 2020, p 34)

2-1 The concept of CyberSecurity :

Cybersecurity is the activity that ensures the protection of human and financial resources related to communication and information technologies and ensures the possibility of reducing losses and damages that result in the event of risks and threats. It also provides the opportunity to restore the situation to what it was as quickly as possible so that the wheel of production does not stop and the damages do not turn into permanent losses.(Mokhtar, 2015, pp 5-6) It is a set of technical, organizational, and administrative means that are used to prevent unauthorized use, misuse, and recovery of electronic information, communications systems, and the information they contain, with the aim of ensuring the availability and continuity of the operation of information systems, enhancing the protection, confidentiality, and privacy of personal data, and taking all necessary measures to protect citizens and consumers from risks in cyberspace.(Al-Baalabaki, 2017, p 212) The International Telecommunication Union defines it as “a set of tasks, such as the collection of means, policies, security procedures, guidelines, risk management approaches, training, practices, and techniques, that can be used to protect the cyber environment, organizations, and users."(Essaid, 2010, p 365)

Cybersecurity, also called "information security" and "computer security," is a branch of technology concerned with protecting systems, assets, networks, and programs from digital attacks that typically aim to access, change, or destroy sensitive information; extort money

from users; or disrupt cybersecurity. (Jabbour, 2017, p 25) It is also known as "the sum of the means that aim to reduce the risk of attack on software or computer hardware and networks." These include tools used to combat hacking, detect and stop digital viruses, and provide encrypted communications. (Khalifa, 2014, pp 33-42)

3-1 : Purposes of Cybersecurity :

- Addressing information security attacks and incidents targeting government agencies and public and private sector institutions.
- Providing a safe and reliable environment for transactions in the information society.
- Resilience of sensitive infrastructure to cyberattacks.
- Providing the requirements to reduce risks and cybercrimes targeting users.
- Eliminate vulnerabilities in computer systems and mobile devices.
- Closing gaps in information security systems.
- Resisting malware and the severe damage it causes to users.
- Reducing cyber espionage and sabotage at the government and individual levels.
- Protecting individuals and consumers from potential risks in various areas of Internet use.
- Training individuals on new mechanisms and procedures to address the challenges of computer hacking. (Mona Abdullah, 2020, p 10)

4-1 : Benefits of cybersecurity :

The most important benefits of cybersecurity can be summarized as follows :

- Protect networks and data from unauthorized access.
- Improve information security and ensure business continuity.
- Enhance the confidence of shareholders and stakeholders in the company.
- Recover leaked data faster in the event of a cyber security breach. (Mona Abdullah, 2020, p 10).

5-1 : Cyber security Elements :

To achieve cybersecurity, a set of elements must be available that work together, the most important of which are the following :

1-5-1 : Technology is crucial to people's and businesses' lives because it offers them the best defense against cyber attacks. This includes securing networks, computers, and smart gadgets in all their forms by using firewalls and antivirus software, among other measures. (Al-Amarat, 2022, p 36)

1-5-2 : People who use data and systems in an organization should use basic data protection principles such as choosing a strong password, avoiding opening external links and attachments via email, and making backup copies of data. (Al-Amarat, 2022, p 36)

6-1 : Cyber security Challenges :

Cyber security elements include all of the following :

- Network security.
- Application security.
- Computer security.
- Data security.
- Database and infrastructure security.

- Computer systems security.
- Phone security. (Jabbour, 2021, p 36)

7-1 : The Future of Cybersecurity in Algeria in Light of the Current Challenges :

In order to achieve cyber security in Algeria, the National Gendarmerie and National Security Services must overcome numerous barriers and difficulties. The following are some ways that we can sum them up:

- Increase in the number of Internet users (more than 10 million subscribers in Algeria)
- The spread of high-speed Internet technology and streaming.
- Technological development. The criminal no longer needs to sit behind computers connected to the Internet to commit his crime.
- Wide use of social networks. (More than 7 million users in Algeria)
- Stealth operations while using Internet services.
- Lack of coordination between countries and governments, especially since cybercrime is a crime that crosses borders and continents. (Bara, 2012, p 03)
- Spread awareness of the concept of cyber security among Internet users.

II- Cyberwar :

The traditional definition of war entails the use of regular armies, followed by a battlefield and a clear declaration of war. However, in the modern era, military armies from all over the world, particularly major nations, have developed an interest in cyberwars, where their attacks have undefined durations, unclear goals, and cross international borders.(Adel-Abdullah, 2017, p 09) While controlling the opponent's will and decisions was the aim of cyberwars, the objective of conventional conflicts was to destroy the opponent by invading his territory or stealing his resources. Network warfare and cyberspace warfare are the two most significant types of warfare in the information era. (Adel-Abdullah, 2015, p 02) The definition of cyber warfare depends on the context of the attacks. According to one definition, "Internet-based conflicts and attacks driven by political goals on information and its systems can result in the disruption of official websites and communication networks, (Jabbour, 2021, p 71) the interruption of critical services, the theft of private data, and the paralysis of the financial system".

Cyber warfare is defined as : “The use of the electronic or electromagnetic spectrum to store, modify and exchange data face-to-face with control systems in associated infrastructures”. (Nadjib, 2021, p 222)

2-1 : Objectives of cyberwarfare :

- Destroying or altering data without the owners' knowledge, which could cause a catastrophe if it is used without them realizing what has happened
- Espionage and gathering information about the opponent, and the targeted information is usually a military, economic, political, or industrial secret.
- Destroying or disabling a facility or organization by disrupting the computing systems that it operates or controls.

- Obtaining information, distorting information, or leaking information, and then publishing it in order to influence the course of events. Such as hacking the emails of prominent international figures in various specialties. (Ahmed, 2022, pp 237-238)

2-2 : Actors in the field of cyber warfare :

Besides countries, we find :

2-2-1 : Individuals who have high technical knowledge in the field of information technology and the ability to employ it, and it is usually difficult to reveal their identities and then pursue them.

2-2-2 : Multinational corporations where major technology companies have cyber capabilities that exceed many countries, such as Google, Face book, Apple, Amazon,

2-2-3 : Criminal Organizations : These organizations carry out many cyber attacks with the aim of stealing information or money or blackmailing to obtain money as well.

2-3 : Characteristics of cyber warfare :

Cyber wars are distinguished from traditional wars by a set of characteristics, including :

- Cyber warfare is sophisticated technological warfare that centers around the Internet.
- Cyber warfare is characterized by speed and evasiveness, which gives the attacker a clear advantage over the defender.
- Cyber warfare is a war with undefined goals and impact, as its risks may extend beyond traditional battlefields to affect the most sovereign and sensitive locations.
- Known deterrence models fail because cyber warfare often leaves no trace or evidence of its occurrence. (Chouirib, 2023, p 163)

III : Cybercrime :

A set of illegal acts and activities that are carried out via electronic equipment or devices over the Internet and require special control of computer technology and information systems to commit, investigate, and prosecute their perpetrators. (Khalifa, 2012, p 43) It is all forms of illegal or socially harmful behavior that are committed using a computer. (Salah, 2017, p 24) It is defined as: “Any criminal act in which a computer is used as a primary tool”(Al-Omari, 2020, p 42) . It is also known as : “a set of legally punishable acts and activities that link the criminal act with the technological revolution”. (Madien, 2020, p 29) Cybercrime is: “anything that occurs on networks, information technology systems, operating systems, and their components with the intent to penetrate, disrupt, use or exploit any project.” (Dalali, 2021, p 538)

3-1 : Causes of Cybercrimes :

- Desire to gather and learn information.
- Information capture and trafficking.
- Conquering the regime and proving superiority over the development of technical means.
- Harm to individuals and governments.
- Achieving profits and material gains.
- Threat to national and military security. (Aatef, 2020, p 35)

3-2 : Types of Cybercrimes :

Cyberspace can be used to conduct a variety of crimes, and users may be exposed to or complicit in them without realizing it:

- The act of imitating the site or a real or fictional person.
- Targeting and altering web pages. A rival could access a rival business's website that showcases its products and change the prices listed.
- Manipulation in e-ecommerce.
- Viruses that tamper with operating systems, disrupt business, and help create confusion, disorder, and insecurity in the use of this medium.
- Moral crimes such as sex, advertisements for vices, and blackmailing some people. (Aatef, 2020 p 37)

3-3 : Motives for committing cybercrimes :

The motives for committing cybercrimes are as follows :

3-3-1 : Making profits and material gains : The financial motive for committing cybercrimes is one of the most important motivations that motivate cybercriminals to commit them, due to the huge financial returns they achieve.

3-3-2 : Conquering the regime and proving superiority over the development of technical means : Sometimes the motive behind committing these crimes is to subjugate the regime and prove the perpetrator’s ability and superiority over the complexities and development of modern technology. (Research and Studies, 2016, p 29)

3-3-3 : Learning motivation : Given that hackers feel that everyone has the right to access and profit from the data stored on computers and systems and that it is not a private property, their passion for learning and exploration is thought to be one of the primary drivers behind these types of crimes. (Al-Hamadani, 2014, p 69)

3-3-4 : Political or ideological motive : It is done by anti-government criminals, by vandalizing government websites or hacking government accounts on social media platforms such as Twitter and Facebook to spread incorrect news and information with the aim of stirring up discord in public opinion.

3-3-5 : Revenge motive : One of the most harmful motivations used by cybercriminals is retaliation. This includes exacting revenge on individuals for private gain, such as a former employee who was let go from the company where he was employed.

3-3-6 : Entertainment and fun : Quite a few hackers consider their work a means of fun and entertainment and spending as much time as possible on other people's systems and computers. This hacking is often peaceful and without any noticeable impact. (Aatef, 2020, p 70)

3-4 : Characteristics of Cybercrime :

Cybercrime is characterized by a set of characteristics, the most prominent of which are :

3-4-1 : The international nature of cybercrime : (Transnational and transcontinental) : It challenges the local and international system, as an international character often dominates it. It is a cross-border crime and may include more than one foreign element. The criminal act may occur in a specific country, and the criminal result may be achieved in another country or countries. (AL6Khalidi, 2018, p 14)

3-4-2 : Soft crime is easier to commit : Cybercrime does not require violence or physical effort to commit, as it requires a kind of mental awareness and thinking based on knowledge of computer technologies. (Al-Hashemi, 2019, p 51)
3-4-3 : Speed of implementation : One of the characteristics of cybercrime is the speed with which it occurs, as damage may occur even before the victim is aware that they are being targeted, which may not allow the victim to defend themselves.
3-4-4 : Committed through technical means : Due to the special nature of this crime, it is committed in an electronic environment, which requires the perpetrator to use technical means and devices, such as a computer, in addition to the fact that it is committed over the Internet. (Habybah, 2022, p 39)
3-4-5 : A crime that is difficult to detect : It is one of the crimes that leaves no trace to be observed and followed up, as the perpetrator uses techniques that prevent access to him or knowledge of the technique by which he committed the crime.
3-4-6 : A crime that is difficult to prove : It is a crime that occurs in cyberspace, and the evidence it leaves behind is electronic, as the cybercriminal can get rid of the physical traces of their crime thanks to the techniques and skills used, such as hiding their identity or confusing investigators. (Sikkar, 2010, p 42)

:5-3 Elements of Cybercrime :

Cybercrime has the following elements :
3-5-1 : The Virtual Aspect : It is the presence of an electronic device, usually a computer, as a hypothetical element that constitutes the means used to commit the criminal behavior of the physical element in the digital environment connected to the Internet. (Al-Baqli, 2010, p 21)
3-5-2 : Material Aspect : The illicit activities and technological activity related to computers and the Internet constitute the material element of cybercrimes. Depending on the crime, the material element might take many different forms. For example, the criminal may prepare the computer to perform the crime by loading it with hacking software or otherwise preparing it. (Al-Hussainawi, 2018, p 74)
3-5-3 : Moral Aspect : The moral element in cybercrimes is represented by the general criminal intent represented by the elements of knowledge and will, such as the intentional introduction of an information program or the dissemination of viruses on the information network or electronic information system or any other intentional act such as flooding, disabling, damaging the contents of, or stopping a website. (Al-Gamal, 2015, pp 37-38)

3-5 : Algerian Authorities responsibility to Combat Cybercrime :

- National Office of Copyright and Neighboring Rights.
- National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies.
- National Authority for the Protection and Promotion of Childhood.
- National Authority for the Protection of Personal Data.

3-7: Cyber crime in International law:

European Council of Governments negotiated the first treaty (approved in Brussels on November 23, 2001) to address the transnational nature of cybercrime. It was the first convention to address the global nature of cyber crime, and it came into effect in January

2002 after being ratified by five signatory nations, three of which were required to be from the European Union Council.

3-8 : Legislative and Legal Mechanisms to Combat Cyber crime in Algeria :

As evidenced by the issuance of Law No. 09/04 dated August 16, 2009, which includes special rules for preventing and combating crimes related to information and communication technologies, it primarily focused on the field of taking legal measures without taking any other measures. This law determined the circumstances in which it is acceptable to use electronic communication monitoring.

Based on what was stated in Article 4, which states the following :

- To stop actions categorized as crimes against state security, terrorism, and sabotage.
- In the event of information about a possible attack on an information system that threatens public order, national defence or state institutions.
- For the requirements of investigations and judicial inquiries. (Aamish, 2022, p 385)

By issuing Presidential Decree No. 15-261 on October 8, 2015, which establishes the structure, composition, and procedures of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies. (Law, 2009, p 06) the same law's Article 13 allows for the creation of a national body to prevent and combat crimes involving ICTs.

The tasks carried out by the Authority include those stated in the decree, which states the following :

- Proposing elements of the national strategy related to information and communication technologies and combating them.
- Assisting security services in combating crimes related to information and communication technologies.
- Collecting, recording, storing and identifying the source of digital data for use in legal proceedings.
- Contribute to updating legal standards in its field of expertise. (Boualam, 2016, p 39)

IV- Cybercriminal :

4-1 : Definition of the cybercriminal :

A cybercriminal refers to a criminal with a high level of intelligence, as he uses his technical skills to hack networks, crack codes and passwords, and employ his skills in storing data and information and controlling electronic network systems. He has no sense of the illegality of his actions or that he does not deserve punishment. He also lacks feelings of guilt, and the cybercriminal usually has a distinguished position in society ,(Al-Amarat, 2022, p 81)

4-2 : Characteristics of the Cybercrimes Perpetrator :

The perpetrator of cyber crimes is characterized by a set of characteristics, which are as follows :

4-2-1 : The perpetrator was intelligent : The perpetrator of these crimes has an unconventional outlook, given that he is often described as having a high degree of information intelligence, which makes it difficult to classify him according to the usual criminal classification. (Al- Masry, 2012, p 52)

4-2-2 : A recidivist : Cybercriminals often return to committing other crimes in this area, out of a desire to fill the gaps that led to their identification and prosecution the first time, which leads them to return to crime again. (Nassar, 2017, p 44)

4-2-3 : A specialized and professional criminal : It is easy for an ordinary person to commit cybercrimes unless he is a person specialized in computer and information technology field with a high degree of experience and skill in using it.

4-3 : Types of cybercriminals :

There are several types of cybercriminals :

4-3-1 : Amateurs : They are the ones who commit these crimes for the purpose of entertainment without causing harm to the victim.

4-3-2 : Pirates : delusion :

A/ Hackers : They violate the security of networks and information systems by breaking into computer systems and removing security measures, usually for the sake of self-promotion or curiosity.

B/ Crackers : They are the ones that break into computer systems to access data that has been stored and harm them by either stealing or altering it. To the extent that they establish clubs to share information, they also remotely monitor the most recent news and information and device protection programs.(Al-Amarat, 2022 , p 81)

C/ Pirates/Malicious Hackers : Their goal is to inflict losses on victims, not to gain financial gain, and people in this class include virus inventors and distributors. (Ali-Sikikar, 2010 , p 54)

4-3-3 : Extremist terrorist groups : They are groups that operate under political, social or religious beliefs and ideas, with the aim of imposing their beliefs by resorting to criminal activity through creating special websites and hacking into networks and computer systems.

4-3-4 : Organized groups : Their goal is to commit cybercrimes to achieve financial gain in an illegal manner. They are groups that work in an organized manner, so their actions are described as organized crime, as more than one person participates in carrying out the criminal activity.

4-3-5 : Industry Spies : This category is sometimes considered a subcategory of the criminal group and its objectives are limited to obtaining trade secrets, or extortion for reasons of economic interest. (Refaat, 2018, p 229)

4. CONCLUSION

Ultimately, we can conclude that cyber power has superseded the traditional powers that nations and peoples have relied on for centuries. Wealth, money, and military might alone are no longer enough to have an impact on the world order. The advent of the digital age at the start of the twenty-first century has contributed to the emergence of cyber threats and crimes that now threaten the national security of many countries worldwide, despite the fact that many experts see cyber warfare as an extension of traditional warfare, which frequently uses armies to strike and destroy their opponents' information systems.

Due to the surge in cyber attacks and their quick development, nations are now being forced to think carefully about implementing drastic measures and efforts to safeguard all of their data, particularly sensitive data pertaining to political, military, and economic aspects.

Since they are unable to ascertain the criminal responsibility of those who commit these crimes, one of the biggest problems facing experts in international law is the difficulty of identifying cyber attacks, figuring out their nature and the identities of those responsible, and evaluating their effects and losses. Because of its increased susceptibility to these cyber threats, Algeria is now more worried than ever about cyber security. To stop this hazardous criminal phenomenon that jeopardizes global security and safety, it has started to build an arsenal of local and international processes and means.

6. Bibliography List :

First: Books in Arabic:

Abdul Sabour Abdul Qawi Ali Al-Masry, (2012), The Digital Court and Cybercrime, Law and Economics Library, 1st ed., Riyadh.

Abu Zaid Abdul Rahman Aatef, (2020), Cyber Security in the Arab World, Osama Publishing and Distribution House, Jordan.

Adel Abdel Aziz Saleh, (2017), Evidence of Electronic Crime and its Impact onProof Dar Kunuz Ashbilia for Publishing and Distribution, 1st ed., Riyadh.

Adel Abdel Sadouk, (2017), Cyber Wars: Escalating Capabilities and Challenges to Global Security, Dar Al- Ma'rifa for Publishing and Distribution, Cairo.

Ahmed Amr, (2022), Post-Humanity: Virtual Worlds and Their Impact on Humans, Afak Al-Maarifiah Publishing and Distribution Company, Riyadh.

Ali Jabbar Saleh Al-Husseinawi, (2018), Computer and Internet Crimes, Dar Al-Yazouri, 2nd ed., D.P.N.

Bara Samir, (2012), CyberSecurity: Challenges and Confrontation Requirements, Dar Al Fikr Wal Qanun for Publishing and Distribution, Egypt,.

Bushra Hussein Al-Hamdani, (2014), Electronic Piracy: Weapons of Modern Warfare, Osama Publishing and Distribution House, 1st ed., Jordan.

Diaa Rawan, (2017), The Digital Universe: The Global Revolution in Communications, Hindawi Publishing House, Riyadh.

Essaid Yassin, (2010), Transformations of Nations and the Arab Future, Nahdet Misr Printing, 1st ed.,Cairo.

Fares Muhammad Al-Amarat, (2022), Cyber Security: The Concept and Challenges of the Age, Dar Al- Khaleej for Publishing and Distribution, 1st ed., Riyadh.

Ghada Nassar,(2017), Terrorism and Cybercrime, Al-Arabi for Publishing and Distribution, Cairo.

Haitham Abdel Rahman Al-Baqli, (2010), Electronic Crimes Against Honor: Between Sharia and Comparative Law, Dar Al-Ulum for Publishing and Distribution, Dubai.

Hazem Hassan El Gamal, (2015), Criminal Protection of Electronic Security, Dar Al FikrWal Qanun for Publishing and Distribution, Cairo.

Ihab Khalifa, (2014), Electronic Power and the Dimensions of Transformation in Power Properties, Bibliotheca Alexandrina, Egypt.

Mahmoud Madien, (2020), The Art of Investigation and the Evidence in Electronic Crimes, Egyptian Publishing and Distribution, 1st ed.

Mona Ashqar Jabbour, (2017), Cybernetics: The Obsession of the Age, Osama Publishing and Distribution House, Jordan.

Muhammad Ali Sikikar, (2010), Cybercrime and How to Confront It, Dar Al-Jumhuriya for Press and Publishing, 1st ed., Cairo.

Muhammad Mahmoud Al-Omari, (2020), Introduction to Cyber Security, Dar Zahran Publishing and Distribution, Cairo.

Muhammad Mustafa Refaat, (2018), Public Opinion in Virtual Reality and the Power of Virtual Mobilization, Al-Arabi for Publishing and Distribution, 1st ed., Cairo.

Munir Al-Baalbaki, (2017), The Modern Source, Dar Al-Ulum Lil-Malayin, Lebanon.

Rifaad Ayada Al-Hashemi, (2019), Electronic Terrorism, Dar Amjad for Publishing and Distribution, Amman.

Sari Mohammed Al-Khaled,(2018), Trends in Information Security Art and Security, Al-Obeikan Publishing and Distribution, 1st ed., Riyadh.

Second: French dictionaries:

Le Petit Larousse,(2016), French Dictionnary.

Oxford dictionary, 2013.

Third: Journals:

Adel Abdel Sadouk,(2015), Electronic Power, International Politics Journal, Volume 41, Issue 188, Egypt.

Ahmed IssaNe'ma Al-Fatlawi, (2016), CyberAttacks: Their Concept and the International Responsibility Arising There from in Light of Contemporary Organization, International Investigator Journal, College of Law, University of Kufa, Iraq.

Amish Wahiba, (2022), The Role of National Bodies for the Protection of Digital Worksin Algerian, Legal Journal of Legaland Judicial, Volume 08, Issue 01, University of Medea, Algeria.

Bashir Boualem, (2016), Forum on: The National People's Army and the Challenges of Information Sharing via Social Networks, Army Journal, Military Publications Foundation, Issue 630, Algeria.

Chouirb Djilali, (2023), The Concept of Cyber War and Cyber Security, Journal of Rights and Freedoms, Volume 11, Issue 01, Ag)Watt.

Djalali Dalali, (2021), Cyber security Challenges, Kuwait Law School Journal, Issue 01.

Mohamed Mokhtar, (2015), Can States Avoid the Risks of Cyber Attacks? Ettijahat Haditha (New Perspectives) Journal, Issue 06, Algeria.

Mona Abdullah Al-Sahlan, (2014), Cyber security requirements for administration information systems at King Saud, University, Journal of the College of Education, Issue 111, Mansourah University, Egypte.

Naasib Jabour, (2021), Cyber war fare from the perspective of international humanitarian law, Critical Journal of law and Polotical Science, Volume 16, Issue 04, Faculty of Law and Political Science, Tizi Ouzou, Algeria.

Fourth: Laws

People's Democratic Republic of Algeria, Law No. 9-4 dated 14 Shaaban 1430 AH, corresponding to 05 August 2009,includes special rules for the prevention for crimes

related to Media Communication Technologie and Combating lt, Official Gazette, Issue No. 74, issued on 16 August, 2009