MECHANISMS AND EFFORTS TO COMBAT CYBERCRIME IN ALGERIA

Samira Trad KHODJA
Lecturer, PhD, Mohamed Cherif Messaadia University - Souk Ahras (Algeria)
E-mail: s.tradkhodja@univ-soukahras.dz

Abstract: *Cybercrime is a modern social phenomenon that has surged and dominated the realm of crime due to technological advancements. It is a new mechanism adopted by criminal groups on both global and local levels, amidst the rapid growth of information and communication technologies. Despite the benefits brought about by modern technology, it poses numerous risks and has quickly become a threat to the security and integrity of societies. Although there is a significant gap between developed and developing societies in terms of technology quality, this has not prevented individuals from hastily acquiring it and utilizing its services, while criminals exploit it to commit various types of crimes. Algeria, like other countries, is witnessing an increase in cybercrime rates, and concerns have grown regarding the nature of these crimes, as it is difficult to track and punish the offenders. Through this research paper, we will focus on cybercrime in Algerian society, addressing the most significant types of these crimes, how they are committed, and the various mechanisms to confront them.*

Keywords: cybercrime, internet, cybercriminal, confrontation Mechanisms

1. Introduction

The world today is experiencing a tremendous information revolution, driven by the widespread availability of the internet and mobile technologies. This revolution began in the mid-twentieth century and is considered one of the largest transformations in human history, profoundly impacting individuals, societies, and systems around the globe. Thanks to modern communication and information technologies, the world has become a small, interconnected village, as McLuhan described, enabling access to other realms that would have been unreachable.

In this context, the internet has provided individuals and society with all that previous means of knowledge offered collectively, and even more, by giving access to information that may be forbidden by authorities, represented in the form of the state, religion, or oversight from schools, teachers, or parents. It also offers information that might not have reached us due to geographical, political, or social factors (Bayoumi, 2008: 16). Indeed, this revolution has transformed many concepts, leading to the emergence of what is known as the virtual university, video conferences, e-commerce, and the electronic city. Many community fields have been integrated into this technology, altering their management methods, structures, and even the skill development of the individuals working within them. While some experts claim that communication technology has facilitated direct interaction with specific target individuals despite geographical distances, leading to its recognition as a significant transformation in the realm of communications and information technology, we simultaneously find ourselves grappling, as crime methods have evolved and many criminals now leverage this technology to support their schemes, they have employed the mechanisms of this revolution to gain profits with minimal effort, deceiving victims in the shortest time possible. The question that arises here is: how can new criminals utilize this technology to commit various crimes? What is the reality of modern crime in Algeria? And what are the international and national efforts to combat these?

2. Cybercrime: Concept and Characteristics

2.1. **The concept of crime**: Crime is a social phenomenon as old as human societies themselves, having undergone remarkable development in our modern era due to various social, economic, political, and other factors. Its definition varies with time and place; acts considered acceptable in some countries may be deemed crimes or deviant in others. Additionally, certain actions that were deemed immoral at one time may have been prohibited during another period. Crime can be examined from three perspectives: social, psychological, and legal.

*** From a sociological perspective**, cybercrime is viewed as behavior that is anti-social and contrary to social norms, causing disruption in social relationships and deviating from community values. It harms the collective and threatens its safety, stability, and continuity, thus constituting a crime in terms of custom and tradition (Rashwan, 1990: 11)

*** From a psychological standpoint**, Adler suggests that crime is the fulfillment of a human instinct in a deviant manner, which is not adopted by an ordinary person when satisfying the same instinct.

This is because anomalous psychological conditions affect the offender at the exact moment of committing the crime, making it a result of the conflict between the instinct for self-preservation, which is a drive for superiority, and social awareness (Rashwan, 1990: 6-9).

*** From a legal perspective**: a crime is any deliberate and intentional harmful act that is prohibited by the law enacted by the state, which explicitly defines this behavior as a crime and punishes those who commit it.

2.2. The Concept of Cybercrime

Through the accumulated literature on the subject, it appears that many researchers have disagreed on how to define the concept of cybercrime. There is also confusion between cybercrime, information crime, computer crime, and internet crime. Some view the concepts of cybercrime and internet crime as equivalent, while others differentiate between them. For instance, one definition of information crime describes it as "any unlawful act that requires a significant understanding of computer technology for its commission on one hand, and for its prosecution on the other" (Nidaa, 2022).

While some consider it to encompass all practices carried out against an individual or a group, with a criminal motive aimed at deliberately damaging the victim's reputation or causing psychological and physical harm, whether directly or indirectly through modern communication networks such as the internet and its associated tools like email, chat rooms, and mobile phones (Hirdou Center, 2018).

The Algerian legislator has termed electronic crimes as crimes related to information and communication technologies, defining them under Article 02 of Law 09-04 dated August 5, 2009, as crimes that affect automated data processing systems, as specified in the Penal Code, and any other crime committed or facilitated through an information system or electronic communications network (Hafoudha, 2022)

Despite the differing perspectives on the concept of cybercrime and the lack of a precise definition, it is noted that all forms of cybercrime are fundamentally the same, encompassing all types of offenses conducted via computers, either individually or connected to the internet. Security experts have classified cyber-attacks into two types: the first is the technical attack, employed by individuals knowledgeable about systems and software to carry out attacks on the internet. The second type is the non-technical attack, which uses deception and trickery to manipulate employees within companies, obtaining permissions and authorizations to use services, access information, and breach network security. This is also known as social engineering. (Al-Tayti, 2008: 253-254)

However, launching cyber-attacks requires the presence of three essential elements, which are as follows: (Ghada, 2017: 12)

* Availability of motive: The motive may be a desire for revenge or the pursuit of financial gain.

* Existence of a method to carry out the attack: There must be a clear concept and plan for the attack that fulfils its purpose.

* Presence of vulnerabilities: This refers to weaknesses in the design or configuration of software or storage systems.

Among the emerging crimes are those committed via mobile phones equipped with Bluetooth technology, which allow for the transmission of audio and video messages containing indecent or lewd content. Additionally, ordinary and digital video cameras have reached extreme levels of miniaturization and precision, enabling the invasion of others' privacy by capturing images at their most intimate moments (Bayoumi, 2008: 08) Coupled with various means of eavesdropping on both wired and wireless communications, this situation poses a significant threat to individual privacy and personal freedom at risk

3. The cybercriminal: characteristics and motivations of criminal:

Who is the cybercriminal? What are the most important traits and features that define them? What are the reasons that lead to prosecution as a criminal? These are questions many may pose in order to understand the identity of this new intruder in contemporary modern societies—a criminal shaped by the changing nature of modern technology, the shifting patterns of contemporary lifestyles, and the rapid pace of life, alongside the challenges and transformations it brings to our behaviours, dispositions, and ways of thinking.

3.1. The cybercriminal, as depicted by specialists, is an individual or a group of individuals who commit only computer-related crimes. They specialize in this type of crime, and one of the main characteristics of a cybercriminal is that they revert to criminal behaviour in the realm of computers,

driven by the desire to exploit vulnerabilities that allow them to evade detection and prosecution. Additionally, they are professional criminals in this field, adept at overcoming the obstacles set up by experts to secure computer systems. Cybercriminals are also distinguished by their intelligence and possess a high degree of expertise and skill in using information technology. (Ghada, 2017: 43-45).

Experts have classified the cybercriminal into various categories and diverse designations, which can be clarified as follows (Al- Mayel, Al-Sharbi and Qaboosah, 2019):

***. Amateurs**: Youth captivated by the information revolution, their aim is amusement and play to showcase skills and excellence, engaging in entertainment rather than committing crimes.

***. Hackers**: They are individuals who penetrate devices and are able to view or steal files on them. Hackers can access a computer using a file known as a (Patch) or (Trojan).

***. Professional Criminals**: This category is characterized by extensive experience and technical skills, as well as the organization and planning of the activities committed. They are considered the most dangerous among cybercriminals, aiming for financial gain or to achieve political purposes.

***. Resentful Individuals**: They are less dangerous than others, with the goal of seeking revenge and retribution against the actions of their

3.2. The category of young cybercriminals: is sometimes referred to as young prodigies of information technology. This group consists of young adults who are deeply fascinated by information technology and its systems. They may progress beyond mere hobbyist activities and enter a more advanced stage of committing cybercrimes, reaching a level of professionalism in these offenses. There are also concerns that organized crime groups may embrace this demographic to leverage and enhance their skills, as they are more receptive to any ideas presented or imposed upon them, especially those that involve adventure, excitement, and challenge.

A well-known example of computer crimes committed by this group is the infamous gang known as "Gang 414," which was implicated in sixty acts of intrusion into computer systems in the United States, resulting in significant damage to both public and private organizations.

Pirate Class: They are usually experienced programmers who gain unauthorized access to information systems and breach the security barriers surrounding these systems. There are two types of hackers: the amateur or mischievous hackers, who challenge network security measures but typically lack motives of defiance or self-assertion. This group mainly comprises students from high schools and unemployed youth. On the other hand, professional hackers, known as crackers, are individuals who infiltrate computer systems to access stored information or to cause damage, tamper with data, or steal it.

3.3. The reasons behind committing cyber-crime are similar to those for other types of crime; however, there has been a notable increase in the involvement of youth, often driven by the use of modern technologies. These motivations can be both material and personal and may also stem from purely psychological, social, or political factors, which can be categorized as follows: (Al-Mayel, Al-Shurbugi and Qabousa, 2019)

- Intrinsic motives: These are motives that lead individuals to commit various violations, arising from curiosity and challenge, as well as a desire to overcome the information system and assert oneself.
- Psychological motives: These come from individuals with psychological disorders that reflect in their behaviour.
- Political and military motives: Political motives represent one of the most prominent international attempts to infiltrate government networks in various countries around the world. Scientific and technological advancements have allowed for a near-total reliance on computer systems to obtain political, military, and economic information. Criminals also resort to fabricating news and information or base their claims on a small fraction of the truth, then reproduce the fabricated news surrounding it.

Experts have pointed out that the main causes of cybercrime include unemployment and difficult economic conditions. This issue leads educated youth to invest their skills in online criminal activities as a means of profit and to escape financial hardship. Additionally, the youth's passion for wealth drives them, as individuals seek pleasure and aim to avoid pain, a notion supported by the general theory of crime posed by Guttfridsson and Hirschi (Lobna, 2020). People often turn to socially unacceptable means to achieve socially acceptable goals, as the desire for wealth is met with significant challenges when pursued through socially and legally acceptable methods. Consequently, some individuals resort to cybercrimes, where larger communities are targeted, execution is easier, returns are quicker, and risks are lower. Moreover, the broader societal pressures stemming from poverty, unemployment, illiteracy, and challenging economic conditions place considerable strain on society, particularly among the youth. This

generates negative feelings in large segments of the population against these circumstances and society, prompting them to resort to negative coping mechanisms, which include human trafficking, sexual exploitation, and other forms of cybercrime.

4. The Role of the Internet in Committing Cybercrime

Many consider information and communication technology to be one of the most effective tools for committing crimes due to its ability to reach a vast number of victims simultaneously. Despite the role of mobile phones and the internet in enhancing connectivity and communication among individuals within communities - speeding up relationships and bridging perspectives in the context of marriage - it is notable that this has also led to an increase in divorce rates. This rise can be attributed to the emergence of new capabilities such as cameras, recording, and the revelation of family secrets. In this context, Professor Sana Al-Bayasi pointed out that the information and communication revolution has both numerous benefits and significant drawbacks. We need to harness its advantages and avoid its harms, but how can we coexist with this technology without being adversarial? How can we adapt to the era's changes and transformations in a way that fosters healthy, positive reconciliation with it? (Al-Akhras, 2008: 188-190).

Global statistics indicate a rising global trend in cybercrime, as these crimes are committed with minimal risk. This presents challenges for law enforcement in apprehending or tracking this new category of criminals. A study by the Digital Numbers site reported that the number of victims of cyber-attacks and crimes reaches 555 million users annually, with over 1.5 million victims each day. Identity theft is the most prevalent type of crime. Additionally, the annual cost allocated for cyber security was estimated at100 *billion, up from approximately* 63.1 billion in 2011, and it could exceed $120 billion by 2017. (Hafoudha, 2022)

Among the most significant crimes committed within this network are the following:

4.1.E-commerce crimes:

E-commerce falls under the broader concept of the digital economy, which refers to the execution and management of various commercial activities, including the buying and selling of goods, services, and information through the use of the internet (Aliyan, 2015: 64-65). Despite the numerous advantages brought by this emerging trade, it also presents significant challenges, as highlighted by various reports and statistics. For instance, it was found that 80% of global companies have experienced attacks on their networks. The essence of these incidents is that amateurs and hackers intercept card numbers and use them to acquire the goods they desire, ultimately charging the legitimate cardholder (Bayoumi, 2008: 44-45).

One of the most significant issues related to e-commerce is the risks it poses, particularly to consumers. This necessitates that governments develop regulations addressing consumer protection and privacy concerns, as there is currently no specific protection for privacy in commercial transactions. Additionally, the issue of online intellectual property infringement is particularly challenging (Aliyan, 2015:129-132). Legal measures must adapt to the new characteristics of the internet.

4.2. Email Crimes:

Through email, unsolicited messages can be sent, attempting to engage in harassment and sometimes fraud against consumers. Senders bombard subscribers with massive amounts of spam. The U.S. Federal Trade Commission has released a list of the twelve worst topics of this nature that cause annoyance and frustration for internet users due to the overwhelming volume of junk mail. These topics often revolve around trivial matters such as the lure of making money, quick profits, health and dieting, and miraculous scientific achievements to cure diseases (Al-Laban, 2000:155). This list of messages is referred to as the "dirty list" because it is bothersome and slows down email systems, with most of the content entailing scams and fraud.

4.3. Money Laundering Crime:

New methods of money laundering have been identified through the global information network, emerging in recent years due to the diverse use of the internet in gambling, associated banking activities, online banking operations, and the facilitation of electronic money transfers. This has led to a rapid movement of electronic currencies, in contrast to the traditional use of paper money. (Bayoumi, 2008: 34)

4.4. Risks Related to Computer and Communication Crimes:

This involves deliberately causing harm and destruction, such as disabling a company's computer through viruses, which has led scientists to tackle this issue with anti-virus programs. Despite the efforts made to detect and combat viruses, experts anticipate a shift towards a form of "Electronic Terrorism," (Al-Laban, 2000: 123) where dangerous viruses attack computers and information networks, resulting in significant losses. Thus, the new terrorists do not use bombs and explosives but instead focus on the systematic destruction of computers and information networks, which could potentially lead to a nuclear war through the launch of missiles equipped with nuclear warheads, guided by computer programs.

4.5. Risks Related to Online Pornography:

The phenomenon known as "online pornography" has spread through the Internet, where pornographic photographs are exchanged freely. Pornographic clubs have emerged in the West, operating with the aid of the global web. While the West has often overlooked adult pornography under the pretext of the right to privacy, this does not apply to young children, especially with the rise of "child prostitution." In light of the seriousness of this issue, UNESCO organized the first international conference to combat child exploitation online in 1999. (Bayoumi, 2008: 218)

Furthermore, the Internet has facilitated the dissemination of extremist ideas, whether political, religious, or racial, thereby influencing the sentiments of youth and exploiting their ambitions, impulsiveness, inexperience, and superficial thinking to propagate their beliefs and fuel their rebellion. This exploitation often takes advantage of their suffering to achieve ends that conflict with the interests and stability of their country. It becomes evident that rates of cybercrime are increasing and diversifying at an unprecedented scale across all countries in the world. It is up to governments to implement monitoring, awareness, and filtering to enable the beneficial and effective use of modern technology. Additionally, it is necessary to instill confidence in youth, engage in discussions with them, and raise awareness of the risks and crimes associated with cyberspace, all within the framework of genuine political will.

5. Digital statistics on cybercrime in Algeria

Algeria was not in isolation from the information revolution and its positive and negative effects at all levels. Including the growing and high rates of crimes, in this context security interests have warned of the rise in cybercrime in Algeria, She emphasized that crime had already moved from the real world to the virtual transnational world. In view of its rapid implementation, the gendarmerie and police services recorded nearly 8,000 cybercrime offences in 2020, with the Directorate General of National Security registering a record high, That is, from 500 offences in 2015 to 5,200 cybercrime cases in 2020, while the National Gendarmerie Command recorded 1,362 cybercrime offences involving 1,028 people during 2020. The data analysis of recorded crimes showed that slander and insult through the virtual space; he took the lead by more than 55 per cent, followed by crimes against public security, then acts against private life and disclosure of secrets, and finally extortion, fraud and deception, sexual exploitation, acts against public morals and similar issues (Bachouch, 2021.) During the first eight months of 2021, the General Directorate of National Security, which specializes in combating crimes related to information and communication technologies, recorded 567 cases of internet crimes involving 543 individuals. The specialized teams for combating cybercrime within the national security apparatus managed to process 385 electronic crimes out of the 567 recorded cases by examining all technical data and physical evidence associated with the aforementioned cases (Cybercrime, 2022). This is illustrated by the data presented in the following table:

Table showing the distribution of cyber-crimes in Algeria

Type of Crime	Registered Cases	Addressed Issues	Number of Involved Parties	Rate of Resolved Cases
Online Crimes Against Individuals	430	289	365	68
Crimes against the integrity of systems	57	31	39	55
Online Fraud Crimes	25	17	32	68
Internet incitement and extremism crimes	14	14	31	100
Crimes against public decency	12	08	22	67
Crimes involving the sale of prohibited goods online	06	05	15	84

Various crimes (unauthorized software copying, piracy	23	21	39	92
Total	567	385	543	534

Source: *Cybercrime*, 2022

The table above indicates that cyber-crimes in Algeria are varied and diverse, with the most notable being incitement and extremism, copyright infringement, the sale of prohibited goods, as well as fraud and scams. We can assert that crime in Algeria is on the rise, reflecting the worsening of this social phenomenon and its spread among individuals within the same society, along with the challenges in tracking the perpetrators. One cannot claim that crimes are decreasing when compared to the statistics from 2020, as these statistics pertain only to national security authorities. Additionally, many victims of digital technology within Algerian society do not file official complaints to the relevant authorities. This is due to two main reasons: the first being the fear of exposure, particularly concerning vices and extortion, and the second being a lack of awareness among community members regarding the importance of deterring and punishing cyber criminals.

Cybercrime specialists emphasized; According to DATAREPORTAL's latest report on statistics on the world's fixed and mobile Internet, the number of Internet users in Algeria has risen by 3.6 million in a year, moving to 26.35 million in January 2020, as is known by the number of social media users. "Facebook, Twitter, YouTube, Instagram" has risen in Algeria to 31 January 2021, with about 3 million new social media users registered, up 13.6% over one year, bringing the total number of users of these apps to 25 million, 56.5% of the total population (Bachouch, 2021). Where the majority of users of social media sites use smartphones and electronic boards to connect to these networks. For its part, the company "Kaspersky", which is competent to fight cybercrime, thwarted 95 thousand cyber-attacks against Algeria during 2020, ranking the first Arab and 14th 2018 year globally in terms of countries most vulnerable to cyber-attacks./

6. International and National Efforts to Combat Cybercrime

The development of information and communication technology has led to an unprecedented increase in crime among community members, prompting countries to quickly seek ways to combat the rise of cybercrime. They have worked to update their legal frameworks and security apparatuses with the aim of combating internet and mobile offenses.

6.1.-International efforts:

With increasing cybercrime and various damages resulting therefrom, as they transcend the boundaries of a single State to reach individuals' computers, Financial institutions and Governments are therefore necessary and imperative for international cooperation. As a result, many conferences have been held to combat cybercrime and reduce its prevalence, among them was the Seventh United Nations Conference in 1985, which resulted in some modifications at the Havana Conference (1990), which recommended the following principles:

- Updating national criminal laws.
- Improve computer security.
- Adopt adequate training for staff and agencies responsible for the prevention of economic and cybercrime.
- Receive computer ethics as part of communications and information courses.
- Adopt policies that address the problems of victims of such crimes.
- Increased international cooperation to combat crimes.

Overall, The United Nations has entrusted the issue of confronting cybercrime; of particular interest during the Tenth United Nations Congress on Crime Prevention and the Follow-up to Offenders, held in Vienna on 10-17 April 2000, as well as during the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok on 18-25 April 2005, The European Commission on Crime Problems and the Committee of Experts on Computer Crime have also Draft international convention on this subject, the Council of Europe announced the draft convention on 27 April 2000 and taking into account the international character that characterized this type of crime (Zaiti, 2019).

The legislative sector has witnessed the introduction of numerous laws, as several European countries have enacted specific laws addressing internet and computer crimes, including the UK, the Netherlands, France, Denmark, Hungary, Poland, Japan, and Canada. Western countries have also focused on establishing specialized divisions for combating internet crimes and have created centers to support the victims of these crimes. In this context, a report published by a cyber-security projects company titled "Cyber Security Economy Predictions" indicates that the world spent approximately $1 trillion between

2017 and 2021 on cyber-security products and services to combat cybercrime. As a result, around one million cyber-security jobs were opened in 2016, while there was a shortfall of about 1.5 million positions in 2019 (Hafoudha, 2022).

Given the rising incidence of cybercrime in Arab countries, the General Secretariat of the Council of Arab Interior Ministers has prioritized combating this issue. They developed an Arab strategy derived from the Arab Convention on Combating Information Technology Crimes, which was adopted in Cairo at its 31st session on December 21, 2010. This strategy aims to tackle information technology crimes and enhance the capacity to enforce policies related to information technology and information security. This ensures the effective implementation of plans stemming from those policies across all institutions and organizations in both the public and private sectors. When preparing this strategy, the General Secretariat recognized that addressing information technology crimes necessitates strategic cooperation across national, Arab, and international levels, (Arab Banking Union, 2022)

Despite various international efforts to find effective solutions to confront the risks of modern technology, there are legal issues raised by the internet, primarily concerning the applicable law. Crimes committed online do not recognize geographical boundaries, and the perpetrator may be in one country while the crime takes place in another. Additionally, networks can be breached for the purpose of information espionage, which poses a threat to national security. Therefore, combating such crimes becomes an urgent necessity that requires international cooperation, including the sharing of data, technical assistance, and funding tools to resolve this global.

6.2. National Efforts:

In the face of cybercrime, the Algerian state has implemented a series of legal and legislative measures mainly aimed at amending substantive and procedural provisions in line with the nature of the crime itself. Additionally, special units and agencies have been established to combat crime and deter offenders.

6.2.1. The legal and legislative framework: Prior to 2004, Algeria did not have laws governing information systems; however, with the increase in cybercrime, it became necessary for lawmakers to establish an appropriate legal framework to prevent attacks on these systems or their misuse. This was aimed at filling the legal void and following the example of most countries around the world. Thus, the Algerian legislator took the initiative to issue amended and supplementary laws to the Penal Code, as well as specific laws, the most important of which are Law 09-04 dated July 5, 2009, and Law No. 09-04 dated August 5, 2009, which set forth the specific rules for the prevention and combating of crimes related to information and communication technology (Bouznoun, 2019)

The law includes 19 articles divided into six chapters, prepared by a group of legal experts in collaboration with specialists and professionals in the field of electronic media. This law encompasses specific provisions related to its scope of application, as well as others concerning the monitoring of electronic communications. It outlines the circumstances that permit the resort to electronic surveillance, in addition to procedural rules that include the inspection of information systems and the seizure of data that could be useful for uncovering cybercrimes

Despite the enactment of such laws to combat cybercrime, the implementation of their provisions has been weak. Technical aspects necessary for classifying these crimes and determining appropriate penalties for offenders have been neglected. Consequently, penalties have often been limited to financial fines. (Hafoudha, 2022)

In general, it can be said that Algerian law has kept pace, albeit to a limited extent, with the legislative movement to combat cybercrime. This is based on the prevailing legal opinion that computer programs and data are considered tangible property belonging to others. They are thus subject to theft, which occurs when the information contained on a storage device is transferred to another ledger. In this context, misappropriation applies, with Article 350 of the Penal Code governing theft, including the theft of data. Consequently, Algerian judges apply the theft provisions to information technology assets. On the other hand, software and data fall under the scope of fraud, as they are regarded as property and movable assets, with Article 372 of the Penal Code applicable in these cases

The Algerian legislator has criminalized acts that violate the system of automated data processing, also known as information fraud, according to Section 7 bis of the Penal Code. Offenders face imprisonment for a period of three months to one year, along with financial penalties. If these actions result in the deletion or alteration of data, the punishment is doubled. However, if such actions lead to

the destruction of the operational system of information management, the penalties increase to imprisonment for six months to two years and a financial fine (Hirdou Centre, 2018).

Law number 09-04, in its fifth article, establishes the National Authority for the Prevention and Combat of Crimes Related to Information and Communication Technologies. This authority is responsible for the following:

- Coordinating efforts to prevent cybercrime.
- Assisting judicial authorities and law enforcement in investigations.
- Exchanging information with counterparts abroad to gather all relevant data to identify perpetrators of cybercrimes and to determine their locations.

Additionally, this law reiterates, in its final article, the principle of international judicial cooperation and assistance based on mutual treatment. In this context, the head of the parliamentary group of the Justice and Development Front, Lakhdar Bin Khallaf, explained to the newspaper "Al-Salam" that our issue lies in the laws enacted by the government regarding cybercrime, which have not been implemented. There are decrees related to this law, ratified in 2009, which have not been activated, resulting in the processing of cases in this regard facing a significant legal vacuum. This has, in many instances, led to the issuance of approximate judgments and penalties without any legal basis (Hafoudha, 2022).

6.2.2. Structures for Combating Cybercrime in Algeria: Given the escalation of cybercrime in Algeria and the unique nature of these crimes, it has become essential to develop judicial police departments to keep pace with advancements in the field of information-related crimes. To complement this vision, specialized bodies and units associated with the National Security and Gendarmerie have been mobilized.

The specialized technical bodies for investigation and inquiry into electronic crimes consist of units dedicated to combating cybercrime, comprising investigators with a unique profile that combines the attributes of judicial police with extensive knowledge of information systems. Among the most significant branches are the following: (Bouznoun, 2019)

Section One: The National Authority for the Prevention of Crimes Related to Information and Communication Technology. This authority was established in Algeria under Article 13 of Law 09-04, which outlines specific provisions for preventing crimes related to information and communication technology and combating them.

Section Two: Units affiliated with the National Security Corps. Within the national security apparatus, there are three units responsible for investigating cyber-crimes as follows:

- The Central Laboratory of Scientific Police in Algiers.
- The Regional Laboratory of Scientific Police in Constantine.
- The Regional Laboratory of Scientific Police in Oran.

In 2010, the General Directorate of National Security created approximately 23 cells to combat cybercrime across the central, eastern, western, and southern provinces, which were later extended to all security services nationwide.

Section Three: Units affiliated with the General Command of the National Gendarmerie. The main units of the National Gendarmerie responsible for investigating cyber-crimes include the National Institute of Forensic Evidence and Crime Sciences at the central level. The basic function of this unit is to support investigative units in the context of judicial police tasks in combating various types of crimes, including cybercrime. This institute has a section dedicated to Information Technology and Electronics that specializes in investigating cyber-crimes. Additionally, there are other entities within the National Gendarmerie, including (Bouznoun, 2019):

- The Centre for the Prevention of Information Technology Crimes and Cyber Crimes of the National Gendarmerie.
- The Directorate of Public Security and Exploitation.
- The Central Directorate of Criminal Investing

In the context of enhancing mechanisms to combat cybercrime, the National Centre for Combating Cybercrime has been established. Officials in charge of security have emphasized that individual posts will not be targeted, nor will citizens' freedoms be curtailed, but rather those posts that promote false and misleading news that threaten state and societal security (Bachouch, 2021). Furthermore, in the same vein, technology and information expert Younes Qarar underscored that the establishment of this

specialized centre is crucial, but it must be effectively implemented in practice, as cybercrimes have become more dangerous than traditional crimes.

Despite the variety of preventive and deterrent measures adopted in Algeria, along with a range of laws and regulations issued in this regard, the confrontation remains challenging, particularly due to the lack of technical foundations capable of investigation, research, and classification of crime severity before penalties are imposed. This is especially critical as the risks associated with modern technology crimes conducted online are transnational, raising issues regarding the applicable law and competent jurisdiction (Bayoumi, 2008: 8). Additionally, punishing these crimes in the absence of legislative support often conflicts with the principle of legality, which stipulates that there is no crime or punishment without a text.

It can be stated that the seriousness of cybercrime necessitates a concerted effort between legal and societal dimensions to address it, especially since this phenomenon can evolve from mere enthusiasm for technology into harmful motives detrimental to individuals and community institutions. Moreover, it is essential to highlight the role of education and guidance in protecting against and preventing cybercrime. This was emphasized at the Cybercrime Conference held in Tripoli, Lebanon, on March 24-25, 2017, where a series of techniques aimed at combating cybercrime were adopted (Kourari and Rahli, 2017)

- It is essential to adopt what is referred to as a firewall, which acts like the border customs to prevent the entry of foreign and harmful entities.
- Use encryption technology to prevent the disclosure of information.
- Utilize digital signature technology to prevent the forgery of electronic messages.
- Employ systems to detect various intrusions and find solutions for security vulnerabilities.
- It is vital to have backups of important and sensitive files and store them in secure locations.
- It is necessary to use programs designed to detect and prevent viruses and avoid using simple passwords.
- Exercise caution when opening email, ensuring the identity of the sender is verified.

The conference clarified that the guidance aspect plays a role in preventing cybercrimes by engaging all media outlets, including journalism, television, radio, theatre, and cinema, as they are widely accessible mass media. The goal is to raise awareness about the dangers of crimes, both at the individual and societal levels. It emphasized the importance of ethical conscience, which seeks objectivity and integrity when using modern technologies. Additionally, it called for strengthening the willpower and determination among Muslim youth to prevent them from succumbing to the temptations associated with cybercrimes. There is also a focus on investing in the youth through various forms of care, particularly in health, religion, mental well-being, and social aspects, aiming for the healthy upbringing of community members

7. Conclusion

Cybercrime takes various forms and has distinct characteristics associated with its perpetrators, it also has societal, media, and security strategies and mechanisms for combating it, as methods of committing crimes in the information age evolve, we must develop our countermeasures in line with societal advancements and changes. Algeria, like many other countries, faces numerous challenges in confronting these emerging crimes, particularly as we deal with a new class of white-collar criminals and a tech-savvy generation of youth who quickly adapt to new technologies. Consequently, it is crucial for community actors, security services, and active institutions to seek out weaknesses and strengths in the use of modern technology to enhance their ability to tackle these challenges. Furthermore, it is essential for all governments and nations to mobilize every stakeholder involved in maintaining security, while specialists are particularly urged to renew their knowledge and advance their skills to keep pace with technological innovations, aiming for effective and serious engagement with these technologies.

References:

1. Al-Laban, S.D. (2000). C*ommunication Technologies, Risks, Challenges, and Social Impacts*, 1st ed., Egyptian Lebanese House, Cairo, Egypt.
2. Rashwan, H.A. (1990). *Crime: A Study in Criminal Sociology*, Modern University Books, Alexandria, Egypt.

3. Al-Akhras, I. (2008). *The Economic and Social Impacts of Communication and Information Technology Revolution on Arab Countries* (with the Internet and Mobile as a Model), Etrak for Printing, Publishing, and Distribution, 1st ed., Egypt.
4. Bayoumi, A.F. (2008). *Crime in the Age of Globalization: A Study of the Criminal Phenomenon*, Dar al-Fikr al-Jami'i, Alexandria, Egypt.
5. Ghada, N. (2017). *Terrorism and Cybercrime*, Al-Arabi for Publishing and Distribution, Cairo, Egypt.
6. Aliyan, R.M. (2015). *Electronic Environment*, Dar Safaa for Publishing and Distribution, 2nd ed., Amman, Jordan.
7. Al-Tayti, K.M. (2008). *E-Learning from Commercial, Technical, and Administrative Perspectives*, Dar Al-Hamed for Publishing and Distribution, 1st ed., Amman, Jordan.
8. Al-Mayel, M. Al-Shorbaji, A. M & Qaboos, A. (2019), *Cybercrime in the Digital Space: Concepts, Causes, and Avenues for Combating, with a Focus on the Case of Libya*, ASJP (cerist.dz), downloaded on 19/07/2023 at 16:30.
9. Hafoudha Al-Amir, A. Q. (2022), *Cybercrime and Mechanisms for Combating It* [online] available at: https://www.politicsdz.com.
10. *Cybercrime Division of the Police* (2022). [online] available at: https://www.algeriepolice.dz/?%.
11. Bachouch, N. (2021). *Cybercrime, terrifying statistics* [online] available at: https://www.echoroukonline.com.
12. Bouznoun, S. (2019). *Combating Cybercrime in Algerian Legislation* [online] available at: http://revue.umc.edu.dz/index.php/.
13. Lobna, M. (2020). *Causes of Cybercrime at the Societal Level* [online] available at: https://e3arabi.com.
14. Nidaa, F.A. (2022). *The Privacy of Cybercrimes* [online] available at: https://www.google.com/search .
15. Arab Banking Union (2022). *Collaboration of Arab efforts to combat cybercrime and information crimes and their impact on financial operations* [online] available at: https://uabonline.org/ar/%D8
16. Hirdou Center for Digital Expression Support (2018). *Legal Regulation and Cyber Crimes between Information Security and Restriction of Freedoms*, Cairo. [online] available at: https://mail.google.com/mail/u/0/#advanced-
17. Zaiti, A. (2019). *Combating Cyber Crimes in Light of the Algerian Penal Code: A Comparative Study*. [online] available at: ASJP www.cerist.dz .
18. Kourari, S. & Rahli, S. (2017). *The Role of Education and Guidance in Protection and Prevention from Cyber Crimes* [online] available at: https://jilrc.com/archives/6165