

The Role of Cybersecurity in Combating Cybercrime in Algeria: Prospects and Challenges



Received: 19/08/2024; Accepted: 04/06/2025

Fatma Zohra GUEDOUARI ^{1,2*}, Mehdi ALLOUACHE ³

¹ Laboratory of Artificial Intelligence and Society, University of Algiers 1, Algeria.

² Private Law Department, Faculty of Law and Political Science, University of Biskra, Algeria. fatmazohra.guedouari@univ-biskra.dz

³ Laboratory of Contracts and Business Law, Faculty of Law, University of constantine1, Algeria. mehdi.allouache@umc.edu.dz

Abstract

This study aims to highlight the role of cybersecurity as a fundamental pillar in combating cybercrime at the national level, particularly in the context of the increasing technological advancements across all economic, cultural, social, and security sectors. Cybercrime is viewed as one of the adverse effects of advanced technology, posing a genuine challenge threatening the lives of individuals, communities, and national security.

The study concludes that significant national efforts are being made to achieve cybersecurity in the fight against cybercrime by enacting relevant laws and establishing specialized structures for combating cybercrime in Algeria. Additionally, it emphasizes the necessity of international cooperation and governmental coordination to exchange information and develop joint strategies to address transnational cybercrimes, thereby contributing to a comprehensive cybersecurity framework that safeguards individuals, institutions, and nations.

Keywords

Cybersecurity;
Cybercrime;
Challenges;
Countermeasures;
Technological advancement.

الكلمات المفتاحية

أمن سيبراني؛
جريمة إلكترونية؛
تحديات؛
آليات مكافحة؛
تطور تكنولوجي.

دور الأمن السيبراني في مكافحة الجريمة الإلكترونية في الجزائر: آفاق وتحديات

ملخص

تسعى هذه الدراسة إلى إبراز دور الأمن السيبراني باعتباره ركيزة أساسية في مواجهة الجريمة الإلكترونية على الصعيد الوطني، خاصة في ظل التطور التكنولوجي المتزايد في كافة ميادين الحياة الاقتصادية، الثقافية، الاجتماعية والأمنية، إذ تعتبر الجريمة الإلكترونية إحدى السلبيات التي خلفتها التقنية العالية، وهي تشكل تحدياً حقيقياً يهدد حياة الأفراد والمجتمعات وأمن الدول. وخلصت الدراسة إلى أن هناك جهوداً وطنية مبذولة لتحقيق الأمن السيبراني لمكافحة الجريمة الإلكترونية من خلال سن قوانين في هذا السياق، وإنشاء هياكل مختصة في محاربة الجريمة الإلكترونية في الجزائر، بالإضافة إلى تسليط الضوء على ضرورة التعاون الدولي والتنسيق بين الحكومات لتبادل المعلومات وتطوير استراتيجيات مشتركة للتصدي للجرائم الإلكترونية العابرة للحدود، مما يساهم في تحقيق أمن سيبراني شامل يحمي الأفراد والمؤسسات والدول.

* Corresponding author. E-mail: fatmazohra.guedouari@univ-biskra.dz
Doi: <https://doi.org/10.34174/0079-036-002-030>

I- Introduction :

In the face of technological advancements and the increasing use of networks, information systems, and computers in our current era—an era marked by an explosion of information and advanced technology resulting from the evolution of communication and computing means that have turned the world into an electronic village, dissolving geographical and political borders. Despite the benefits provided by these programs and electronic networks, they are a double-edged sword, bringing with them new risks that have given rise to complex crimes known as cybercrimes, such as breaching secret systems, identity theft, electronic bank fraud, electronic espionage, crimes against public morals and ethics, and violations of privacy. As society advances technologically, crime evolves continuously, with criminals using the latest technologies to execute their cyberattacks.

Consequently, cybercrimes are considered one of the negative impacts of high technology and a real challenge that threatens individuals' lives, communities, and national security across all economic, cultural, social, and security aspects.

Algeria hasn't been immune to these increasing cyber threats, necessitating the need to keep pace with this notable development in such crimes and confront them with legal legislation to counter this emerging crime. The Algerian authorities have strived to strengthen an adequate legal framework compatible with these challenges, in addition to international agreements aimed at enhancing international cooperation to ward off the dangers of these cross-border cybercrimes.

Cybersecurity is fundamental in combating these crimes and strengthening states' legal and security systems. Due to their complex nature and difficulty tracking the involved parties, cybersecurity has become imperative in confronting cybercrimes that threaten states' stability and sovereignty.

Based on the above, the following issue can be raised: **To what extent are Algeria's mechanisms effective in enhancing cybersecurity to confront cybercrime in the face of rapid technological development and current challenges?**

This study employs descriptive and analytical methods to address the posed issue according to the following study:

I.1- The conceptual framework of the study:

In this section, we will delve into the concept of cybercrime by defining it, highlighting the characteristics that distinguish it from traditional crimes, and exploring its various types. Following this, we will address the concept of cybersecurity by defining it, outlining its objectives, and identifying its dimensions as follows:

I.1.1- Concept of Cybercrime:

Cybercrimes are among the modern crimes that have emerged in our contemporary era, primarily due to their association with modern technological means such as computers, internet networks, and electronic platforms. The widespread adoption of advanced technology and the prevalence of these crimes have attracted the attention of researchers and specialists in this field.

Researching the concept of cybercrime requires initially defining it, outlining its characteristics, and specifying its types as follows:

I.1.1.1- Definition of Cybercrime:

The issue of defining cybercrime has been subject to scholarly debate, resulting in various interpretations by jurists. Definitions of cybercrime vary widely, ranging from crimes committed specifically using computers to those involving any form of digital equipment. Cybercrimes are offenses using computers, networks, and technological devices such as mobile phones. Some define cybercrimes as offenses with tangible outcomes involving any illegal behavior facilitated by electronic devices that result in the perpetrator gaining material or moral benefits while inflicting corresponding losses on the victim. Often, these crimes aim at piracy for theft or destruction of information stored on devices, which may be used for extortion.^[1]

"Cybercrime" also refers to crimes committed using computers and the Internet. These terms denote crimes arising from exploiting and utilizing information technology, particularly advanced information technology. The United Nations defined cybercrime in 2000 as any crime committed through a computer system, computer network, or electronic environment.^[2]

Cybercrime, defined as any harmful act perpetrated against or using a computer or network, differs from traditional crimes in several distinct ways, as outlined by McConnell International: it is easily learnable, requires minimal resources relative to potential damages, can be committed remotely across jurisdictions, and often lacks clear legal boundaries. Another definition, provided by the Director of the Computer Crime Research Centre (CCRC) during an interview on April 27, 2004, describes cybercrime (or 'computer crime') as any unlawful behavior conducted through electronic operations targeting the security of computer systems and their processed data. Cybercrime occurs within a virtual space where information about individuals, objects, facts, events, phenomena, or processes is represented mathematically, symbolically, or otherwise and transmitted via local and global networks. From this perspective, cybercrime involves

disrupting computer data or networks through interception, interference, or destruction, encompassing direct attacks on computer systems and using computers to perpetrate crimes.^[3]

Some scholars define cybercrime as: "Unauthorized activity aimed at copying, altering, deleting, or accessing information stored within a computer or transmitted through it."^[4]

This definition underscores the necessity of the computer itself as the locus of electronic crime. In legal doctrine, some interpret this crime as an assault on informational assets, including the computer's components, software, and equipment.^[5]

Others define cybercrime as "any act or omission planned or prepared using any type of computer, whether personal computers, computer networks, the Internet, or social media platforms, to facilitate the commission of a crime or unlawful act", these crimes also include those targeting networks by hacking them to store, modify, tamper with, or alter the programs they contain.^[6]

I.1.1.2- Characteristics of Cybercrime:

Cybercrimes are characterized by a set of features that distinguish them from conventional crimes, as follows:

A- Difficulty in Detecting Cybercrime:

Cybercrimes are characterized by their secretive and hidden nature, often unnoticed by victims even while they are online. Perpetrators possess technical capabilities that allow them to execute crimes precisely, such as sending viruses, stealing money and personal data, or destroying them, in addition to activities like espionage, call interception, and other harmful electronic actions.^[7]

Due to their secretive nature, these crimes often leave minimal traces after being committed, making it highly challenging for forensic investigators to retain digital evidence if found. This complicates the task for regular investigators, who face challenges from criminals' use of advanced camouflage and deception techniques.

Combating cybercrimes requires highly specialized technical expertise to prove and pursue their perpetrators effectively.^[8]

B- Transnational Nature of Cybercrime:

Cybercrimes transcend the geographic boundaries of states and continents, facilitated by the widespread network connectivity linking the world's countries and regions. This connectivity allows offenders to be in one country while their victims are in another, often resulting in cybercrimes across multiple international borders. Moreover, the technological capability of information systems to bridge distances and establish connections across different parts of the world has influenced the nature of criminal activities, as criminals exploit these technologies to violate laws. Consequently, this signifies that the stage for cybercrime is no longer local but global, where perpetrators commit their crimes remotely without physical presence at the crime scene. As a result, distances widen between the perpetrator using computer systems and the information being attacked, potentially harming individuals in different countries due to this criminal behavior.^[9]

C- Quiet Crimes:

While traditional crimes require physical effort, such as murder and theft, cybercrimes do not necessitate physical exertion but rely on mental reasoning and deliberate scientific analysis based on understanding computer technologies.

This type of crime involves altering, modifying, or deleting data in computer records without physical effort. Nonetheless, some individuals liken these crimes to violent offenses, as the FBI did, due to similarities in motives between those targeting computer systems and those committing violent acts.^[10]

D- Difficult-to-Prove Crimes:

Proving cybercrimes is exceedingly challenging, as they are difficult to trace and detect easily, given their tendency to leave minimal traceable evidence. Most cybercrimes are discovered unexpectedly after a considerable time since their commission, lacking traditional physical evidence such as fingerprints. Moreover, tracking cybercrimes requires technical expertise that surpasses the capabilities of regular investigators, as cybercriminals employ camouflage, deception, and trickery to complicate identification and apprehension processes.^[11]

I.1.1.3- Types of Cybercrime:

Cybercrimes encompass a variety of illegal activities conducted online or targeting computer systems and electronic networks:

A- Cyber Espionage:

Cyber espionage represents a form of traditional espionage but utilizes advanced technology. It's characterized by sophisticated cyber attacks aimed at infiltrating and obtaining confidential information through unlawful means to achieve economic, strategic, or military advantages. Cyber espionage relies on electronic techniques to gather information, and it varies in its methods, including espionage through individuals, wired communication networks, or even satellite-based surveillance.^[12]

B- Cyber Terrorism:

Cyberterrorism refers to using information resources such as media, computers, the Internet, and satellite communications to intimidate individuals, coerce them for political purposes, and propagate aggressive and hostile ideologies. Cyberterrorism requires complex and advanced technologies dependent on modern information and communication technology (ICT), which has become integral to all aspects of global life. Cyberterrorism can disrupt command and control systems, sever communications between units and central command, and turn off air defense systems and other critical infrastructure reliant on seamless communications.^[13]

C- Phishing:

This involves using fake emails, text messages, or websites to obtain personal information such as usernames, passwords, and credit card details. The primary aim of electronic fraud is often identity theft or manipulating users to gain sensitive information.^[14]

D- Cyber Extortion:

French law defines extortion as: "obtaining something through violence, the threat of violence, or coercion to sign, commit, relinquish a secret, transfer money, securities, or any other goods", So Cyber extortion is a type of cybercrime in which the perpetrator uses technology to threaten or pressure the victim to gain material or immaterial benefits. Cyber extortion involves threats to disclose sensitive or personal information and destroy or disrupt systems or data if the perpetrator's demands are unmet.^[15]

E- Intellectual Property Crimes:

Intellectual Property (IP) crimes refer to a range of illegal activities that involve the unauthorized use, reproduction, or distribution of intellectual property. This includes inventions, literary and artistic works, designs, symbols, names, and images used in commerce. The primary types of IP crimes are piracy, counterfeiting, and infringement of copyrights, trademarks, patents, and trade secrets. Cyber piracy is an unauthorized process aimed at penetrating computer systems or networks to obtain confidential information, disrupt services, achieve financial gains, or achieve other unlawful objectives. This process exploits security vulnerabilities in software or systems, executed by individuals or groups proficient in hacking computer programs and their management and demonstrating advanced programming skills.^[16]

These types represent a portion of the wide range of illegal electronic activities that can negatively impact individuals and organizations, necessitating effective defense strategies and legislation to combat them.

I.1.2- Concept of Cybersecurity:

Cybersecurity has become an urgent necessity for all countries without exception, as it pertains to protecting systems and electronic networks from potential risks originating from external sources via the Internet. Cybersecurity is no longer an option; it has become a fundamental pillar to combat cyber warfare in all organizations, institutions, and even nations. Cybersecurity protects information stored on computers and their networks, including the processes and mechanisms to safeguard computer equipment, information, and services from unintentional or unauthorized access, alteration, or destruction.^[17]

Accordingly, we will address the concept of cybersecurity by defining it, outlining its objectives, and identifying its dimensions.

I.1.2.1- Definition of Cybersecurity:

Cybersecurity is the protection of networks, information systems, data, and devices connected to the Internet. This field involves the procedures, measures, and standards necessary to address threats and attacks or mitigate their negative impacts. It is also defined as: "the process of organizing and assembling resources, processes, and structures that enable cyberspace to prevent various forms of illegal and improper intrusions."^[18]

Another definition states that it is: "the activity that ensures the protection of human and financial resources associated with communication and information technologies, guaranteeing the ability to minimize losses and damages resulting from realized risks and threats, as well as restoring the situation to its original state as quickly as possible so that production does not halt, and damages do not turn into permanent losses."^[19]

Cybersecurity encompasses a comprehensive set of technical and administrative procedures that include the necessary processes and mechanisms to prevent unintended or unauthorized interventions such as espionage, hacking, or misuse of electronic information and data found on communication and information systems. Cybersecurity aims to ensure the protection and confidentiality of citizens' data, as well as to maintain the continuity of operations and the protection of computer equipment, information systems, communications, and services from any alteration or damage.^[20]

I.1.2.2- Objectives of Cybersecurity:

System security is considered a fundamental and crucial pillar in protecting individuals and organizations from the damages resulting from security shortcomings. Both individuals and organizations rely on the performance of their information systems by ensuring their security through precise, appropriate, and reliable methods. Security aims to maintain the effectiveness and efficiency of information systems, ensuring an adequate level of availability, confidentiality, and integrity while facilitating their development and use by relevant individuals for new, unconventional purposes different from those currently applied. Furthermore, it enables the optimal exploitation of information technology's full potential and capabilities. Consequently, the field of information security contributes to protecting the rights and interests of all who depend on it by safeguarding and maintaining it from damage resulting from failures in availability, confidentiality, and integrity procedures.^[21]

Among the objectives of cybersecurity are:

- It's providing a secure environment with high reliability in the information society.
- They are enhancing the protection of operational technology systems at all levels and their components, including hardware, software, services, and data.
- Addressing information security attacks and incidents targeting government devices and institutions in both the public and private sectors.
- We are providing the requirements to reduce cybercrimes targeting users.
- Resisting malware and mitigating the severe damages it aims to inflict on users and information systems.
- We are reducing electronic espionage and sabotage at the level of governments and individuals.
- We are eliminating vulnerabilities in computer systems and mobile devices and addressing gaps in information systems.^[22]

These objectives collectively enhance system security and protect individuals and organizations from cyber threats, ensuring information systems' reliable and efficient performance.

I.1.2.3- Dimensions of Cybersecurity:

Cybersecurity encompasses all military, economic, political, and humanitarian issues, aiming to establish an integrated security framework that safeguards national security from all cyber threats. Therefore, it is crucial to elucidate the dimensions of cybersecurity:

A- Military Dimension:

Ensures the capability of military units to communicate via secure military networks, facilitating the exchange and flow of information and orders and enabling remote targeting. However, these networks also pose vulnerabilities if not adequately secured against breaches, which could destroy military databases, disrupt communication between command and military units, and potentially unauthorized control over weapons.^[23]

B- Political Dimension:

The political dimension of cybersecurity is fundamentally based on protecting the state's political system and its integrity. Technologies can be employed to disseminate information and data that may destabilize the security of states and governments, as they can rapidly reach large segments of the population regardless of the accuracy of this information. The Russian cyber intervention in the American elections is a prominent example of the significance and necessity of cybersecurity in its political dimension. Additionally, leaks of sensitive documents and breaches often lead to diplomatic crises between countries. Moreover, cyberspace has become a fertile environment for electoral campaigns and propaganda by various international actors.^[24]

C- Economic Dimension:

The Internet has become fundamental for commercial, financial, and economic transactions. Computers are essential for managing industries, driving economic growth, and interconnecting global economies through computer networks, underscoring the critical role of cybersecurity in the economic sphere.

D- Social Dimension:

With over four billion internet users globally, including over 2.6 billion on social media platforms, it has become the largest hub for human interaction, facilitating extensive exchange of ideas and experiences. However, this connectivity also exposes societal ethics to risks due to the challenges in monitoring internet content. Identities are vulnerable to external breaches that could threaten societal stability, necessitating public awareness to achieve cybersecurity in its social dimension.^[25]

E- Legal Dimension:

The rapid technological advancements necessitate the adaptation of legal frameworks to establish regulations and legislation to govern both legal and illegal activities in cyberspace. Cybercrime lacks stringent legal frameworks in many countries, highlighting the crucial need to enhance international cooperation in combating this phenomenon.^[26]

These dimensions collectively underscore the multifaceted nature of cybersecurity and its pivotal role in securing individuals, organizations, and nations against diverse cyber threats with remarkable precision and clarity.

I.2- Mechanisms for Achieving Cybersecurity to Confront Cybercrime in Algeria:

Given that cybercrime is one of the most distressing issues affecting citizens in their personal lives and threatening the security and sovereignty of states, owing to the tremendous technological and digital advancements and their widespread impact, the repercussions of this technological revolution have also encroached upon the sanctity and privacy of individuals. This has prompted legislation, including Algerian legislation, to strive earnestly to combat it by adopting various mechanisms to achieve cybersecurity, which we will address in this section.

I.2.1- Legal Mechanisms for Achieving Cybersecurity:

The Algerian legislator criminalized acts of tampering with computer systems due to the emergence of new forms of crime from the information revolution. This prompted amendments to the Penal Code under Law No. 04-15 ^[27], supplementing Order No. 66-156, which introduced the concept of crimes related to automated data processing systems. Section Seven, specifically Article 394 bis seven under Law No. 04-15, delineated these acts, each assigned its corresponding penalty.

Not stopping there, the legislator also imposed criminal protection on individuals' private lives through Law No. 06-23, dated December 20, 2006 ^[28], amending Article 303 and reaffirming it as Article 303 bis 3 in response to the misuse of modern technology. Shortly after that, another term was adopted, namely crimes related to information and communication technologies within Law No. 09-04 ^[29], which expanded the scope of cybercrimes. This law established a set of preventive measures to prevent or at least detect cybercrime early to mitigate its risks, such as electronic monitoring. The Algerian legislator allowed recourse to this measure strictly in specific cases (Article 04 of Law No. 09-04), requiring written authorization from the competent judicial authorities. This measure aims to protect against crimes that seriously threaten national security or in cases where information indicates a potential attack on an information system that could jeopardize public order, national defense, state institutions, or the national economy. Additionally, measures include using service providers to prevent cybercrimes by collecting and recording data related to communications content at the time and making this data available to the authorities.^[30]

I.2.2- Structural Mechanisms for Cybersecurity Effectiveness:

Algeria has established several entities aimed at achieving cybersecurity and combating electronic crime, including:

I.2.2.1- National Authority for Prevention of Crimes Related to Information and Communication Technologies:

This authority was established under Article 13 of Law No. 09-04, which deals with specific rules for preventing crimes related to information and communication technologies. The second paragraph of the same article delegated the issue of defining the authority's composition, organization, and operational procedures to regulations, as outlined in Presidential Decree No. 15-261.^[31]

This authority is an independent administrative body with legal personality and financial autonomy. It is headquartered in Algeria under the supervision of the Minister responsible for justice.

The tasks of this authority include:^[32]

- We are activating and coordinating efforts to prevent and combat crimes related to information and communication technologies.
- I assist judicial authorities and police in investigating crimes involving information and communication technologies, including gathering information and conducting judicial expertise.
- They exchange information with counterparts abroad to gather valuable data on perpetrators of crimes related to information and communication technologies and their whereabouts.

I.2.2.2- The National Institute of Criminal Evidence and Criminology of the National Gendarmerie:

The National Institute of Criminal Evidence and Criminology was established under Presidential Decree No. 04-183 dated June 26, 2004 ^[33], which established the institute and defined its fundamental law. It is a public institution with administrative character under the supervision of the Minister of National Defense, and its powers are exercised by delegation by the Commander of the National Gendarmerie.

The National Institute of Criminal Evidence and Criminology comprises eleven specialized departments in various fields, all involving expertise, training, education, and technical assistance. Among these departments is the Department of Information Technology and Electronics, responsible for processing and analyzing all digital evidence, aiding justice, and providing technical support to investigators in examinations.

Its assigned tasks, as stipulated in Article 04, include:

- Conducting expertise and scientific examinations under the jurisdiction of judges, investigators, or qualified authorities, upon their request, within the framework of preliminary investigations and judicial inquiries, aimed at establishing evidence enabling the identification of perpetrators of crimes and misdemeanors.
- We provide scientific assistance during complex investigations, using scientific and technical police methods to collect and analyze objects, traces, and documents taken from crime scenes.
- We are participating in studies and analyses on preventing and reducing all forms of crime.
- I am designing and creating data banks, including genetic data, that are legally accessible to investigators and judges for developing approaches and extracting possible links between criminals and criminal activities.
- We are initiating research related to crime and conducting it using advanced technologies.
- We promote applied research and investigative methods proven effective in criminology and criminal evidence nationally and internationally.
- I participate in all necessary national and international conferences, lectures, and seminars to develop the institute's users.
- It proposes research entrusted to third parties and ensures its follow-up and evaluation.

I.2.2.3- The Judicial Pole for Combating Cybercrimes:

This pole was established under Order No. 21-11 dated August 25, 2021, amending and supplementing the Code of Criminal Procedure by establishing the Judicial Pole for Combating Cybercrimes.^[34] It is located at the level of the court headquarters of the Algiers Judicial Council. This pole has been entrusted with two main tasks: ^[35]

- We monitor and investigate cybercrimes and related offenses involving information and communication technologies.
- Adjudicating crimes stipulated in Chapter VI of Order No. 21-11 if they constitute misdemeanors

I.2.2.4- Central Office for Combating Cybercrime:

This entity is subordinate to the Directorate of National Security and relies on highly professional human resources. These enable it to perform its tasks at the international level through collaboration with specialized agencies such as Interpol and Afripol and with police forces in major countries. At the national level, this entity coordinates with scientific police and specialized decentralized criminal offices such as judicial police.^[36]

I.2.2.5- Center for Prevention of Cyber and Information Crimes:

An entity under the National Gendarmerie Command is similar in investigative and inquiry tasks in this field to its counterpart in national security. Coordination between them falls under the direct responsibility of the prosecutor within the jurisdiction.^[37]

I.2.3- Role of International Cooperation in Combating Cybercrime:

In order to combat cybercrime and achieve cyber security, the Algerian legislature has encouraged international cooperation in information and evidence gathering, extradition of criminals between states, and general judicial assistance. Recognizing that no single state can effectively confront cyber risks alone, Algeria has engaged in numerous regional and international agreements emphasizing the necessity of international cooperation to combat these crimes, given their border-transcending nature. Treaties and international agreements are crucial in establishing a legal framework for inter-state cooperation in combating cybercrime. The Budapest Convention on Cybercrime is considered one of the most significant agreements, setting standards for legal cooperation and information exchange.

International cooperation in combating cybercrime takes several forms, among them:

I.2.3.1- International Security Cooperation: ^[38]

Practical reality has demonstrated that no single state can effectively combat cybercrime due to the remarkable advancements across all facets of life. Consequently, there is an urgent need for an international entity tasked with this mission, enabling police forces from various countries to collaborate, especially concerning the swift exchange of information regarding cybercrimes and criminals.

Practical examples of international cooperation include the International Criminal Police Organization (INTERPOL), which plays a vital role in combating cybercrime through its INTERPOL Global Complex for Innovation (IGCI). The IGCI provides technical support and investigative assistance. Established by a decision of the United Nations General Assembly in 1923, INTERPOL operates under its auspices and supervision, aiming to enhance and promote international police cooperation in security matters. INTERPOL supports member-state law enforcement agencies by facilitating cooperation and coordination in combating transnational and organized crime. This involves collecting and exchanging data and information about criminals and crimes through INTERPOL's National Central Bureaus in member states.

Furthermore, cooperation extends to aiding in the apprehension of criminals with the support of police forces from partner countries, as well as providing available information within their jurisdictions, particularly in complex crimes involving multiple countries, including cybercrimes.

I.2.3.2- International Judicial Assistance:

International judicial assistance is any legal measure undertaken by one country to facilitate proceedings for a specific crime in other countries. Algerian legislation enshrines the principle of mutual international judicial assistance in Law No. 09/04 concerning special rules for preventing and combating crimes related to information and communication technologies. Article 16 of this law states that, in the context of international investigations and judicial inquiries aimed at gathering electronic evidence, international judicial assistance can take various forms, including: ^[39]

- Information exchange.
- Transfer of proceedings.
- International legal commissions.

I.2.3.3- Extradition of Criminals:

Extradition is when a state, based on a treaty or the principle of reciprocity, surrenders a person requested by another state to face charges for a specific crime or to serve a criminal sentence. Most countries require dual criminality for the conduct prompting extradition, meaning the act must be punishable under the laws of both the requesting and requested states.^[40]

The importance of this international cooperation is evident in addressing transnational crimes, including cybercrimes like internet offenses. If a country's legislation allows prosecuting an accused individual within its territory, it proceeds; otherwise, the individual is tried in another competent state. This cooperation aims to ensure that criminals do not escape justice, particularly when the national law of the state where the criminal is present does not permit prosecution.^[41]

I. 3- The Role of Artificial Intelligence in Achieving Cybersecurity:

Artificial Intelligence (AI) has ushered in a profound transformation in the contemporary world, emerging as a vital tool in addressing cybersecurity challenges. AI contributes to developing intelligent agents, which can be hardware or software. These agents are designed to efficiently tackle specific security issues through monitoring, learning, and making informed decisions. They can identify vulnerabilities in complex code, detect unusual patterns in user login methods, and even recognize new types of malicious software that traditional tools may overlook. Intelligent agents operate by processing vast amounts of data to discern patterns. When deployed in defense systems, they leverage this knowledge to analyze incoming data, including previously unidentified data points. The role and utilization of AI in cybersecurity are experiencing rapid growth, with many organizations adopting this technology as a fundamental tool in their security strategies.^[42]

Among the applications of artificial intelligence in enhancing cybersecurity, we mention the following:

I. 3.1- Handling Large Amounts of Data:

There are many activities on our servers, meaning vast amounts of data are transferred daily between our clients, facilities, devices, and networks. Cybersecurity personnel face significant challenges in manually reviewing all activities to detect potential threats. Here, artificial intelligence plays a crucial role by automatically scanning and analyzing these activities, facilitating threat detection, and effectively enhancing preventive measures against them.^[43]

I. 3.2- Predicting Future Threats:

Artificial intelligence analyzes large datasets from multiple sources, such as network logs and security systems, to extract potential threat patterns. Machine learning techniques are used to identify unusual or suspicious behaviors that may indicate potential future attacks. In this context, the software company Seculancy, founded in 2012, has integrated artificial intelligence into its cybersecurity, replacing lightweight machine learning models with virus-resistant software. Artificial intelligence's capabilities have expanded to include vulnerability monitoring, behavioral analysis, predictive analytics, and strengthening defensive mechanisms against sophisticated attacks.^[44]

I. 3.3- Streamlining Operations:

One of the significant benefits of using artificial intelligence in security is its ability to detect and prevent core security threats regularly. It also plays a comprehensive analytical role in identifying potential security vulnerabilities, enabling companies to implement network security best practices without exposing themselves to human error or the monotony that affects cybersecurity teams.

I. 3.4- Accelerating Detection and Response Times:

By integrating artificial intelligence with cybersecurity, companies ensure rapid detection of security threats and timely response. AI conducts comprehensive system scans, identifies threats early, and facilitates security operations.

I. 3.5- Combating Malicious Robots:

Many robots are used in malicious activities such as malware distribution and data theft. Artificial intelligence can identify patterns of these robots, recognize them, and block them.

I. 3.6- Securing Authentication:

Artificial intelligence provides various tools, such as fingerprint scanners and facial recognition, which are essential for securing authentication during login attempts on sites containing sensitive information, requiring an additional security layer for protection. These tools help detect fraudulent login attempts and electronic attacks to steal data.

I. 3.7- Improving Accuracy and Efficiency:

AI-based cybersecurity systems offer better accuracy and efficiency compared to traditional security solutions. AI algorithms can identify patterns that human eyes cannot detect, thereby increasing the accuracy of detecting malicious activities.^[45]

However, artificial intelligence (AI) technologies in cybersecurity face significant challenges. Integrating AI into cybersecurity systems involves numerous obstacles and typical constraints, hindering its adoption and utilization by cyber criminals. These challenges include the critical need for substantial investments in computing power, storage, and data centers to build and maintain AI systems. The integration of AI in cybersecurity has become indispensable for organizations despite the many challenges obstructing its adoption and advancement. These challenges include the difficulty of acquiring specialized talents and the need for expertise in artificial intelligence technologies and information security. Analyzing complex data is also a significant challenge, as AI requires precise and comprehensive data interpretation to effectively analyze behavioral patterns and potential threats. Furthermore, it remains crucial to select and deploy the right AI technologies. These tools must be sophisticated and tailored to the enterprise's cybersecurity needs.^[46]

Artificial intelligence applications in cybersecurity require robust and advanced systems capable of processing large volumes of data in real time, which can pose challenges in performance and efficiency. These challenges underscore the importance of continuous innovation and strategic investments in AI technology to enhance organizations' ability to efficiently and effectively combat growing cyber threats.^[47]

II- Conclusion:

The issue of achieving cybersecurity constitutes one of the most significant challenges facing Algeria amidst rapid and advanced technological developments. Algeria has diligently exerted efforts by adopting comprehensive and practical legal and structural mechanisms to enhance cybersecurity and protect society from diverse electronic threats. These efforts have included legislative developments, such as Law No. 04-15, which criminalizes actions that interfere with computer systems and automated data processing. This law penalizes crimes related to unauthorized hacking, misuse of data, and other illegal cyber activities. Additionally, Law No. 09-04 has provided a set of preventive measures for early detection of cybercrimes and necessary actions to prevent them, emphasizing international cooperation and judicial assistance. Law No. 06-23 focuses on protecting individuals' private lives by providing criminal protection against the misuse of modern technology.

Furthermore, Algeria has established entities dedicated to combating electronic crime and enhancing cybersecurity at all levels, such as the National Authority for Preventing Crimes Related to Information and Communication Technologies, the National Institute of Criminal Evidence on Cybercrime, and the Judicial Pole for Combating Crimes Related to Information and Communication Technologies...

Based on the above, the following recommendations can be proposed:

- The Algerian legislature must address deficiencies in laws related to cybercrime and enhance and update legislation to combat cybercrimes effectively, ensuring the protection of individuals and institutions against increasing threats and securing appropriate penalties for perpetrators of cybercrimes.
- Enhancing international cooperation and the principle of mutual legal assistance in combating cybercrimes, exchanging information and expertise, and developing a collaborative framework to counter cyberattacks is imperative. This cooperation can be fortified by adopting international standards, organizing knowledge-sharing events, and consolidating efforts.
- Activating civil society and institutions' role in raising awareness about the importance of cybersecurity is a fundamental step in combating cybercrimes. It is imperative for individuals to understand cyber threats and potential risks and to take appropriate preventive measures. This can be achieved through comprehensive awareness campaigns and education about best practices in technology use and protection against electronic attacks.
- Utilizing advanced technology and innovative solutions, such as artificial intelligence and big data analysis, to enhance cybersecurity is crucial. Developing monitoring and automatic detection systems to combat potential attacks and enhance preventive measures is also necessary.
- We are achieving cybersecurity through specialized agencies to prevent and combat electronic crime.
- We are enhancing cybersecurity in educational institutions by providing programs focused on information security, personal data protection, and comprehensive training for students and teachers on safe and effective technology use.
- Companies can develop advanced technological solutions for detecting and defending against attacks. Government and private institutions should collaborate to exchange information and expertise to enhance cybersecurity and ensure the security of the digital society.
- Adhering to best practices and international standards in information security, including preventive protection measures, incident response, and risk management, is essential for both the public and private sectors.

In conclusion, achieving cybersecurity in combating electronic crime requires comprehensive cooperation among all relevant entities, concerted efforts, and adopting a proactive and integrated approach. International cooperation and coordination significantly enhance the state's protection and cyber stability, building a safe and protected environment from ongoing cyber threats.

Referrals and References:

- [1] Ismahane Bouadiyaf (2018), “**Electronic Crime and Legislative Measures to Confront it in Algeria**”, *Journal of Teacher Researcher of Legal and Political Studies*, Number 11, Algeria: Faculty of Law and Political Science, University Mohammed Boudiaf Msila, pp. 350-351.
- [2] Abdel Salam Mohammed Almayel, Adel Mohammed Al-Sharabaji (2019), “**Cybercrime in Cyberspace (Concept, Causes, Countermeasures with a Case Study on Libya)**”, *AFAQ Review of Research and Studies*, Number 04, Algeria: University Center El-Ilizi, pp. 245-246.
- [3] Azeez Nureni Ayofe, Osunade Oluwaseyifunmitan (2009), “**TOWARDS AMELIORATING CYBERCRIME AND CYBERSECURITY**”, *International Journal of Computer Science and Information Security*, Number 1 (Volume 3), p. 2.
- [4] Huda Hamed Qushqush (1992), **Cybercrimes in Comparative Legislation**, Cairo, Egypt: Dar Al-Nahda Al-Arabiya, p. 05.
- [5] Mohamed Ali Al-Aryan (2009), **Information Crimes**, Alexandria, Egypt: Dar Al-Jami'a Al-Jadida, 2nd edition, p. 170.
- [6] Abdullah Daghash Al-Ajmi (2014), “**Practical and Legal Issues of Cybercrimes: A Comparative Study**”, Master's Thesis in Public Law, Middle East University, p. 14.
- [7] Mohamed Obaid Al Kaabi (2009), **Cybercrimes arising from unauthorized internet use**, Cairo, Egypt: Dar Al Nahda Al Arabiya, p. 31.
- [8] Mohamed Rahmouni (2017), “**Characteristics of Cybercrime and its Applications**”, *EL - HAKIKA (the Truth) Journal*, Number 41, Algeria: Ahmed Draya University-Adrar, p. 441.
- [9] Naila Adel Mohamed Fareed Qurra (2005), **Economic Computer Crimes**, Beirut, Lebanon: Al Halabi Legal Publications, 1st edition, p. 52.
- [10] Tamim Abdullah Saif Al-Tamimi (2016), **Cyber Crimes in Assaulting Individuals**, Riyadh, Saudi Arabia: Law and Economics Library, First Edition, p. 16.
- [11] Mohamed Rahmouni, Op-Cit, p. 443.
- [12] Idris Attia (2019), “**The position of cybersecurity in the Algerian national security system**”, *Credibility Journal*, Number 01 (Volume 01), Higher Military School of Information and Communication, p. 109.
- [13] Soliman Gataf, Abdel Halim Bougrin (2022), “**Facing Cybercrimes in Light of International Agreements**”, *Journal of Legal and Economic Research*, Number 02 (Volume 05), Algeria: the University Center in Aflou, p. 72.
- [14] Jamal Maatouk (2022), “**Introduction to Cybercrime**”, a paper presented as part of Proceedings of the Virtual National Forum on **(Cybercrime in Algerian Society)**, organized by the Faculty of Humanities and Social Sciences, Algeria: Yahia Fares University of Medea, p. 17.
- [15] Mansour Abdul Salam Abdul Hameed Hassan (2023), “**Cyber Extortion Crime: A Comparative Study between Egyptian, French, Emirati, and Saudi Laws**”, *Legal Journal*, Number 05 (Volume 17), Egypt, p. 881.
- [16] Mariem Baltah, Asia Burgit (2022), “**Cyber Security in Confronting Cyber Piracy**”, *Studies in Human Rights*, Number 01 (Volume 06), Egypt, p. 14.
- [17] Mohammed Taha Ibrahim Alfalih (2024), “**Cybercrime in the Jordanian Legal System**”, *Al-Zarqa Journal for Research and Humanities Studies*, Number 01 (Volume 24), Jordan: Zarqa University, p. 114.
- [18] Mona Al-Ashqar Jabbour (2012), “**Cybersecurity: Challenges and Requirements for Confrontation**”, *First Annual Meeting of Cybersecurity Specialists*, Beirut, Lebanon: League of Arab States, Arab Center for Judicial and Legal Research, pp. 27-28.
- [19] Shweireb Djilali, Mourad Faiza (2023), “**The Concept of Cyber Wars and Cybersecurity**”, *Journal of Rights and Freedoms*, Number 1 (Volume 11), Algeria: Faculty of Law and Political Science, University of Biskra, p. 165.
- [20] Abdul Rahman Al-Laqani (2023), “**The Role of Cybersecurity in Enhancing the Security of Electronic Financial Information**”, Amman, Jordan: Al-Yazouri Scientific Publishing and Distribution House, p. 151.
- [21] Nada bint Khaled Al-Murdas (2023), “**Cyber security in the Kingdom of Saudi Arabia between Reality and Hope (Analytical Theoretical Study)**”, *International Journal of Research and Studies Publishing*, Number 49 (Volume 05), p. 214.
- [22] Mohammad Abdullah Shaheen Mohammad (2023), **Cybersecurity and Information Protection Systems**, Amman, Jordan: Dar Yafa Al-Elmia for Publishing and Distribution, pp. 9-10.
- [23] Nada bint Khaled Al-Murdas, Op- Cit, p.214.
- [24] Nada bint Khaled Al-Murdas, Op- Cit, p. 215.
- [25] Abdul Rahman Al-Laqani, Op – Cit, pp. 153-154.
- [26] Mohammad Abdullah Shaheen Mohammad, Op-Cit, p. 11.

- [27] Law No. 04-15, dated November 10, 2004, amending and supplementing Ordinance No. 66-156, dated June 8, 1966, **which includes the Penal Code**, Official Journal, Number 71, dated 2004.
- [28] Law No. 06-23, dated December 20, 2006, amending and supplementing Ordinance No. 66-156, dated June 8, 1966, **which includes the Penal Code**, Official Journal, Number 84, dated 2006.
- [29] Law No. 09-04, dated August 5, 2009, **containing specific rules on preventing and combating crimes related to information and communication technologies**, Official Journal, Number 47, dated August 16, 2009.
- [30] Mehdi Reda (2021), “**Cybercrimes and Their Countermeasures in Algerian Legislation**”, Eliza Journal of Research and Studies, Number 02 (Volume 06), Algeria: Eliza University Center, pp. 118-119.
- [31] Presidential Decree No. 15-261, dated October 8, 2015, **delineates the composition, organization, and operational procedures of the National Authority for the Prevention of Crimes Connected with Information Technology and Communication**, as published in the Official Journal, Number 53, dated October 8, 2015.
- [32] Article 14 of Law No. 09-04 aforementioned.
- [33] Presidential Decree No. 04-183, dated June 26, 2004, **establishes the National Institute of Criminal Evidence and Criminology for the National Gendarmerie and defines its statutory framework**, as published in the Official Journal, Number 41, dated June 27, 2004.
- [34] Decree No. 21-11, dated August 25, 2021, **amending and supplementing the Criminal Procedure Law and establishing the Judicial Pole for Combating Cybercrimes**, Official Journal, Number 65, dated August 26, 2021.
- [35] Refer to: Salma Abd al-Nabi (2024), “**The Role of the National Judicial Pole for Combating Crimes Related to Information and Communication Technologies in Addressing Attacks on Data**”, Journal of Rights and Political Sciences, Number 02 (Volume 11), Algeria: University of Khenchela, pp. 22-23.
- [36] Asia Lamrani (2012), “**International Cooperation in confronting Cybercrimes: Algeria as a Model**”, Algerian Journal of Political Science and International Relations, Number 02 (Volume 03), Algeria: University of Algiers 3, p. 75.
- [37] Jamal Bouazdia (2019), “**Algeria's Strategy in Confronting Cybercrime: Challenges and Future Prospects**”, Journal of Legal and Political Sciences, Number 01 (Volume 10), Algeria: Faculty of Law and Political Sciences, University of Eloued, p. 1280.
- [38] Bricchi Belkacem (2023), “**International Cooperation in Combating Cybercrime**”, Academic Journal of Legal and Political Research, Number 2 (Volume 7), Algeria: Faculty of Law and Political Science, Amar Telidji University in Laghouat, p 50.
- [39] Bricchi Belkacem, Op-Cit, p. 51.
- [40] Ghanem Mardhi Al-Shammari (2016), **Cybercrimes (Their Nature, Characteristics, and Legal Countermeasures)**, Amman, Jordan: International Scientific Publishing and Distribution House, p. 102.
- [41] Farid Nashef (2022), “**Mechanisms of International Cooperation in Combating Cybercrimes**”, Journal of Legal and Political Sciences Research, Number 1 (Volume 8), Algeria: Faculty of Law and Political Sciences, Ibn Khaldoun University in Tiaret, p. 442.
- [42] <https://www.encryptionconsulting.com/the-role-of-artificial-intelligence-ai-in-modern-cybersecurity>, the website was visited on: 17/07/2024, at 14:00 (GMT).
- [43] Urvi Sharma (2023), “**Strategies and challenges in combating cybercrime: A comprehensive Analysis Of Cybersecurity Technologies, Legal, Frameworks, and Preventative Measures**”, China Petroleum Processing and Petrochemical Technology, Number 2 (Volume 23), China, p. 4634.
- [44] **Confronting Cyber Threats in the Age of Artificial Intelligence**, <https://aawsat.com>, the website was visited on 17/07/2024 at 14:50 (GMT).
- [45] <https://bakkah.com/ar/knowledge-center> the website was visited on: 16/07/2024, at 21:49 (GMT).
- [46] Mohammed Dahmani (2023), “**Artificial Intelligence as a Mechanism to Enhance Cyber security**”, the Journal of Legal and Political Thought, Number 02 (Volume 07), Algeria: Faculty of Law and Political Science, University of Laghouat, p. 606.
- [47] Mohammed Dahmani, op-cit, p 606.