

Cybercrime and Its Threats to Cybersecurity

الجريمة السيبرانية وتهديداتها للأمن السيبراني

La cybercriminalité et ses menaces pour la cybersécurité

Bouchala, Samira^{*1}

Date of submission 14/03/2025- Date of acceptance 11/05/2025- Date of edition : 11 /06 /2025

ملخص:

تروم هذه الورقة البحثية إلى تسليط الضوء على الجريمة السيبرانية كواحدة من التحديات المعاصرة المهددة للأمن السيبراني، والتي تمثل الوجه السلبي لتطور وانتشار تكنولوجيا الإعلام والاتصال. جريمة سنعمل على تعريفها، استخلاص أهم مميزاتها، رصد أنواعها، الكشف عن تهديداتها والنظر في سبل مكافحتها.

الكلمات المفتاحية: الجريمة السيبرانية؛ الأمن السيبراني؛ تهديدات.

Abstract:

This study aims to shed light on cybercrime as one of the contemporary challenges threatening cybersecurity, representing the negative aspect of the development and spread of information and communication technology. The study will define cybercrime, identify its key characteristics, examine its types, reveal its threats, and explore ways to combat it.

Keywords: Cybercrime; Cybersecurity; Threats.

Résumé :

Cette étude vise à mettre en lumière la cybercriminalité en tant que l'un des défis contemporains menaçant la cybersécurité, représentant l'aspect négatif du développement et de la diffusion des technologies de l'information et de la communication. L'étude définira la cybercriminalité, identifiera ses principales caractéristiques, examinera ses types, mettra en évidence ses menaces et explorera les moyens de la combattre.

Mots-clés : Cybercriminalité ; Cybersécurité ; Menaces.

* Corresponding author.

¹ Bouchala, Samira, University of Salah Bounider Constantine 3, Laboratory of Sociology of Communication for Research and Translation: Algeria, samira.bouchaala@univ-constantine3.dz

Introduction :

The massive development and widespread expansion of modern communication technology, along with its increasing use by individuals and various institutions, have brought numerous advantages. Among the most significant are fast, precise, cost-effective, and highly efficient digital services. However, this technological advancement has also become a major concern for societies due to the negative consequences it has produced, foremost among them being cybercrime.

Cybercrime has become a significant challenge to cybersecurity, posing both material and moral threats to cyberspace users on one hand and spreading rapidly and evolving daily on the other. This widespread and alarming growth necessitates urgent measures to combat this phenomenon.

This study seeks to examine cybercrime, as any attempt to deter this negative phenomenon cannot achieve its objectives without a deep understanding of its nature. Therefore, we have endeavored to comprehend cybercrime by defining it, identifying its characteristics, categorizing its types, diagnosing its causes, assessing its threats, and finally, exploring ways to combat it.

1- Definition of Cybercrime

Cybercrime is a concept that combines two terms: "crime" and "cyber." Therefore, we will examine each term separately before arriving at the composite meaning of both words.

1-1. Linguistic and Terminological Definition Crime

1-1-1. Linguistic Definition of Crime

The term "crime" (jarīmah) is derived from "jurm," which means cutting; for example, a "shajarat jarīmah" refers to a cut-down tree (Nadia, 1992, p. 192). The plural of "jarīmah" is "jarā'im," referring to an offense punishable by law (Al-Munjid in Contemporary Arabic Language, 2001, p. 195). According to *Lisan al- 'Arab*, "jurm" means committing a crime. The phrase "jurm idhā 'aẓuma jurmuhu" indicates that someone has sinned greatly, meaning the act involves wrongdoing and transgression (Ibn Manzur, 1997, p. 19).

The linguistic meaning of "crime" also implies illicit or undesirable gain. It can refer to any act that is socially or morally unacceptable and contradicts justice and fairness (Akram, 2005, p. 39). The phrase "kharaja yajrimu li'ahlīhi" means seeking or scheming for gains, with the term specifically used to denote sinful earnings (Rawdah, 1992, p. 40). Thus, linguistically, the term "crime" signifies wrongdoing, transgression, illicit gain, undesirable acts, fraud, and violations of justice and fairness.

1-1-2. Terminological Definition

Several definitions of crime have been proposed, including:

- Crime is any behavior that contradicts what society deems acceptable, harms social interests, violates traditions, customs, and norms, and necessitates accountability and punishment for its perpetrators (Barakat, 1997, p. 32).
- It is any act or omission punishable by law with a criminal penalty (Ahsan, 2011, p. 27).

Therefore, in its social sense, crime represents a deviation from the collective norms of society. From a legal perspective, it refers to a failure to comply with legal provisions, whether by committing acts that violate the law or by neglecting obligations mandated by it.

1-2. Linguistic and Terminological Definition of Cyber

1-2-1. Linguistic Definition:

The term *cyber* is derived from the word *cyber* itself, referring to anything related to computer culture, information technology, or virtual reality. *Cyber* essentially means "internet space" and is derived from the Greek term *kubernan*, which means management and control ([Hakima, 2021, p. 651](#)).

According to the Oxford Dictionary, *cyber* is defined as "the study of human work efficiency by comparing it to the efficiency of computing machines; it relates to the characteristics of computers, information technology, and virtual reality." However, in Arabic, specialists face challenges in finding an exact equivalent for the term *cyber* ([Idris, 2019, p. 103](#)).

1-2-2. Terminological Definition

Cyber refers to anything electronic, and the term "cyber" has been conventionally used to describe anything related to computer networks and the internet. For instance, *cyberspace* refers to the electronic space, encompassing everything related to computer networks, the internet, and various applications such as WhatsApp, Facebook, and hundreds of other digital platforms. It also includes online services such as money transfers, e-commerce, and other internet-based activities across various fields worldwide.

Norbert Wiener defines cybernetics as "the science of leadership and control in both living organisms and machines, as well as the study of communication mechanisms" ([Idris, 2019, p. 103](#)).

1-3. Cybercrime

Based on the linguistic definitions of "crime" and "cyber," the linguistic meaning of cybercrime refers to offenses such as fraud, deception, unauthorized gain, violation of rights and justice, all committed via the internet or electronically.

Numerous definitions of cybercrime have been proposed, including:

- "Any criminal act in which a computer is used as a primary tool" ([Al-Qadi, 2021, p. 17](#)).
- "The use of information and communication network technologies as a medium for committing crimes" ([Finey, 2025](#)).
- "Cybercrime is a broad term referring to crimes committed using electronic data storage or communication devices" ([Brown, 2015, p. 57](#)).

These definitions focus on the means through which cybercrimes are committed. The first definition emphasize the role of computers as the primary tool for committing cybercrimes. However, some argue that for a crime to be classified as a cybercrime, it must involve at least two electronic devices. Crimes committed using a single device, such as document forgery or illegal publication, may be classified as computer crimes but not necessarily as cybercrimes. However, once the act

involves transmission from one electronic device to another, it qualifies as a cybercrime (Soumia, 2021, p. 293).

The second and third definitions focus on the technologies associated with information and communication networks as essential tools for committing cybercrimes. This implies that cybercrime is linked to modern electronic devices beyond just computers, as technological advancements have expanded to include various electronic devices capable of storing and transmitting information, such as digital planners, smartphones, and other innovations appearing daily in the global tech landscape (Soumia, 2021, p. 294).

Thus, cybercrime is only possible with the internet and digital technologies, often targeting technological infrastructures through means such as creating and spreading computer viruses or launching cyberattacks against critical national IT facilities.

Given the reliance on technology, cybercrime has been referred to by multiple names, including electronic crime, computer crime, internet crime, information crime, high-tech crime, and the crime of the digital age. All these terms share a common element: unauthorized access to computer systems and data (Hakima, 2021, p. 652).

Other definitions of cybercrime include:

- "Any unlawful act where substantial knowledge of computing technology is required both to commit and to investigate the crime" (Soumia, 2021, p. 291).
- "A newly emerging crime where the perpetrator relies on technical means and possesses sufficient expertise in using information systems" (Nabil, 2017, p. 19).

These definitions emphasize expertise, knowledge, and proficiency in information and communication technologies as key factors in committing cybercrimes. Since technology is the foundation of cybercrime, it cannot be carried out without the perpetrator's knowledge of how to use these advanced technologies. This knowledge is not limited to criminals but also extends to law enforcement officials investigating such crimes and judges overseeing legal proceedings.

Other perspectives define cybercrime as:

- "An unlawful activity aimed at copying, modifying, deleting, or accessing information stored within a computer system and transmitted through it" (Soumia, 2021, p. 292).
- "Any act or omission by an individual that causes harm to the physical or digital components of a computer system and its communication networks, as they represent protected legal interests" (Mehdi, 2021, p. 113).
- "All unlawful behaviors that utilize electronic processes to target the security of information systems and the data they process" (Beas, 2016, p. 26).

These definitions approach cybercrime from a different perspective. Instead of focusing on the means of committing the crime or the technical expertise of the criminal, they highlight the nature of the crime, its domain, and the interests it targets. Cybercrimes encompass cyberattacks, espionage,

trespassing, and inflicting material or psychological harm. In a broader sense, cybercrime refers to "unlawful activities occurring in cyberspace."

There is no universally accepted definition of cybercrime. Each definition attempts to frame it from a specific angle: the means by which it is committed, the technical knowledge required, or its subject matter and domain.

Ultimately, cybercrime involves illegal and unethical actions that take place in cyberspace, leveraging the perpetrator's expertise in information and communication technologies to harm information systems and communication networks.

2- Characteristics of Cybercrime

Based on the previous definitions, cybercrime is distinguished by several characteristics, including:

2-1. Underreporting

Cybercrime victims often refrain from reporting incidents, especially when the victims are financial institutions or large corporations. This is due to concerns among board members about negative publicity, which may affect the institution's reputation or lead to a loss of trust from clients and stakeholders. Consequently, they avoid disclosing security breaches and violations against their information systems (Soumia, 2021, p. 295).

2-2. Difficulty in Detection

Cybercrimes are difficult to detect as they leave no physical traces, relying instead on digital information traces (Mehdi, 2021, p. 114). Moreover, perpetrators employ sophisticated technical methods that allow them to erase incriminating evidence, making tracking them more complex.

2-3. Difficulty in Proving the Crime

Cybercrimes are often committed by individuals with high intelligence, expertise, and proficiency in information technology. They execute crimes with meticulous planning to ensure success and evade detection by authorities (Ismail, 2021, p. 70). Additionally, these crimes are often carried out within seconds, making it easy for criminals to erase or manipulate evidence. A further challenge is that many judicial systems do not recognize digital evidence, which consists of magnetic fields and electrical impulses that are intangible to human senses (Hakima, 2021, p. 652).

2-4. Difficulty in Enforcing Punishment on Perpetrators

Several obstacles hinder the punishment of cybercriminals, primarily the lack of legal frameworks addressing this type of crime. Additionally, cybercrime laws vary from one country to another, meaning certain unlawful acts may not be classified as crimes under some legal systems. This creates challenges in applying criminal law, especially considering the legal principle that "no crime and no punishment exist without a legal provision" (Soumia, 2021, p. 298).

2-5. High Appeal to Perpetrators

Cybercrimes are particularly attractive to criminals due to the substantial financial gains they can generate, their ease of execution compared to traditional crimes, and the low risk of detection or prosecution (Al-Ajmi, 2014, pp. 23-25).

2-6. Transnational Nature

Cybercrimes transcend geographical boundaries, as the widespread use of the internet enables criminals to operate from one country while targeting victims in another (Al-Qatawneh, 2010, p. 05). This necessitates international and domestic legal frameworks to combat such crimes effectively. Addressing these crimes poses legal and political challenges similar to those associated with money laundering and drug trafficking (Hakima, 2021, p. 652).

3- Types of Cybercrime

With the advancement and widespread use of information and communication technology, crimes committed within cyberspace have also evolved. These types include (Abdelaziz, 2021, p. 261):

- **Crimes Against Individuals:** Also known as personal internet crimes, these include identity theft, unauthorized access to online accounts, and impersonation of individuals—whether they hold political or diplomatic positions or are ordinary people. These crimes involve illegal access to individuals' electronic identities, such as email accounts and passwords, and may extend to impersonation, stealing important files and photos from their devices to exploit their identity, conceal the criminal's identity, or blackmail victims into compliance.
- **Crimes Against Governments** These crimes target official government websites and network systems, aiming to destroy their infrastructure completely. Perpetrators of such crimes are referred to as hackers, and their objectives are often politically motivated.

Additional types of cybercrimes include (Hakima, 2021, p. 653):

- **Financial Crimes:** These crimes cause financial damage to victims through fraud, including electronic theft, hijacking ATM machines and banks, creating counterfeit websites resembling major banks, and sending fraudulent emails soliciting financial contributions in exchange for promised rewards.
- **Cultural Crimes:** These involve the theft of intellectual property and attributing it to the perpetrator without the victim's consent. Examples include software piracy, where criminals copy and sell copyrighted software at lower prices, piracy of satellite channels, and the unauthorized reproduction of scientific and literary works.
- **Political and Economic Crimes:** These crimes are often used by terrorist groups to communicate, spread false information, transfer funds, take control of sensitive websites, steal confidential data, and distribute viruses. They also aim to mislead and influence youth by promoting terrorism and drug addiction to destabilize states for political and economic reasons.
- **Sexual Crimes:** These include blackmail, deception, and enticement through online platforms.
-

4- Reasons for Committing Cybercrime

Several factors have contributed to the commission and spread of cybercrime, including:

4-1. Fascination with Information Technology

With the emergence and widespread use of information technology, including computers and data systems, some criminals become fascinated by these advancements. These individuals are not necessarily highly dangerous but often seek to achieve technological victories without having malicious intent ([Abdelaziz, 2021, p. 238](#)).

4-2. Passion for Collecting Information

Some individuals commit computer crimes to gain access to new information. Hackers believe that information should be unrestricted and dedicate their efforts to learning how to breach secure websites. Often, hackers operate in groups that collaborate to exchange information, share programs, and distribute news. Their goal is to remain anonymous for as long as possible to continue accessing restricted systems and improving their knowledge of hacking techniques and espionage technologies ([Hakima, 2021, p. 654](#)) ([Nabil, 2017, p. 31](#)).

4-3. Desire for Financial Gain

The need for quick wealth can drive individuals to cybercrime, as they seek to access and sell sensitive information to interested parties. Various techniques are employed to achieve this goal, making financial gain one of the most common motives for cybercrime. Many offenders are driven by financial pressures such as debt, financial struggles, or even drug addiction ([Abdelaziz, 2021, p. 238](#)).

4-4. Desire to Overcome Information Systems and Prove Self-Worth

Hacking into electronic systems and bypassing security barriers can provide a sense of enjoyment and entertainment for offenders. For some, it serves as a way to pass the time while demonstrating their superiority, power, and even a sense of grandeur ([Hakima, 2021, p. 654](#)).

4-5. Personal Motives

Individuals may be influenced by external factors surrounding them, and being in an automated information-processing environment can contribute to the commission of cybercrimes. Various influences can push individuals toward such behavior, whether for amusement or revenge ([Nabil, 2017, p. 31](#)).

5- Cybercrime Threats

Cybercrime threats refer to attacks carried out using electronic mechanisms and networks such as the internet and computer systems. These attacks aim to harm devices, networks, or data rather than directly targeting individuals. Instead, they impact the digital space by affecting the networks and systems that individuals and nations rely on, ultimately posing a significant threat to national security ([Hakima, 2021, p. 658](#)).

Cyber threats have become a major challenge to cybersecurity, including:

5-1. Infection through Viruses and Malicious Software

Malware and viruses can corrupt computer systems, destroy software, and damage user data. Attackers exploit vulnerabilities by injecting malicious programs into victims' computers, often through deceptive advertisements or links designed to attract users. These harmful codes are planted into the victim's device once the link is clicked. Social media platforms are commonly used to spread such malicious links, potentially affecting hundreds of users, including officials ([Abdelaziz, 2021, pp. 246-247](#)).

Additional threats include ([Hakima, 2021, pp. 658-659](#)):

5-2. Information Sabotage and Misuse

This involves erasing files or destroying storage media. One of the most significant forms of sabotage is encrypting critical data and withholding the decryption key. Misuse of information also includes actions that prevent authorized users from accessing their data, exposing confidential information, or exploiting it to harm the interests of the data owner.

5-3. Data Forgery and Counterfeiting

Cybercriminals manipulate databases by inserting false data or deliberately modifying records using specialized software. This includes falsifying documents, creating counterfeit financial instruments like bank notes and securities, and forging trademarks.

5-4. Privacy Violations

Unauthorized collection and storage of personal data, along with its misuse or unlawful disclosure, pose a significant cybersecurity risk. Violations also include unauthorized access to private communications and correspondence.

5-5. Cyber Espionage

The digital environment allows unauthorized access to confidential information that governments and organizations seek to protect. Cyber espionage now extends to various fields, including industrial, military, economic, and security domains. One of the most targeted areas is military intelligence, which involves sensitive state secrets related to strategic and national security matters. The use of advanced information systems has made it easier for hackers to access such classified data, threatening national security.

5-6. Hacking and System Breaches

Hackers exploit security vulnerabilities in websites and networks to gain unauthorized access to private data. They use various software tools to achieve illegal objectives such as data theft, system sabotage, file deletion, or inserting harmful programs. These activities contribute to numerous cybersecurity threats, undermining digital security on a global scale.

6- Ways to Combat Cybercrime

There are various ways to address the threat of cybercrime. With the emergence of this risk, efforts have been made to develop technologies and software to protect information and electronic devices, leading to the establishment of multiple mechanisms aimed at achieving **cybersecurity**. Cybersecurity refers to the technologies and measures designed to protect computers, networks, and data from unauthorized access or attacks intended for exploitation (Ismail, 2021, p. 73).

Cybersecurity can be achieved through several approaches and mechanisms, including:

6-1. Protection Programs

Protection programs enhance cybersecurity by filtering and blocking dangerous websites, as well as managing internet usage time. Some specialized programs are designed to protect children by restricting their access to certain websites and preventing them from sharing personal information online (Cherif, 2019, p. 70). Among these programs are:

6-1-1. Firewalls

Firewalls help prevent cyberattacks and reduce the risks of account breaches and unauthorized access to government and private information systems. They play a critical role in protecting national security, the economy, banking institutions, and government data, while also increasing trust in national information systems (Ismail, 2021, p. 74).

One of the most widely used firewall programs is Firewall Software, which acts as a robust strategy to prevent unauthorized access from the internet. The firewall functions as an electronic gateway that monitors network traffic. Statistics indicate that more than one-third of websites on the internet are protected by some form of firewall (Cherif, 2019, p. 70).

6-1-2. Antivirus Protection

Antivirus software is essential in cybersecurity, playing a key role in protecting computers and networks. Every computer should have one of these programs installed. Effective antivirus programs include Norton Antivirus, PC-Cillin, McAfee, and Kaspersky, among others.

Antivirus software is capable of detecting and preventing harmful or malicious programs from infiltrating and damaging devices. Users should regularly update their antivirus programs to ensure protection against newly emerging cyber threats. Ideally, these programs should be set to update automatically via the internet on a daily basis (Allouti, 2009, p. 173).

6-1-3. Intrusion Detection and Misuse Prevention

This mechanism aims to detect malicious activity in its early stages by monitoring suspicious behaviors. If a potential threat is identified early, it can be stopped before causing harm. Additionally, intrusion detection systems serve as digital evidence that can be used in court to prosecute cybercriminals (Cherif, 2019, p. 70).

6-2. Electronic Signature

An electronic signature is a small digital file composed of letters, numbers, and electronic symbols issued by a certified authority recognized both nationally and internationally. This

certification, known as a Digital Certificate, contains all relevant information about the user, including the certificate number, issuance date, and issuing authority.

Each certificate is accompanied by two cryptographic keys: a public key that is accessible to everyone and a private key used for personal authentication. Unlike a handwritten signature, an electronic signature is not a simple digital scan of a signature. Instead, it is a unique digital certificate issued by an independent organization that verifies the identity of the user.

Electronic signatures can be used to send documents, commercial contracts, commitments, and official decisions. They are legally recognized under U.S. law and are expected to gain legal recognition in many other countries soon ([Allouti, 2009, pp. 173-174](#)).

6-3. Establishing National Cybersecurity Agencies

Cyberspace is a non-physical domain where communication networks and information storage systems operate globally. As a result, protecting stored data from hacking, theft, and espionage is crucial. Establishing national cybersecurity agencies enables governments to respond effectively to cyber threats and assist both public and private entities in countering cyberattacks.

These agencies play a vital role in raising awareness, enhancing understanding of cyber threats, and mitigating the risks associated with rapid technological advancements. As e-government services continue to expand, ensuring the security of electronic government platforms becomes a priority. This requires developing policies and security standards to protect information and maintain trust in digital services ([Ismail, 2021, p. 74](#)).

6-4. Legislative Regulations

Legal frameworks, particularly in the field of intellectual property protection, are crucial in the fight against cybercrime. Artistic creations such as images, graphics, and animations are protected by law. In this regard, the U.S. Congress has passed the No Electronic Theft Act, which imposes legal penalties on digital piracy and unauthorized use of protected content.

Many Arab and Islamic countries have also taken steps to combat cybercrime. For instance, Egypt's Ministry of Communications and Information Technology is working on legislation that includes strict penalties for individuals or organizations that engage in activities such as document forgery, data breaches, and unauthorized access to electronic information.

Experts have called for an Arab strategy to combat cybercrime, which includes:

- Developing laws and regulations tailored to the internet's unique characteristics.
- Implementing secure electronic payment systems in Arab banks.
- Providing consumer protection guarantees for online transactions.
- Criminalizing hardware and software theft in the IT sector.
- Strengthening coordination among security agencies in Arab countries to unify efforts against cybercrime using advanced technology ([Roux, 2025](#)).

6-5. Awareness and Education

Raising awareness is one of the most effective ways to prevent cybercrime. The "Education for Justice" Initiative, supported by academics worldwide, has developed a series of educational modules specifically focused on cybercrime.

These university-level modules cover various aspects of cybercrime, including theoretical concepts and practical knowledge. Since cybercrime is a multidisciplinary field, these modules focus on different topics and provide reference materials on cybercrime investigations. Additionally, the Cybercrime Teaching Guide within the initiative offers further educational guidance for instructors.

Conclusion:

This study examined "Cybercrime and Its Threats to Cybersecurity," concluding that cybercrime constitutes actions that are illegal from both religious and legal perspectives and socially unacceptable. These crimes occur in cyberspace through the expertise of cybercriminals in handling information and communication technology, utilizing advanced techniques and various applications to inflict harm on information systems and communication networks.

Cybercrime possesses several characteristics: it is difficult to detect, prove, and punish, making enforcement challenging. Additionally, it is appealing to perpetrators and transcends geographical boundaries. While initially targeting individuals, cybercrime has expanded to include attacks on government websites. Its damages are no longer solely financial but also impact cultural, political, economic, and even personal aspects.

This crime thrives under various facilitating factors, such as fascination with information technology, obsession with data collection, the pursuit of financial gains, and the desire to challenge information systems and assert one's capabilities. Given these attributes, cybercrime poses a significant threat to cybersecurity, manifesting in privacy violations, information espionage, hacking, and system breaches.

Addressing these risks necessitates proactive measures, including the development of protective software for information and electronic devices, raising awareness, and revising legal frameworks to effectively combat cybercrime in cyberspace.

Bibliography:

- Abdelaziz, B. (2021). *Crime in the Algerian City: Reality and Confrontation Methods. First Edition.* Constantine. Algeria: Alpha for Documents.
- Ahsan, B. (2011). *The Concise Guide to General Criminal Law.* Algeria: Houma Publishing and Distribution.
- Akram, A. A.-M. (2005). *The Reality and Trends of Crime in the Arab World – An Analytical Study of Theft, Premeditated Murder, and Drug Crimes.* Saudi Arabia, Riyadh: Naif Arab University for Security Sciences.
- Al-Ajmi, A. D. (2014). *Scientific and Legal Issues of Cyber Crimes: A Comparative Study.* Egypt: Middle East University.
- Allouti, L. (2009). Challenges of Cybersecurity in Institutions. *Journal of Economic and Administrative Research, Mohamed Khider University of Biskra*, pp. 160-178.
- Al-Munjid in Contemporary Arabic Language. (2001). *Arabic-Arabic Dictionary.* Beirut, Lebanon: Dar Al-Mashreq.
- Al-Qadi, R. M. (2021). *Combating Cybercrimes.* Egypt: Dar Al-Nahda Al-Arabiya.
- Al-Qatawneh, M. (2010). *Special Criminal Procedures in Cyber Crimes.* Jordan: Law Network.
- Barakat, A.-N. A.-M. (1997). *Geography of Crime: The Cartographic Criminology.* Jordan: Al-Jalawi Library.
- Beas, R. (2016). La lutte contre la cybercriminalité au regard de l'action des États. *Doctorate in Private Law and Criminal Sciences.* Paris: Faculty of Law, Lorraine.
- Brown, C. (2015). Investigation and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology.*
- Cherif, W. (2019). Methods of Cybercrime: The Transition from Traditional Terrorism to Cyberterrorism in the Information Society. *Cultural Dialogue Journal, Abdelhamid Ibn Badis University of Mostaganem*, pp. 54-65.
- Finey, A. (2025, 01 03). *Les différentes formes de cybercriminalité.* Retrieved 03 13, 2025, from cybercriminalite: <http://cybercriminalite-penal.fr>
- Hakima, J. (2021). Implications of Cybercrime on the Digital Environment: A Study on Mechanisms and Strategies for Its Combat. *Annals of the University of Algiers 1*, pp. 649-667.
- Ibn Manzur. (1997). *Lisan Al-Arab.* Egypt: Dar Al-Ma'arif.
- Idris, A. (2019). The Status of Cybersecurity in the Algerian National Security System. *Misdakia Journal, Higher Military School of Media and Communication*, pp. 100-123.
- Ismail, J. (2021). The Role of Cybersecurity in Confronting Electronic Threats: A Case Study of Algeria. *Tahawulat Journal, University of Ouargla*, pp. 65-80.
- Mehdi, R. (2021). Cybercrimes and Their Combating Mechanisms in Algerian Legislation. *Eliza Journal for Research and Studies, University Center of Illizi*, pp. 111-125.
- Nabil, D. (2017). Cybercrime: Between Concepts and Legislative Texts. *Journal of Law and Society, Ahmed Draia University of Adrar*, pp. 20-40.
- Nadia, M. A.-O. (1992). *The Judiciary in Islam and Its Role in Eliminating Crime.* Saudi Arabia, Riyadh: Arab Center for Security Studies and Training.
- Rawdah, Y. (1992). *The Qur'anic Approach to Protecting Society from Crime.* Saudi Arabia, Riyadh: The Arab Center for Security Studies and Training.
- Roux, L. (2025, 01 22). *Cybercrimes: Examples and Measures to Protect Sensitive Projects.* Retrieved 03 13, 2025, from CEO Wimi: CEO Wimi
- Soumia, B. (2021). The Legal Framework for Preventing and Combating Cybercrimes Against Children. *Journal of Legal and Social Sciences*, pp. 286-324.