
Strengthening international cooperation to combat cybercrime

Dr: ABDELHADI ABDELKARIM

Received: 29/03/2025

Accepted: 30/05/2025

publication: 05/06/2025

• **University of Adrar, (Algeria) e-mail. (Abdelkarimdl01@gmail.com)**

Abstract:

Information crime is one of the most widespread topics at the international and regional levels. From this paper, we will attempt to identify the concept of this crime, both by defining its definition and by describing its characteristics from conventional crimes, attempting to showcase international Cooperation against it requires a multifaceted approach that requires updating, legislation and strengthening security and political cooperation, and legal cooperation between states in order to ensure the effectiveness of such cooperation, given the emergence of problems and obstacles that the international community must confront, by adopting an approach consistent with changing technological variables.

Keywords: cybercrime, international cooperation, mechanisms to combat.

Introduction:

In light of rapid technological advancements and the increasing reliance on digital space, cybercrime has emerged as one of the most dangerous threats facing the international community. This phenomenon manifests in various forms, including online fraud, cyber extortion, identity theft, digital espionage, and targeted attacks on critical infrastructure. Consequently, nations are actively seeking to combat these threats and enhance information security at the international level.

The term “cybercrime” has generally sparked debate regarding its definition and the scope of the activities it encompasses. It has become a significant and pressing threat to international security, as it is a complex phenomenon intricately linked to other types of criminal activities, particularly in the context of rapid technological development and its exploitation.

Accordingly, states have united under criminal and security policies aimed at deterring cybercrimes through the conclusion of numerous international agreements, the imposition of criminal penalties, and the strengthening of international cooperation in combating cybercrime. This is achieved through the establishment of legal bodies and institutions dedicated to addressing such crimes, and by adopting both legal and technical mechanisms to track down and extradite cybercriminals, thereby ensuring criminal justice.

This research paper aims to analyze the current state of international cooperation by reviewing the most significant strategies employed to enhance such collaboration and by highlighting the challenges it faces. It also sheds light on international efforts to combat cybercrime and to reinforce global cooperation in addressing these transnational threats.

The importance of studying cybercrime from an international perspective lies in understanding the nature of the threats it poses, which underscores the necessity for unified policies and legislation to effectively counter these crimes.

This raises the central issues of the topic as follows: What measures can be taken to enhance international cooperation in combating cybercrime? What are the various legal challenges that impede this cooperation?

Based on these questions, this study will focus on three main axes:

- **1-The Concept of Cybercrime**
- **2-Forms of International Cooperation in Combating Cybercrime**
- **3- Legal Challenges and Obstacles Facing International Cooperation in Combating Cybercrime.**

1-The Concept of Cybercrime

To shed light on a specific meaning of cybercrime, we have discussed this in two aspects: first, clarifying the definition of cybercrime, and second, reviewing its key characteristics. It can be described as the crime of the modern era, being a recent phenomenon in most respects, as we strive to establish a comprehensive framework for its concept.

1.1- The Definition of Cybercrime:

Opinions regarding the definition of cybercrime have varied, with each perspective adopting its own concept based on its viewpoint. Some approaches define it from a technical angle, others from a legal one, while yet another considers its definition in terms of the means of commission, its subject matter, the perpetrator's knowledge of information technology, or other criteria proposed by different scholars. This divergence led the United Nations, through its documentation on cybercrime, to conclude that a universally agreed definition could not be reached.

It is also observed that there is no consensus among jurists or legislators on the use of a specific term for crimes committed via the Internet, which sometimes even constitutes their target. This leaves room for legislators to keep pace with the continuous advancements in rapidly evolving technologies that have given rise to emerging crimes. Moreover, legislations at various levels have differed in establishing uniform concepts for these offenses. In addition, cybercrime is a transnational offense and is considered one of the evolving crimes that have asserted themselves at both international and national levels, compelling criminal legislators

to address it through criminal laws and impose penalties on its perpetrators¹. Here, by cybercrime and information network offenses, we refer to unauthorized access to private networks of companies, banks, and individuals, as well as tampering with the digital data contained within an information network—such as fabricating, damaging, erasing, disclosing, or possessing tools or passwords to facilitate the commission of such crimes that harm the data and the information itself. Meanwhile, traditional crimes such as money laundering, drug trafficking, terrorism, prostitution, unauthorized use of electronic cards, e-commerce fraud, and defamation employ information technology as a tool in their commission without being cybercrimes in the strict technical sense, although they are sometimes referred to as electronic crimes².

At the Tenth United Nations Congress on Crime Prevention and Criminal Justice, held in Vienna from April 10 to 17, 2000, a comprehensive definition of cybercrime was adopted as “any crime that can be committed by means of a computer system or computer network or within a computer system,” which, in principle, encompasses all crimes that can be committed in an electronic environment³. Professor Mohammed Amin Al-Shawabkeh, for his part, defines cybercrime as any assault on the physical or moral aspects of an automated computing system⁴. On the legislative level, the Saudi legislator defined it through the Anti-Cybercrime Law as “any act committed that involves the use of a computer or an information network in violation of the provisions of this system.” Similarly, the Kuwaiti legislator, through Law No. 63 of 2015, stated in its first article that it is “any act committed through the use of a computer or an information network, or other means of information technology, in violation of the provisions of this law.”

The Algerian legislator defined this type of crime in the first paragraph of Article Two of Law No. 09-04 dated August 5, which contains the specific rules for the prevention of crimes related to media and communication technologies and their combating. It is termed as crimes related to media and communication technologies and defined as “crimes involving interference with the automated data processing systems specified in the Penal Code and any other crime committed or facilitated by means of an information system or an electronic communication system”⁵.

The “information” that forms the basis of cybercrime is understood as stipulated in Article 02, paragraph } of Law 09-04 concerning the prevention of crimes related to media and communication technologies and their combating, which states: “Any process of presenting events, information, or concepts in a form ready for processing within an information system, including programs that enable the information system to perform its function.”

¹ Hamid Asaad Nadawi Al-Jawari, Cybercrime, Bilad Al-Rafidain Journal for Humanities and Social Sciences, Special Issue for the Fourth International Scientific Conference, Maliyat Al-Rafidain University, Diyali University, Iraq, 2023, p. 124.

² Abdul Razzak Talal Jassim, Safaa Hassan Nadeef, The Need to Modernize International Cooperation in the Field of Combating Cybercrime, Tikrit University Law Journal, Volume 5, Issue 1, 2020, pp. 231–232.

³ Mohammed Al-Saeed Zanati, Cybercrime in Light of Algerian Legislation and International Conventions, Eliza Journal for Research and Studies, Issue 02, December 2017, Eliza University Center, Algeria, p. 31

⁴ Ibid.

⁵ Law No. 09–04 dated 05 August 2009, containing the Special Rules for the Prevention of and Combating Crimes Related to Information and Communication Technologies, the Official Gazette of the People’s Democratic Republic of Algeria, Issue No. 47, issued on 16 August 2009.

From the above definitions, we conclude that cybercrime is any illicit act or omission carried out using a computer or any electronic data processing device, regardless of whether the outcome is positive or negative, provided that there is an intent to commit the criminal act. Despite the lack of consensus on its definition and the ambiguity of the term used to denote it, it has acquired the character of an international crime. Some of these offenses are transnational, making them difficult to address due to the significant evolution in their methods, thereby necessitating cooperation to eliminate them and punish their perpetrators.

1.2- Characteristics of Cybercrime:

The interconnection between cybercrime and digital technology has endowed this type of crime with distinctive features that set it apart from traditional crimes, which can be summarized as follows:

1.2.1 Cybercrime is a Transnational Crime:

The fundamental characteristic of cybercrimes is their ability to transcend geographical boundaries due to their association with the Internet and information technology. This enables multiple countries to be affected simultaneously by these crimes owing to their rapid execution. A perpetrator may commit the crime in one country while the victim resides in another within a short time in the digital age⁶, raising questions regarding jurisdiction and the applicable law in prosecuting the offender—namely, whether it is the state where the criminal behavior occurred, the state in which the victim is located, or the state of the offender⁷.

1.2.2 The Magnitude of Losses Compared to Traditional Crimes:

The global company specialized in information protection technologies, "Intel Security," revealed that cyber attacks have evolved into a burgeoning economy in their own right, with an estimated value ranging between 2 to 3 trillion dollars annually—accounting for 15 to 20% of the economic value generated online. Moreover, global business sectors incur annual losses of up to 400 million US dollars, with one British company suffering losses amounting to 1.3 billion dollars from a single cyber attack, and two banks in the Gulf losing 45 billion dollars within a few hours between 2015 and 2017⁸.

1.2.3 The Difficulty in Detecting and Proving Them:

Cybercrime is characterized not only by the challenge of preserving any technical traces, if they exist, but also by its tendency to leave no trace upon commission. No tangible funds are embezzled; rather, it involves numbers that change in records. In addition, most cybercrimes are discovered accidentally and after a considerable delay, and are often not

⁶ Osama Ahmed Al-Manasa, Jalal Mohammed Al-Zughbi, *Electronic Information Systems Technology Crimes*, Dar Al-Thaqafa for Publishing and Distribution, Third Edition, Amman, 2014, p. 93.

⁷ Saeed Naeem, *Mechanisms for Investigating Cybercrime under Algerian Law*, Master's Thesis in International Business Law, Faculty of Law and Political Sciences, Mouloud Maamari University in Tizi Ouzou, 2013, p. 15.

⁸ Bin Shahra Shoul, Mourad Meshoush, *The Specific Characteristics of Cybercrime*, Al-Mustaqbal Journal of Legal and Political Studies, Institute of Economic and Commercial Sciences and Management, Ahmed Zabana University, Ghardaia, Algeria, Volume 4, Issue 1, June 2020, p. 05.

reported—either because the victim fails to detect them or out of fear of reputational damage—resulting in the actual extent of cybercrimes being far greater than reported.

1.2.4 Cybercrimes Are Attractive to Criminals:

Traditional crimes require the use of physical tools and typically involve violence, as seen in drug trafficking, terrorism, and armed robbery. In contrast, cybercrimes are considered non-violent offenses that do not necessitate the use of force. An internet criminal only requires the technical competence to operate a computer for illicit activities, access to a global information network, and the will to achieve an illegal objective, all of which are devoid of violence⁹.

1.2.5 Their Commission Requires the Presence of an Electronic Device and Technical Knowledge for Its Use:

What distinguishes cybercrime from other offenses is that it demands sufficient understanding of technical aspects, such as computer and Internet usage. The relationship between proficiency in the technical aspects of computers and the commission of cybercrime is directly proportional; the greater the expertise individuals have in computer technologies, the higher the likelihood of their skills being misused for illicit purposes.

The solution to this problem lies in the installation of protection software on all computers—whether at home or in workplaces—to ensure the preservation of personal and professional secrets, and to prevent the device connected to the Internet (and its power supply) from being used outside designated times¹⁰.

2- Forms of International Cooperation in Combating Cybercrime:

The fight against cybercrimes has garnered international attention—whether the focus is on cybercrimes per se or on electronic crimes in general—and in both cases, cybercrimes have received the lion's share, as they represent the main gateway to committing electronic offenses overall. In reviewing the efforts made at the international level, one finds that they are primarily defined by international agreements as an initial step, followed by the initiatives adopted by international organizations to develop effective solutions in confronting these crimes.

2.1- International Agreements in the Field of Combating Cybercrime:

2.1.1 The Budapest Convention on Cybercrime and Electronic Communications (2001):

⁹ Ali Fadel Jouaid, The Legal Challenges of Combating Cybercrime in the Digital Age, Iraqi University Journal, Volume 80, Issue 01, 2024, p. 286.

¹⁰ Boudiaf Asmahan, Cybercrime and the Legislative Procedures to Confront It, Professor Researcher Journal for Legal and Political Studies, Issue 11, University of M'sila, Algeria, September 2018, p. 356.

This convention represents the culmination of global efforts to establish a universal legal framework to combat cybercrime. It obliges its members—comprising both European and non-European countries that have signed or acceded to it—to adopt appropriate legislative measures to criminalize nine offenses related to economic technology, intellectual property, and harmful or illegal content. The European Convention on computer or Internet crimes, known as the Budapest Convention and signed on November 23, 2001, is divided into five sections. The first four address four types of offenses:

- **Offenses affecting the confidentiality, security, integrity, and availability of computer data and systems:** These include unauthorized access, unauthorized use, data interference, unauthorized system interference, and misuse of devices.
 - **Computer-related offenses:** Encompassing computer-related forgery and computer-related fraud.
 - **Offenses related to child pornography:** Specifically, the illegal production or distribution of pornographic materials and indecent images of children.
 - **Offenses involving violations of intellectual property and associated rights:** Such as those related to publishing and printing.
- The fifth section is devoted to liability and sanctions, including additional provisions regarding attempt and participation as well as penalties and measures in accordance with modern international conventions concerning the liability of legal entities¹¹. This convention is regarded as one of the most important and diverse agreements for coordinating new laws in numerous countries against the misuse of the Internet. It follows a long period of consultations between governments and the computing sector, with its text drafted by a number of legal experts at the Council of Europe with assistance from other countries¹².

2.1.2 The European Convention on Combating Cybercrime:

The Special Committee on Crime Issues, under the auspices of the Council of Europe, endorsed the final draft of a comprehensive treaty aimed at assisting countries in combating cybercrime amid criticisms from advocates of personal freedom. Once ratified by the Presidency of the Council and signed by the concerned countries, the convention will oblige the signatory states to enact the minimum necessary laws to address high-tech crimes—including unauthorized network access, data manipulation, computer-related fraud and forgery, child pornography, and violations of digital copyright. Notably, the treaty's provisions—amended 27 times before its approval—include clauses that grant governments extensive surveillance powers and require states to assist one another in gathering evidence and enforcing the law. However, these new international powers might compromise the protection of citizens if governments misuse the authorities granted under the convention¹³.

2.1.3 The Berne Convention for the Protection of Literary and Artistic Works:

¹¹ Mohammed Al-Saeed Zanati, Cybercrime in Light of Algerian Legislation and International Conventions, Eliza Journal for Research and Studies, Issue 2, December 2017, Eliza University Center, Algeria, p. 37.

¹² Ibid., same page.

¹³ Saiedani Salami, The Evolution of Legislations and International Conventions in the Field of Cybercrime (Reality and Approaches), Professor Researcher Journal for Legal and Political Studies, Issue 10, Volume 1, 2018, p. 200.

To most effectively safeguard the rights of authors over their literary works, the Berne Convention was concluded on September 9, 1886, supplemented in Paris in 1896, amended in Berlin in 1908, supplemented in Berne on March 20, 1914, expedited in Rome in June 1928, in Brussels in 1948, in Stockholm in July 1967, and in Paris in 1971. Under this convention, the member states form a union for the protection of authors' rights over their literary and artistic works. Moreover, under the Berne Convention, computer programs—whether in source code or machine language—are granted protection as literary works, as stipulated therein. This is complemented by the TRIPS Agreement concerning aspects of international trade, in which nine signatory countries aim to encourage effective and appropriate protection of intellectual property rights in order to reduce barriers to international trade¹⁴.

2.1.4 The Arab Convention on IT Crimes:

Signed in Cairo on December 21, 2010, this convention aims to enhance cooperation among Arab states in combating IT crimes to preempt the dangers posed by these offenses and to safeguard the security, interests, and integrity of Arab countries and their citizens¹⁵.

The convention consists of a preamble and forty-three articles distributed over five chapters. The first chapter contains general provisions (Articles 1–4); the second chapter is devoted to criminalization (Articles 5–21); the third chapter covers procedural provisions (Articles 22–29); while the fourth chapter enshrines legal and judicial cooperation (Articles 30–43).

This convention is also considered one of the most significant agreements concluded in the field of combating information technology crime, aiming to prevent, investigate, and prosecute its perpetrators—including those responsible for attacks on data integrity, misuse of IT resources, forgery, fraud, pornography, violations of privacy, and cyber terrorism-related offenses... etc¹⁶.

2.2-Efforts of International Bodies and Organizations Active in the Field of International Cooperation

International bodies and organizations play a significant and prominent role in advancing international cooperation to confront cybercrimes.

2.2.1United Nations:

The United Nations has made considerable efforts in addressing cybercrimes, emphasizing the need to strengthen joint work among its member states to curb their spread and mitigate their impact. Cybercrimes have attracted the attention of several United Nations conferences, most notably:

¹⁴ Mohammed Al-Saeed Zanati, *Ibid.*, p. 37.

¹⁵ Refer to Article 1 of the Arab Convention on Combating Information Technology Crimes.

¹⁶ Refer to Articles 06 to 11 of the Arab Convention on Combating Information Technology Crimes.

- The Havana Conference of 1990, during which the United Nations urged member states to intensify their efforts to combat computer misuse and called for the establishment of a governmental committee for crime protection, which would serve as the primary United Nations entity in this field¹⁷. This conference also reaffirmed the adoption of policies concerning cybercrime victims in harmony with the United Nations Declaration of Principles of Justice in this context.

- The Tenth Conference on Crime Prevention and Criminal Justice, held in Vienna in 2000, which discussed computer-related crimes.

- The Twelfth Conference on Crime Prevention and Criminal Justice in Brazil, held from April 12 to 19, 2010, during which member states discussed various recent developments employed by both criminals and competent authorities in combating crime, including computer crimes¹⁸.

In addition, the United Nations General Assembly has adopted numerous resolutions and recommendations in this context, such as Resolution (121/45) of 1990; the publication of the Computer-Related Crime Prevention and Combating Guide in 1994; Resolution (63/55) dated December 4, 2000; Resolution (121/56) dated December 19, 2001, regarding the combat against the misuse of the criminal administrative information system for information technology; Resolution (199/58) dated January 30, 2004, concerning the establishment of a global cyber security culture; and a call for member states to cooperate and enhance a culture of cyber security.

2.2.2 International Criminal Police Organization (INTERPOL):

INTERPOL, established in 1923 and headquartered in Lyon, France, is the largest international police organization. Its origins date back to the establishment of the “International Criminal Police Committee,” which aimed to coordinate the national security forces of European countries in combating crime, particularly cybercrime.

This organization is dedicated to affirming and encouraging effective cooperation among the police forces of member states in combating crime—ranging from gathering data and information related to criminals and crimes through national central offices, to exchanging such information, in addition to cooperating in apprehending criminals with the assistance of police forces from member states¹⁹.

Among INTERPOL’s tasks regarding cybercrime are tracking cybercriminals in general and internet-based criminals in particular, tracing and seizing digital evidence, and conducting cross-border inspections of computer components, logical systems, and communication networks in search of evidence and proof of cybercrime. Information is exchanged via a

¹⁷ Mourad Meshoush, International Efforts to Combat Cybercrime, Al-Wahat Journal for Research and Studies, University of Ghardaia, Volume 12, Issue 02, 2019, p. 706.

¹⁸ Saghir Youssef, Mechanisms for Combating Crimes Committed over the Internet, PhD Dissertation in Law, Faculty of Law and Political Sciences, Moulaud Maamari University, Tizi Ouzou, p. 24.

¹⁹ Mohammed Ahmed Suleiman Isa, International Cooperation in Confronting Cybercrimes, The Academic Journal for Legal Research, Faculty of Law and Political Sciences, University of Bejaia, Volume 14, Issue 2, 2016, p. 53.

secure communications platform that operates 24/7 to facilitate investigations into cybercrimes carried out by agencies of the Ministries of Justice and National Security²⁰.

The organization's efforts in this field have progressed through several stages, resulting in the establishment of regional communication centers in Tokyo, New Zealand, Nairobi, Azerbaijan, and Buenos Aires to streamline message exchange, in addition to a regional sub-office in Bangkok.

2.2.3 World Intellectual Property Organization in Combating Cybercrime:

In the astonishing digital age, with its rapid developments, there are no longer boundaries or restrictions preventing the copying of any manuscript or electronic version of a book and other materials without supervision in a virtual world teeming with people, ideas, and opinions. This phenomenon has facilitated cybercrimes that infringe on intellectual property rights in general.

This situation has posed a significant challenge for the World Intellectual Property Organization, as well as for other organizations and entities concerned with protecting intellectual property rights, in finding the best means to safeguard these rights by enacting legal and legislative measures that guarantee their protection²¹.

The key efforts of the World Intellectual Property Organization can be summarized as follows:

-Protection of Software and Its Impact on Developing Countries:

Software is the result of a globally advanced activity characterized by high-value ideas, creativity, and intellect, reflecting the prevailing trend toward strategic progress in defining capital determinants. In this regard, software has been a crucial means throughout the information age with all its manifestations. Therefore, it is vital for developing countries, and the cooperation of the World Intellectual Property Organization with developing and least developed countries is focused on enhancing the intellectual property system, including the TRIPS Agreement. For this purpose, the World Intellectual Property Organization works to achieve the following²²:

- Harnessing the capacities of developing and least developed countries to formulate policies and modernize intellectual property legislation while adhering to international standards and trends, including the TRIPS Agreement.
- Enhancing the enforcement of intellectual property rights in developing and least developed countries.
- Facilitating the dissemination of information related to intellectual property and promoting access to updates of intellectual property legislation texts by preparing electronic

²⁰ Shantir Khadra, *The Legal Mechanisms for Combating Cybercrime (A Comparative Study)*, PhD Dissertation in Criminal Law, Faculty of Law and Political Sciences, Colonel Ahmed Derayea University, Adrar, 2020–2021, p. 210.

²¹ Saghir Youssef, *Ibid.*, p. 26.

²² Mohammed Ahmed Suleiman Isa, *Ibid.*, p. 58.

versions of these legislative texts for inclusion in the World Intellectual Property Organization's online collection of laws.

-The organization has adopted a technical rather than legal standard that is compatible with the technical nature of digital classifications and has given freedom to states' legislation to determine the legal nature of the right to transport, distribute, transmit, and store classifications through networks in conformity with the domestic legislation of the contracting states, insofar as it is not incompatible with the author's legitimate rights and at the same time conforms with the right to trade and transfer classifications²³.

2.3 International Cooperation Means for Combating Cybercrime:

2.3.1 Exchange of Information

Exchange of information includes the provision of data, documents, and evidentiary materials requested by a foreign judicial authority reviewing a particular crime, concerning the charges brought against its nationals abroad and the measures taken against them. This may also encompass the criminal records of the perpetrators²⁴. This is affirmed by Article One of the United Nations Model Treaty on the Exchange of Information in Criminal Matters, and was implemented in Article Eight of the United Nations Convention against Transnational Organized Crime. In contrast, Article 26 of the Budapest Convention emphasizes the duty of a state that possesses significant information to assist another state during investigations or while conducting criminal proceedings when the investigating or prosecuting authority becomes aware of such information.

It also covers matters related to the movements of organized criminals within transnational criminal groups and all information connected with their criminal activities. This is corroborated by the various manifestations of cybercrime, as confirmed by the Schengen Agreement of the European Union through its formulation of an integrated information exchange system²⁵. Moreover, this approach is applied in Articles One and Two of the model guideline for the Legal and Judicial Cooperation Agreement issued by the Gulf Cooperation Council in its fourth session in 2004²⁶.

2.3.2 International Judicial Assistance Exchange

²³ Hassan Jamaia, International protection of copyright and neighboring rights from the Berne Convention and the TRIPS Agreement to the WIPO Copyright Treaty. WIPO Treaty on Copyright and WIPO Treaty on Performances and Phonograms, WIPO National Seminar on Intellectual Property for government officials, organised by the World Intellectual Property Organization (WIPO) for 2114 Bahrain, p. 21 ff.

²⁴ Muntasir Saeed Hammouda, The International Police Organization "INTERPOL", Dar Al-Fikr Al-Jami'i, Volume 1, Alexandria, 2007, p. 11.

²⁵ Naqmoosh Mohamed, Meiloudia Ahmed, Cybercrime: The Imperative of Developing International Cooperation Mechanisms in Combating It, Journal of Legal and Political Studies, Volume 4, Issue 02, 2018, p. 275.

²⁶ Abdul Razzak Talal Jassim, Ibid, p. 243.

International judicial assistance is one of the most important pillars of international judicial cooperation. It refers to a request by a state for a foreign state to undertake public prosecution measures regarding a matter presented before the judicial authority of the requesting state, in circumstances where it is unable to proceed on its own.

This mechanism aims to facilitate criminal proceedings between states by ensuring the necessary investigations are carried out to bring the accused to trial and overcome the obstacle of territorial sovereignty. It involves the transfer of procedures in criminal matters to address the evolving nature of criminal phenomena and to mitigate obstacles hindering the conduct of criminal proceedings in cases with extraterritorial dimensions. Judicial assistance is grounded in national laws, international conventions, and the principle of reciprocity²⁷.

2.3.3 Exchange of Expertise and Technical Assistance

It is evident that there is a disparity in the level of development among countries regarding information technology and communication means, even among developed nations. In contrast, cybercrime is a transnational offense that also exploits the vulnerabilities some states face in the realm of information security. Consequently, combating it can only be achieved through the synergy and exchange of technical expertise among the agencies responsible for its counteraction, as well as through training on the implementation of the relevant treaties²⁸.

In this regard, it is incumbent upon the legislative authority of any state to amend its Criminal Procedure Code to legitimize these measures in a manner consistent with the multifaceted nature of the crime, which necessitates a specialized legal framework²⁹.

2.3.4 Recognition of Foreign Judgments

The non-enforceability of foreign judgments, justified on the grounds of state sovereignty and the right to punishment, is an obstacle that must be overcome to strengthen international cooperation. The issue should not be confined merely to the negative repercussions of a foreign judgment related to the prohibition of double jeopardy, since criminal jurisprudence necessitates recognition of judicial precedents to prevent offenders from evading punishment in accordance with the requirements of justice³⁰.

This measure is critically necessary in combating cybercrime, given its transnational nature and the extensive impact it has on many countries, in order to prevent the perpetrator of such a crime from escaping punishment³¹. Thus, it is essential to overcome the obstacle of the non-enforceability of foreign judgments, at least among states bound by an agreement or treaty that provides for the enforceability of such judgments, or at minimum, based on the principle of reciprocity.

²⁷ Ibid., p. 272.

²⁸, Ibid, p273.

²⁹ Naqmoosh Mohamed, Meiloudia, p. 276.

³⁰ Rabhi Aziza, Informational Secrets and Their Criminal Protection, Doctoral Dissertation in Private Law, Faculty of Law and Political Sciences, Aboubakr Belkaid University, Tlemcen, 2017–2018, p. 314.

³¹ Saghir Youssef, Ibid., p. 63.

2.3.5 Transfer of Proceedings

This refers to a situation where a state, based on an agreement or treaty, undertakes criminal proceedings for an offense committed in the territory of another state and for the benefit of that state, provided that certain conditions are met—most notably, the principle of double criminalization and the legitimacy of the measures to be taken, ensuring that such measures are crucial to uncovering the truth³².

This mechanism has been endorsed by numerous international and regional conventions, and is considered one form of judicial assistance³³, subject to certain conditions³⁴:

- The act attributed to the person must constitute a crime in both the requesting state and the requested state.
- The measures to be taken must be prescribed by the law of the requested state regarding the same offense.

The measures taken must be capable of uncovering the truth.

3- Obstacles Facing International Cooperation in Combating Cybercrime:

Despite the importance of international cooperation in confronting cybercrime, the current reality faces several challenges that hinder the achievement of the desired cooperation. We will attempt, albeit partially, to highlight the most significant of these obstacles—some of which are of an objective nature, while others pertain to the procedural difficulties in implementing international cooperation in this context.

3.1- Obstacles to International Cooperation of an Objective Nature :

3.1.1 Inadequacy and Inappropriateness of Domestic Criminal Legislation

National penal systems do not evolve at the same pace as cybercrime. Consequently, many provisions of domestic criminal laws in certain countries are insufficient in their current form to address these newly emerging types of crimes, as most legal texts require a physical element in the commission of the offense—a requirement that is incompatible with the nature of information-based crimes. As a result, these manifestations evade criminalization and punishment. Despite the issuance of cybercrime-related legislation by numerous countries and their accession to various international conventions that criminalize acts in violation of treaties regulating such offenses, these legal texts remain inadequate for addressing all crimes committed in the computer and internet sphere, thereby diminishing the efforts of law enforcement in apprehending criminals and uncovering offenses³⁵.

3.1.2 Lack of a Unified System for Criminal Activity

³² Abdul Razzak Talal Jassim, Ibid., p. 244.

³³ Mohammed Ahmed Suleiman Isa, Ibid., p. 130.

³⁴ Ibid., p. 59.

³⁵ Hashifa Abdulhadi, Ibid., p. 48.

The legal systems established to combat cybercrimes differ in their characterization of the criminal acts involved, due to variations in customs, traditions, religions, cultures, and other societal factors. This has led to discrepancies in legislative, particularly criminal, policies; certain types of cybercrime may be permissible under one legal system while being criminalized under another³⁶. Furthermore, the absence of consensus among different legal systems on unified definitions of criminal behavior in internet-related crimes tempts computer hackers to organize and commit their offenses without regard to geographical boundaries, thereby underscoring the necessity of international cooperation in combating this crime³⁷.

3.1.3 Double Criminalization of Criminal Behavior

Double criminalization is a critical condition for the extradition of criminals, which may impede international cooperation in surrendering individuals involved in cybercrimes—especially as many countries still lack legal provisions to address this criminal phenomenon. The collective interest of nations requires the exploration of methods to overcome these challenges and establish genuine international cooperation that aligns with the characteristics of this new type of crime, ensuring the harmonization of domestic criminal legal systems³⁸. Recognizing the importance of international cooperation as essential for addressing issues posed by cybercrimes, many countries have resorted to concluding bilateral agreements to simplify the investigation of these crimes.

3.1.4 Deficiencies of International Treaties

The shortcomings of bilateral and multilateral treaties among states represent one of the most significant challenges in achieving the necessary protection against crimes committed over the internet, particularly given the rapid advancements in computer systems, software, and internet networks that have rendered international cooperation in this field ineffective³⁹. Furthermore, these deficiencies stem from divergent perspectives among nations; each state maintains its own view regarding the necessary protection of its information infrastructure, due in part to a steadfast commitment to the concept of state sovereignty over its territory on one hand, and concerns about compromising its fundamental interests if it becomes open to the international community on the other⁴⁰.

3.2- Obstacles to International Cooperation of a Procedural Nature :

3.2.1 Obstacles Related to International Judicial Assistance

These difficulties manifest as delays in responses, since the recipient state of the request is often slow to reply—whether due to a shortage of trained personnel, language barriers, procedural discrepancies that complicate the response, or other reasons⁴¹. It is also noteworthy that the concept of public order differs from one country to another, and the fundamental

³⁶ Shantir Khadra, *Ibid.*, p. 216.

³⁷ Saghir Youssef, *Ibid.*, p. 195.

³⁸ Ali Fadel Jouaid, *Ibid.*, p. 280.

³⁹ Saghir Youssef, *Ibid.*, p. 193.

⁴⁰ *Ibid.*, same page.

⁴¹ Mohammed Ahmed Suleiman Isa, *Ibid.*, p. 62.

interests of a state—as noted by the European Committee on Criminal Issues in its 1990 report—are neither well known nor clearly defined within international law. This ambiguity has allowed states to exploit these legal gaps to refuse judicial assistance whenever the opportunity arises⁴².

3.2.2 The Issue of Jurisdiction in Cybercrimes

Criminal law jurisdiction is often governed by one of the following four principles: territoriality, personal jurisdiction, objective, or universality. These principles vary in importance and are arranged in a hierarchical order. Most criminal laws adopt the principle of territoriality as the primary basis, subsequently reinforced by other principles. However, the issue of jurisdiction becomes complex at the international level due to differences in legislation and legal systems, which can lead to conflicts of jurisdiction between states regarding internet-related crimes that are inherently transnational. For instance, if a crime is committed in the territory of a particular state by a foreigner, the offense may fall under the criminal jurisdiction of that state based on territoriality, while also being subject to the jurisdiction of another state on the basis of personal jurisdiction. Moreover, if the crime threatens the security and stability of another state, it may invoke that state's jurisdiction under the objective principle. Jurisdictional conflicts may also arise when jurisdiction is based on territoriality—for example, if a perpetrator broadcasts obscene, pornographic images from the territory of one state that are accessed in another. In such cases, jurisdiction is established for each state affected by the crime according to the principle of territoriality⁴³.

3.2.3 Absence of Communication Channels

One of the primary objectives of international cooperation is to obtain information and data related to cybercrime and cybercriminals. To achieve this, it is imperative to have a communication system that enables investigative authorities to contact other entities—particularly foreign ones—to facilitate the collection of critical evidence and information pertaining to the committed crime. The absence of such a system means an inability to gather the electronic evidence and information that would assist in combating cybercrime and cybercriminals⁴⁴.

3.2.4 Diversity and Differences in Procedural Legal Systems

Due to the diversity and differences in procedural legal systems, the investigative, inquiry, and trial methods that prove effective and efficient in one country may be ineffective in another, or may not even be permitted—such as electronic surveillance, monitored surrender, covert operations, and other similar measures⁴⁵. Consequently, these procedures may become ineffective, resulting in significant human effort and financial costs for the

⁴² Fakiri Amal, Issues of Evidence and Jurisdiction in Transnational Information and Communication Technology Crimes, Journal of Legal and Political Sciences, University of Oued Souf, Issue 17, January 2018, p. 645.

⁴³ Mohammed Ahmed Suleiman Isa, Ibid., p. 61.

⁴⁴ Shantir Khadra, Ibid., p. 217.

⁴⁵ Saghir Youssef, Ibid., p. 196.

implementing state, ultimately giving the cybercriminal an opportunity to evade punishment if these measures fail to be accepted by the judiciary⁴⁶.

Moreover, the inability of officials in affected institutions to recognize the seriousness of cybercrimes represents a major obstacle to investigations, compounded by the reluctance to report such crimes—an essential and critical component of reporting cybercrimes—as individuals often refrain from notifying the competent authorities about crimes committed against them, particularly when it involves financial institutions or similar entities⁴⁷.

Conclusion :

Cybercrime is an increasingly global challenge that requires the adoption of effective strategies to confront this transnational phenomenon, thereby necessitating enhanced international cooperation among states to combat it. Despite discrepancies in laws and regulations between countries, governmental coordination is essential to address this shared challenge. International agreements, such as the Budapest Convention on Cybercrime, constitute one of the most important mechanisms enabling states to cooperate in pursuing criminals across borders. Moreover, cooperation within international organizations and bodies such as the United Nations and INTERPOL contributes to strengthening security investigations and information exchange in combating cybercrimes at both international and national levels. The most significant findings of this research study are as follows:

- The absence of a clear policy for international cooperation and coordination among states in confronting cybercrime, despite the rapid escalation and evolution of its dangers to the international community, along with the exchange of expertise and various modern technologies by the perpetrators of these crimes.
- The enhancement of international cooperation mechanisms to combat cybercrime faces several challenges due to the novelty of this type of crime, which requires concerted international efforts and legal amendments tailored to its unique nature.
- Numerous challenges remain that must be addressed to fully realize international cooperation, primarily those related to the principle of sovereignty and its associated legal and procedural issues, such as the enforcement of foreign judgments, judicial assistance procedures, and others.
- The lack of a unified model for criminal activity, given that existing legal systems for combating cybercrime in many countries do not share a common consensus on the patterns of misuse of information systems and the internet that should be criminalized.
- The dilemma is further manifested in international legal cooperation, where states have not reached an agreement on a convention to confront cybercrime, nor on a specialized treaty on electronic crime, with divergent political interests and ideological orientations undoubtedly playing a significant role in hindering the efforts of international organizations to establish a comprehensive legal framework for combating cybercrime.

Based on the discussions presented in this paper, we conclude with a set of recommendations, the most important of which are:

⁴⁶ Shantir Khadra, *Ibid.*, p. 216.

⁴⁷ Ali Fadel Jouaid, *Ibid.*, p. 279.

- Update international laws and regulations to align with rapid technological developments and activate the exchange of security information to track cybercriminals.
- Increase coordination and international judicial and procedural cooperation in the field of combating cybercrime.
- It is insufficient to merely update legislative texts in line with comparative legislations without providing practical implementation mechanisms, such as enhancing the training of judicial enforcement teams, establishing specialized judges for this type of crime, and supplying all necessary material and technical resources for their performance.
- Strengthen the role of international and regional police organizations in combating cybercrime by enabling them to utilize the latest electronic technologies and software within their operational framework, and by providing a legal basis for their criminal procedures, including ensuring the protection of their personnel from all forms of electronic extortion.
- Establish joint international platforms to enhance the exchange of expertise and develop more integrated preventive strategies, thereby contributing to the creation of a secure and sustainable digital environment for all.

Sources and references:

1- Textes législatifs et réglementaires :

1. Law No. 09–04 dated 05 August 2009, containing the Special Rules for the Prevention of and Combating Crimes Related to Information and Communication Technologies, the Official Gazette of the People’s Democratic Republic of Algeria, Issue No. 47, issued on 16 August 2009.

2– Book:

1. Muntasir Saeed Hammouda, The International Police Organization “INTERPOL”, Dar Al-Fikr Al-Jami‘i, Volume 1, Alexandria, 2007.

2. Osama Ahmed Al-Manasa, Jalal Mohammed Al-Zughbi, Electronic Information Systems Technology Crimes, Dar Al-Thaqafa for Publishing and Distribution, Third Edition, Amman, 2014.

Article:

3. Abdul Razzak Talal Jassim, Safaa Hassan Nadeef, The Need to Modernize International Cooperation in the Field of Combating Cybercrime, Tikrit University Law Journal, Volume 5, Issue 1, 2020.

4. Abdul Razzak Talal Jassim, The Need to Modernize International Cooperation Mechanisms in the Field of Combating Cybercrime, Tikrit University Law Journal, Volume 5, Issue 1, 2020.

5. Ali Fadel Jouaid, The Legal Challenges of Combating Cybercrime in the Digital Age, Iraqi University Journal, Volume 80, Issue 01, 2024.

6. Ben Shahra Shoul, Mourad Meshoush, The Specific Characteristics of Cybercrime, Al-Mustaqbal Journal of Legal and Political Studies, Institute of Economic and Commercial Sciences and Management, Ahmed Zabana University, Relizane, Algeria, Volume 4, Issue 1, June 2020.

7. Boudiaf Asmahan, Cybercrime and the Legislative Procedures to Confront It, Professor Researcher Journal for Legal and Political Studies, Issue 11, University of M'sila, Algeria, September 2018, .
8. Fakiri Amal, Issues of Evidence and Jurisdiction in Transnational Information and Communication Technology Crimes, Journal of Legal and Political Sciences, University of Oued Souf, Issue 17, January 2018:
9. Hamid Asaad Nadawi Al-Jawari, Cybercrime, Bilad Al-Rafidain Journal for Humanities and Social Sciences, Special Issue for the Fourth International Scientific Conference, Maliyat Al-Rafidain University, Diyali University, Iraq.
10. Law No. 09–04 dated 05 August 2009, containing the Special Rules for the Prevention of and Combating Crimes Related to Information and Communication Technologies, the Official Gazette of the People's Democratic Republic of Algeria, Issue No. 47, issued on 16 August 2009.
11. Mohammed Ahmed Suleiman Isa, International Cooperation in Confronting Cybercrimes, The Academic Journal for Legal Research, Faculty of Law and Political Sciences, University of Bejaia, Volume 14, Issue 2.
12. Mohammed Al-Saeed Zanati, Cybercrime in Light of Algerian Legislation and International Conventions, Eliza Journal for Research and Studies, Issue 2, December 2017, Eliza University Center, Algeria.
13. Mourad Meshoush, International Efforts to Combat Cybercrime, Al-Wahat Journal for Research and Studies, University of Ghardaia, Volume 12, Issue 02, 2019.
14. Naqmoosh Mohamed, Meiloudia Ahmed, Cybercrime: The Imperative of Developing International Cooperation Mechanisms in Combating It, Journal of Legal and Political Studies, Volume 4, Issue 02, 2018.
15. Saiedani Salami, The Evolution of Legislations and International Conventions in the Field of Cybercrime (Reality and Approaches), Professor Researcher Journal for Legal and Political Studies, Issue 10, Volume 1, 2018.

3–Thesis and dissertation:

1. Rabhi Aziza, Informational Secrets and Their Criminal Protection, Doctoral Dissertation in Private Law, Faculty of Law and Political Sciences, Aboubakr Belkaid University, Tlemcen, 2017–2018, p. 314.
2. Saeed Naeem, Mechanisms for Investigating Cybercrime under Algerian Law, Master's Thesis in International Business Law, Faculty of Law and Political Sciences, Moulaud Maamari University in Tizi Ouzou, 2013, p. 15.
3. Saghir Youssef, Mechanisms for Combating Crimes Committed over the Internet, PhD Dissertation in Law, Faculty of Law and Political Sciences, Moulaud Maamari University, Tizi Ouzou.
4. Shantir Khadra, The Legal Mechanisms for Combating Cybercrime (A Comparative Study), PhD Dissertation in Criminal Law, Faculty of Law and Political Sciences, Colonel Ahmed Derayea University, Adrar, 2020–2021.