INTERNATIONAL PROCEDURAL OBSTACLES IN COMBATING CYBERCRIME

ABDELKADER CHATRI

PhD student, Institute of Law and Political Science, University Centre of Maghnia, Mediterranean laboratory for legal studies, (Algeria).

E-mail : a.chatri@cu-maghnia.dz

Received: 20/09/2024 **Accepted: 15/12/2024** **Published: 25/02/2025**

Abstract: *Cybercrime is regarded as one of the most important crimes affecting the international community due to its cross-border nature, facilitated by technological advancements and the rapid, widespread use of the internet. As a result, individual states have become unable to fight it effectively on their own, even when possessing sufficient material and human resources. This has necessitated integration into an international framework, reflected in the adoption of several regional and international agreements. However, the effective implementation of these agreements faces several international procedural challenges, most notably jurisdictional conflicts and difficulties in executing letters rogatory, including judicial requests and extradition procedures.*

Keywords: *Cybercrime, International Agreements, International Letters Rogatory, Extradition.*

INTRODUCTION:

Cybercrime is an emerging phenomenon linked to technological advancements and the widespread use of the internet, which has significantly expanded its scope. It is no longer confined to a single country but now poses a threat to the interests of multiple nations simultaneously. This type of crime is characterized by its international reach, emphasizing the need for coordinated global efforts through treaties to address it. No single state, regardless of how advanced its legal framework, security systems, or judiciary may be, can effectively combat this issue in isolation. Integration into various regional and international agreements is crucial for developing a unified policy to combat cybercrime. An example of such efforts is the Convention of Budapest on cybercrime. However, despite ongoing international initiatives, the practical implementation of this cooperation faces several procedural obstacles. These challenges include conflicts of international jurisdiction and the ineffective execution of international letters rogatory, particularly regarding cross-border requests and extradition procedures. the significance of this topic lies in recognizing international cybercrime as a growing threat to numerous countries, despite ongoing efforts at international coordination through various treaties and agreements. This study specifically focuses on identifying the procedural issues that impede effective cooperation between nations in combating this crime. As a result, the following problem statement arises: **What procedural difficulties obstruct the realization of international coordination in combating cybercrime?**

1. International Cooperation in Fighting Cybercrime:

Cybercrime poses a threat at both the local and international levels due to its unique nature. Therefore, it is necessary to define it, emphasize its key features, and explain the concept of international cooperation in combating cybercrime, along with the primary reasons that have led countries to embrace such measures.

1.1. Definition of Cybercrime and its Key Features:

Cybercrime is among the most serious threats to the stability of nations, which explains the substantial focus it has received from various legal frameworks. As such, it is essential to define its concept and outline the key features that **distinguish it.**

1.1.1. Cybercrime Definition:

There has been no consensus on a unified definition of cybercrime. The United Nations Conference on the Prevention of Crime and the Punishment of Offenders, held in Vienna in 2000, defined it as: "Any crime that can be committed through a computer system, a computer network, or within a computer system, and this crime includes, in principle, all crimes committed in an electronic environment.[1]" The Arab Convention on Fighting Cybercrime did not provide a definition but focused on defining information technology[2]. As for Algerian legislation, this crime is addressed in Article 02, Paragraph "A," of Law 09/04 regarding the special rules for preventing and fighting crimes associated with information and communication technologies. It is defined as: "Crimes that harm automated data processing systems as specified in the Penal Code, and any crime committed or facilitated through an information system or communication network[3]." Hence, cybercrime refers to any illegal act that involves electronic means to assault interests protected by criminal law, including violation to information or electronic data**, etc.** This constitutes the description of cybercrime.

1.1.2. Key Features of Cybercrime:

Cybercrime is regarded as a newly emerging crime, distinct in several ways from traditional crimes. It has unique features, the most notable of which are:

First: The Difficulty of Legislative Adaptation to This Crime

These crimes are constantly evolving, creating obstacles in their legislative adaptation, especially in establishing applicable legal frameworks. Each time a new technique or method emerges that facilitates hacking and cybercrime, it introduces a new criminal model. Most legislative authorities rely on traditional legal texts in their criminalization policies, which have become inadequate and insufficient in addressing this type of crime. Consequently, judicial authorities sometimes find themselves unable to effectively deter suspects in cases associated with information technology crimes, in adherence to the principle of legality[4].

Second: International Reach of Cybercrime

The information network, being an open virtual world that transcends both time and space, does not recognize geographical borders. Data can be transferred between computers in different countries, making this one of the key features that give cybercrime its international dimension. A criminal act may occur in one country, but its consequences can be felt in another country or even various countries.

Third: Difficulty in Detecting and Proving Cybercrimes

Despite ongoing efforts to develop several mechanisms to detect cybercrime, including electronic

[1] Ahmed Khalifa Al-Malt, *Cybercrimes*, Dar Al-Fikr Al-Arabi, Egypt, 2005, p. 96.

[2] Article 02 of the Arab Convention on Combating Information Technology Offenses, held at the headquarters of the General Secretariat of the League of Arab States in Cairo on 21/12/2010, ratified by Presidential Decree No. 14/252 on 08/09/2014, published in the Official Gazette No. 57, 2014, states : "Information technology refers to any physical or intangible means, or a set of interconnected or non-interconnected means, used to store, arrange, organize, retrieve, process, develop, and exchange information according to the commands and data stored within it. This includes all related inputs and outputs, whether connected by wired or wireless systems, in a system or network."

[3] Law No. 09/04 dated 05/08/2009, establishing special rules for the prevention and combating of crimes related to information and communication technologies, Official Gazette, Issue No. 47, 2009.

[4] Titouche Radia, Territoriality of Criminal Law and Cybercrime, Revue Cahiers du Politique et de Droit January 2019, p. 32.

surveillance[5] and digital searches as stipulated by international treaties and agreements concerning investigative procedures, discovering and obtaining physical evidence remains challenging due to the nature of these crimes. This necessitates in-depth knowledge and full familiarity with modern technology, particularly since cybercriminals can erase data quickly.

Fourth: Cybercrimes are Based on Intelligence and Expertise

Intelligence is one of the key traits of a cybercriminal, who is assumed to be well-versed in information technology and capable of altering and modifying computer programs[6].

Furthermore, the criminal may be highly skilled in utilizing computers and modern technology, reflecting his of professionalism in committing these crimes.

1.2. Concept of International Cooperation in Fighting Cybercrime and Its Justifications:

The impact of cybercrime is no longer confined to the territory of a single country; it extends to other regions. Therefore, international cooperation is essential to provide the necessary protection and facilitate investigation procedures aimed at apprehending criminals. This has led to many agreements emphasizing the need for cooperation between countries in applying international principles of criminal law. These agreements, which rely on similar or comparable national legislation, aim to extend the scope of cooperation as much as possible for purposes such as investigation, research, and more[7]. Thus, what is meant by international cooperation in this field, and what are its main justifications?

1.2.1. Concept of International Cooperation in Combating Cybercrime Addressing cybercrime requires the convergence and integration of policies from both regional and international states to fight it effectively. This necessitates the international community working together to achieve its goals of eradicating cross-border crimes. There is broad agreement on the general concept of international cooperation, which includes the exchange of assistance and support between countries to fulfill shared public benefits[8]. International cooperation is defined as: "What a state offers to another state in terms of assistance and support to pursue criminals with the aim of punishing them for their crimes, through preventive measures to address the non-national nature of the crime, and to gather evidence in various ways. This process takes time and requires resources that a single state's legal authorities do not possess unless supported and assisted by the efforts of other legal authorities[9]."

From the above, it is evident that international cooperation embodies the collective efforts of states, providing assistance in the security and judicial domains to fulfill common interests in addressing the several forms of cybercrime threats.

---

[5] Both the procedural measures of electronic surveillance and electronic inspection are stipulated by the Algerian legislator in Article 04, paragraph "b," and Article 05 of Law No. 09/04, which establishes special rules for the prevention and combating of crimes related to information and communication technologies.

[6] Farid Nachef, *Mechanisms of International Cooperation in Combating Cybercrimes*, Journal of Research in Law and Political Sciences, Ibn Khaldoun University of Tiaret, Vol. 08, No. 01, 2022, p. 434.

[7] See Article 23 of the Budapest Convention on Cybercrime, 23/11/2001, on the website https://rm.coe.int/budapest-convention-in-arabic/1680739173, accessed on 06/01/2024, which states: "The scope of cooperation should be expanded to cover all crimes related to computer systems and data, that is, the crimes covered under paragraph 2 of Article 14, items 'a' and 'b', as well as the collection of electronic evidence for a criminal offense... etc."

[8] Adel Yahya, *Criminal Policies in the Face of Cybercrime*, Dar Al-Nahda Al-Arabia, Cairo, 1st edition, 2014, p. 92.

[9] Soraya Bourbaba, *International Cooperation in Combating Cybercrime*, Journal of International Law Studies, Faculty of Law and Political Science, Tahri Mohamed University, Bechar, Algeria, Issue 01, published on 20/07/2019, p. 94.

1.2.2. Justifications for International Cooperation in Combating Cybercrime: International cooperation in fighting cybercrime emphasizes that no single country can confront this issue alone, even with substantial human and material resources. Since this type of crime threatens all countries simultaneously, several justifications arise for why nations must pool their efforts to combat it. One of the most important reasons is the geographical spread of the crime, which impacts multiple countries at the same time. This, in itself, justifies the establishment of cooperative bodies focused on coordination and monitoring, alongside the adoption of international measures aimed at uncovering these crimes. These measures work to close off avenues for criminals, ensuring they cannot evade criminal accountability. Furthermore, combating this crime cannot be accomplished by a single country, regardless of how advanced its legislative framework or detection resources may be. There is always a need for international cooperation, particularly in light of the rise of organized crimes such as terrorism, which uses advanced electronic means. Even regional efforts are no longer sufficient to tackle this issue, necessitating international policies and coordination among various security agencies. Another significant justification for cooperation is the pursuit of aligning criminal laws across countries, contributing to the development of international criminal law.

2.Key International Agreements for Fighting Cybercrime and the Procedural Obstacles Preventing Their Implementation:

The international community has not remained passive in the face of the growing and expanding scope of cybercrime, which has become a significant threat due to its connection to various organized crimes, affecting multiple countries simultaneously. Consequently, efforts have been made to lay the groundwork for security and judicial cooperation through the signing of several agreements, including the Budapest Convention, the Arab Convention on Fighting Information Technology Crimes, and the Convention of United Nations against Transnational Organized Crime. Despite the intensified international efforts embodied in these agreements, they continue to face various obstacles.

2-1. Key International Agreements for Fighting Cybercrime:

Cybercrime is no longer confined to a single geographic area; it extends beyond the borders of individual countries. Despite the resources available to individual nations, international assistance is essential. Consequently, numerous agreements have been signed in this domain.

2-1-1- The Budapest Convention on Cybercrime:

This convention is one of the most significant agreements that established a legislative framework (both substantive and procedural) to fight several forms of cybercrime. It was drafted on November 8, 2001, ratified on November 23, 2001, and entered into force in 2004. This convention seeks to define cybercrimes and their perpetrators, as well as assist in identifying and apprehending them. The primary goal of the convention is to coordinate, or at least unify, the efforts of countries to reduce the commission of these crimes that negatively affect economic progress. It also works to establish the best methods for investigating internet-related crimes, with signatory countries committing to close cooperation in fighting them[10].

One of the key aspects of this convention is its coverage of crimes related to information security and confidentiality, computer crimes, fraud and counterfeiting associated with content, as well as child pornography. It also addresses intellectual property crimes. Additionally, the convention covers international cooperation regarding principles related to the extradition of criminals, the provision of mutual assistance, etc.

[10] Abdelhakim Rachid Touba, *Information Technology Crimes*, Dar Al-Mustaqbal for Publishing and Distribution, Amman, Jordan, 1st edition, 2008, p. 228.

2-1-2- The Arab Convention on Fighting Cybercrimes:

Prior efforts at the Arab level to fight cybercrime were driven by the ongoing threats posed by this type of crime. The Arab Model Law on Fighting Cybercrime was issued as a result of collaborative efforts between the Council of Arab Interior Ministers and the Council of Arab Ministers of Justice, following the submission of their respective drafts regarding cybercrime to the Secretariat of the Arab League[11]. In this regard, the Arab League worked to foster relationships among member states, leading to the signing of the convention at the headquarters of the Arab League General Secretariat in Cairo, Egypt, on December 21, 2010[12]. This convention seeks to promote Arab cooperation in combating information technology crimes, to prevent their dangers, and to maintain security. This convention addresses several forms of cybercrime, encompassing illegal interception, misuse of information technology, forgery, fraud, and more. It also outlines key investigative procedures, such as the search and seizure of stored information and the interception of content-related information. With regard to legal and judicial cooperation, the convention deals with issues associated with jurisdiction.

The extradition of criminals[13], and mutual assistance. It necessitates all parties to exchange assistance in facilitating investigations, inquiries, and the collection of evidence.

2-1-3 The Conference of the Parties to the Convention of United Nations Against Transnational Organized Crime:

A report was prepared following the meeting of the working group on international cooperation, which was held in Vienna on October 27 and 28, 2015. This meeting followed a decision from the Conference of the Parties to the Convention of United Nations Against Transnational Organized Crime, which called for the establishment of an open-ended working group to discuss practical issues associated with the extradition of wanted individuals, mutual legal assistance, and international cooperation for confiscation purposes.

The main recommendations from this working group included the development of training materials on the collection and exchange of electronic evidence, which should be distributed alongside existing international criminal cooperation tools. Furthermore, the report emphasized promoting the capacity of member states' cooperation mechanisms in law enforcement by implementing measures such as establishing effective systems for exchanging information and creating communication channels between competent authorities. The possibility of creating a global network through a virtual platform to facilitate and foster direct communication between central authorities was also proposed. Moreover, the development of international cooperation tools in criminal matters was recommended, including the finalization of a standard procedure for drafting mutual legal assistance requests to promote efficiency. This would involve the use of liaison officers and specialized exchange mechanisms for law enforcement agencies[14].

---

[11] Badri Faycel, *Combating Information Crime in International and Domestic Law*, PhD thesis in Public Law, Faculty of Law, Benyoucef-Benkhedda University, Algeria, 2017/2018, pp. 32-33.

[12] The Arab Convention on Combating Cybercrime, held at the General Secretariat of the Arab League in Cairo on December 21, 2010, was agreed to enter into force on February 6, 2014, after 30 days from the deposit of the ratification or acceptance documents.

[13] Article 31, paragraph "A", of the Arab Convention on Combating Cybercrime, held at the General Secretariat of the Arab League in Cairo on December 21, 2010, states: "This article applies to the extradition of criminals between the contracting states for the crimes outlined in Chapter Two of this convention, provided that such crimes are punishable under the laws of the concerned states with imprisonment for at least one year and more severe penalties... etc."

[14] Report of the meeting of the working group on international cooperation, held in Vienna, Austria, on October 27-28, 2015. This group was established by the Conference of the Parties to the United Nations Convention against Transnational Organized Crime, and Algeria was represented by its delegates, with the report being adopted by the working group on October 28, 2015.

2-2- International Procedural Issues in Combating Cybercrime:

The mere existence of criminalization and punishment provisions is not sufficient to fight cybercrime effectively. Countries have aimed to establish procedural frameworks through which cooperation mechanisms can be achieved. However, various issues arise that impede the international coordination process in some cases. Among the most significant of these are conflicts of international jurisdiction. Obstacles may also emerge concerning international legal assistance requests, which can be delayed for long periods. Moreover, issues surrounding the extradition of criminals from one country to another continue to obstruct international cooperation.

2-2-1- Conflict of International Judicial Jurisdiction:

One of the key features of cybercrime is its transnational nature—it can be committed by one or various perpetrators across different countries, either simultaneously or at different times. This type of crime poses considerable challenges concerning international jurisdiction, which grants courts in each state the authority to adjudicate specific cases. This can result in either positive jurisdictional conflicts (when multiple states claim jurisdiction) or negative conflicts (when all states decline jurisdiction). When a cybercrime is committed within a state's territory, it falls under that state's criminal jurisdiction based on the principle of territoriality. The same crime may also fall under the jurisdiction of the perpetrator's home state under the principle of personal jurisdiction. Furthermore, if the crime threatens the security and safety of another state, that state may assert jurisdiction based on the protective principle[15]. Notably, the Algerian legislator has granted Algerian courts the authority to adjudicate such crimes, even if they are committed outside the country by a foreign national, provided they target state institutions, national defense, or the strategic interests of the national economy[16].

2-2-2 Issues of International Letters Rogatory:

The process of seeking evidence to prove a crime is not confined to the country where the crime occurred. Given the nature of cybercrime, which often extends across various countries, assistance from other states—some of which may also be involved in the crime—is required. This is referred to as judicial cooperation between different countries. Judicial assistance involves a state conducting a legal procedure associated with a case within the territorial borders of another country, at the request of that country[17].

This international judicial cooperation, especially in the form of letters rogatory, frequently faces significant obstacles. The most notable challenge is the issue of sovereignty, enshrined in most national constitutions, which grants a state authority over its entire territory, particularly in matters involving public order. This principle is also adopted by the Algerian legislator[18], where the state assumes responsibility for investigating, prosecuting, and adjudicating all crimes committed within its territory. Moreover, letters rogatory often face delays, as responses from the requested state tend to be slow, and the process itself is frequently complex. In practice, national letters rogatory already take considerable time, and international letters rogatory exacerbate the issue, particularly given the fast-paced nature of cybercrime investigations. Swift action is essential in

---

[15] Jamil Abdel Baki, "Procedural Aspects of Internet-Related Crimes," Dar Al-Nahda Al-Arabiya, Cairo, 2001, p. 73.

[16] See Article 15 of Law 09/04 related to the prevention of crimes connected to information and communication technologies.

[17] Taher Yaker, "Combating Cybercrime between National Legislation and International Conventions," *Al-Sada Journal for Legal and Political Studies*, Djilali Bounaama University, Khemis Miliana, Algeria, Volume 04, Issue 04, issued on 30/12/2022, p. 19.

[18] Article 18 of Law 09/04 related to the prevention of crimes connected to information and communication technologies states: "Requests for assistance shall be refused if they are likely to affect national sovereignty or public order."

such cases to prevent the destruction of evidence, presenting a significant challenge for the country conducting the investigation. Algerian legislator acknowledges the need for expedient action in international assistance for investigations or legal proceedings, as outlined in Law 09/04 on preventing crimes associated with information and communication technologies, specifically in Article 16, Paragraph 2: "In urgent cases, and in compliance with international agreements and the principle of reciprocity, judicial assistance requests referred to in the previous paragraph may be accepted if sent via fast communication methods, including fax or email, provided these methods ensure adequate security upon verification of their authenticity." Furthermore, the Arab Convention on Fighting Cybercrime emphasizes the significance of maximizing assistance in the exchange of information between countries to gather electronic evidence[19].

Efforts to fight cybercrime require enhanced cooperation in international letters rogatory to establish and unify communication channels between countries, allowing investigative authorities to communicate with foreign entities to facilitate the process of collecting evidence and critical information. The absence of such a system hinders the collection of electronic evidence and supporting information necessary for effectively combating cybercrime and bringing perpetrators to justice[20].

2-2-3 Challenges Related to Extraditing Wanted Criminals:

Extradition is a significant mechanism for promoting international cooperation in fighting cross-border crimes. It operates on the principle that the state in which an individual accused of committing a transnational crime, such as cybercrime, resides must either prosecute the individual if its legal framework allows, or extradite them to another competent state for **prosecution**[21]**.**

Expanding the application of extradition and streamlining its procedures necessitates strong

legislative and regulatory frameworks at the domestic level, as well as the signing of bilateral and multilateral international agreements. Furthermore, domestic laws must be aligned with international requirements to ensure effective implementation. The primary goal of extradition is to prevent the accused from evading justice, especially when the laws of the state in which they reside do not permit prosecution for the crime in question. Therefore, extradition serves as a cornerstone of international cooperation in crime prevention. This principle has been incorporated into several agreements and treaties, including the Budapest Convention[22].

Despite the significance of extradition procedures in fighting cybercrime and the efforts of states to implement them through several agreements, considerable challenges persist. One key issue is the requirement that the act in question must constitute a legally punishable crime in both the requesting and requested states, as extradition affects individuals' personal freedoms and relies on foreign jurisdiction. The problem arises when certain acts are not criminalized in one of the states, creating an obstacle to achieving the dual criminality requirement. This challenge is further exacerbated by the fact that numerous states have not updated their legal frameworks to address the evolving nature of cybercrimes, relying instead on traditional criminalization provisions that are inadequate for dealing with these modern offenses.

[19] Article 32 under the title "Mutual Assistance" of the Arab Convention on Combating Cybercrime, held at the Secretariat General of the Arab League in Cairo on 21/12/2010, states: "All member states shall exchange assistance to the maximum extent possible for the purposes of investigations or proceedings related to information crimes and information technology, or to collect electronic evidence in criminal cases."

[20] Khadra Chenti, *Legal Mechanisms for Combating Cybercrime: A Comparative Study*, Doctoral Thesis for the Degree of Doctor of Law, Criminal Law, Ahmed Draia University, Faculty of Law and Political Science, Adrar, 2020/2021, p. 215.

[21] Jamil Abdel-Baqi, *Op. Cit.*, p. 88.

[22] See Articles 12, 23, 24, and 25 of the Budapest Convention on Cybercrime, held on November 23, 2001.

Another significant challenge is the issue of multiple extradition requests. This arises when a criminal's actions harm various countries, as is often the case with terrorism conducted via electronic means. In such instances, numerous states may submit extradition requests for the same individual. To address this, the requesting state must provide sufficient evidence to substantiate that the accused committed the crime and is genuinely sought by its legal authorities.

CONCLUSION:

From the above, it is evident that cybercrime has experienced significant growth due to the increasing and widespread use of internet networks. This expansion has transcended national borders, posing a serious threat to the international community as a whole. Consequently, this persistent threat has rendered states, despite their substantial human and material resources, incapable of addressing it independently. Therefore, integration into a global system through regional and international agreements has become essential. However, the implementation of such cooperation faces international challenges, many of which are procedural in nature.

FINDINGS:

- Cybercrime disregards geographical borders, posing a threat to several countries. Its rapid growth is closely linked to the expansion of internet networks and the technological advancements occurring globally.
- International cooperation in combating cybercrime has become an absolute necessity, as no single country can address it independently, even if it possesses sufficient security capabilities.
- Numerous countries have chosen to integrate into a unified global system to fight this type of crime, as reflected in the signing of various regional and international agreements.
- Efforts to unify criminal policy against technological crime face various international obstacles, especially procedural ones. These include conflicts over international judicial jurisdiction to address incidents, challenges associated with international judicial cooperation requests, and issues surrounding the extradition of wanted criminals.

Recommendations:

- Unifying international criminal policy necessitates moving beyond reliance on traditional legal provisions that no longer align with the evolving nature of international cybercrime. Instead, it is essential to establish substantive and procedural laws that effectively address the requirements of fighting this type of crime.
- Efforts should focus on drafting international agreements to unify states' approaches to resolving conflicts over international judicial jurisdiction in cybercrime cases.
- Establishing communication channels between law enforcement agencies is significant to expedite and facilitate mutual assistance requests between states, especially in responding to international judicial cooperation requests and extraditing wanted criminals. This could include appointing a central authority to oversee these processes or enabling direct communication between the relevant agencies.

-SOURCES AND REFERENCES:

1- legal texts:

A) International agreements:

1. The Arab Agreement on Combating Information Technology Crimes held at the headquarters of the General Secretariat of the League of Arab States in Cairo on 12/21/2010, ratified by Presidential Decree 14/252 dated 09/08/2014, Official Gazette, No. 57, of 2014

2. Report of the meeting of the Working Group on International Cooperation held in Vienna, Austria, on 27 and 28 October 2015.

3. The Budapest International Convention on Combating Cybercrime, drawn up on 11/08/2001 and ratified on 23/11/2004.

B) Legislative Texts:

1. Law 09/04 of 05/08/2009 containing special rules for preventing and combating crimes related to information and communication technologies, Official Gazette, No. 47, 2009.

2- references:

A) Books:

1. Ahmed Khalifa Al-Malt, Cybercrimes, Dar Al-Fikr Al-Arabi, Egypt, 2005.

2. Titouche Radia, Territoriality of Criminal Law and Cybercrime, Revue Cahiers du Politique et de Droit, January 2019.

3. Adel Yahya, Criminal Policies in the Face of Cybercrime, Dar Al-Nahda Al-Arabia, Cairo, 1st edition, 2014.

4. Abdelhakim Rachid Touba, Information Technology Crimes, Dar Al-Mustaqbal for Publishing and Distribution, Amman, Jordan, 1st edition, 2008.

5. Jamil Abdel Baki, "Procedural Aspects of Internet-Related Crimes," Dar Al-Nahda Al-Arabiya, Cairo 2001.

B) journal scientific:

1. Farid Nachef, Mechanisms of International Cooperation in Combating Cybercrimes, Journal of Research in Law and Political Sciences, Ibn Khaldoun University of Tiaret, Vol. 08, No. 01, 2022.

2. Soraya Bourbaba, International Cooperation in Combating Cybercrime, Journal of International Law Studies, Faculty of Law and Political Science, Tahri Mohamed University, Bechar, Algeria, Issue 01, published on 20/07/2019.

3. Taher Yaker, "Combating Cybercrime between National Legislation and International Conventions," *Al-Sada Journal for Legal and Political Studies*, Djilali Bounaama University, Khemis Miliana, Algeria, Volume 04, Issue 04, issued on 30/12/2022.

C) Thesis doctorate:

1. Badri Faycel, *Combating Information Crime in International and Domestic Law*, PhD thesis in Public Law, Faculty of Law, Benyoucef-Benkhedda University, Algeria, 2017/2018.

2. Khadra Chenti, *Legal Mechanisms for Combating Cybercrime: A Comparative Study*, Doctoral Thesis for the Degree of Doctor of Law, Criminal Law, Ahmed Draia University, Faculty of Law and Political Science, Adrar, 2020/2021.