International Cooperation in Combating Cybercrime
Coopération internationale dans la lutte contre la cybercriminalité

Dr. Brichi Belkacem[*]
Faculty of Law University Center Aflou
belkacem.brichi1@gmail.com

***Received:* 15/ 08/ 2023** ***Accepted:* 25/ 08/ 2023** ***Published:* 15/ 09/ 2023**

Abstract:

The abstract should be written within 100 words The objective of this study is to explore and identify the emerging features of cybercrime, which relies on leveraging scientific and technological assets, as well as utilizing communication means and information networks. This research includes the analysis of the concept of cybercriminality, as well as the assessment of the effectiveness of international security and judicial cooperation mechanisms in combating it.

Keywords: cybercrime, security and judicial cooperation, Internet, cybercriminality.

Introduction :

Due to significant developments in the field of computing and communications, and the world's entry into the digital era, also known as the era of speed, along with the rapid global spread of the internet, and the use of computers and their applications in all activities and services, there has been a shift in the management of national affairs. Thanks to these modern technologies, the borders between countries have become porous.

This has led to an opening to the outside world and a huge advancement brought by technological civilization in the information age. This has led to the emergence of the term "cybercrime" or "digital crime," its increasing prevalence, and its rising level of danger and complexity, whether in terms of facilitating communication or coordinating its operations.

This calls for rapid and effective international cooperation to prevent these innovative crimes, which have become a global threat due to their ease of commission, their speed in affecting all layers of society, the difficulty of identifying their perpetrators, and the ability to evade the negative consequences of such crimes. Many countries have formulated special laws to address them.

[*] Submitted author

Following the above, the main question that arises is: **How have mechanisms of international cooperation contributed to combating cybercrime?**

THE FIRST TOPIC : Concept of Cybercrime

The sociologist "Daniel Bell" wrote in his book "The Coming of Post-Industrial Society": "It seems that information technology is the fuel of the third industrial revolution, and that information itself is the essential raw material of production on which society depends to produce, find, and profit from.[1]

This quote highlights the positive aspect of information and communication technologies. However, this positive aspect is not immune to the negative aspects that manifest in cybercrime or cyberterrorism. So, what is cybercrime, what are its characteristics and forms?

FIRSTLY: DEFINITION OF CYBERCRIME

Preface There are divergent views on the definition of cybercrime. There is a legal perspective, another technical, and there is also an approach that defines cybercrime based on the method of perpetration, the subject, the technological knowledge of the perpetrator, or based on other criteria according to different viewpoints.

Computer crimes are defined as crimes that require specific knowledge of computer technologies and information systems for their commission, investigation, and prosecution. They are also defined as crimes committed when a person uses their knowledge of information systems to engage in illegal activity. Some define them as unlawful acts using the computer as a tool or object of the crime. They also encompass all criminal activities committed through the computer or the internet, including crimes such as sexual offenses, hacking, illicit e-commerce, piracy, organized crime. In all cases, computer crimes do not recognize borders between countries, and often extend beyond international boundaries.[2]

Cybercrime can be defined as an infringement of computer data stored and information transmitted through information systems and networks, primarily the internet. It is a technological crime that occurs covertly, committed by savvy criminals with technical knowledge, aiming to compromise the right to information.[3]

Likewise, a distinction can be made between crimes on the internet in general and computer crimes in particular, where computer crimes can be committed without the need for an internet connection, such as the use of computers and their components in activities such as counterfeiting, forgery, theft of information, destruction or theft of hardware and software.

[1] Al-Sayyid Ateeq, Internet Crimes, Dar Al-Nahda, Egypt, 2000, p. 25.

[2] Muhammad Saeed Abdel Mageed, "Al-Mu'allimatia wal Jarimah" (Informatics and Crime), 1st edition, Dar Al-Isra for Publishing and Distribution, Egypt, 2006, pp. 13-14.

[3] Younis Arab, "Jaraim Al-Kompuyuter wal Internet" (Computer and Internet Crimes), Ittihad Al-Masarif, 2001, p. 19.

However, for internet-based crimes, an internet connection is necessary to fulfill their constitutive elements

SECONDLY: CHARACTERISTICS OF CYBERCRIME

These cybercrimes stand out for their modernity in how they are executed, their speed, their ability to conceal themselves easily, and their capacity to erase their traces. They come in various forms and dimensions, but what characterizes them is their cross-border global nature. This reality is entirely natural, especially considering that the Internet, by its very nature, knows no boundaries, making it a worldwide reality.[4] In general, cybercrime possesses several distinguishing features that set it apart from other forms of criminal activity.

1- Covert Crime: The cybercriminal quietly deletes data, information, or programs stored in the computer's memory discreetly. They manage to do so through invisible and imperceptible electronic pulses. This distinctiveness sets cybercrime apart from traditional crime. In addition to its increased frequency of commission and resulting damages, it is characterized by its discreet nature. The perpetrator can destroy, corrupt, or alter information without any physical movement, limiting their action to mental effort and technical skills, committing their crime calmly and serenely.

2- Borderless crime: National borders are no longer an obstacle for cybercriminals. Their criminal activity is no longer confined to a specific region but extends across multiple territories. For instance, a criminal can plan their act in one country, execute it in another, and seek refuge in a third to evade legal authorities. This characteristic indicates that cybercrime does not adhere to the geographical borders that blur in the virtual world. Indeed, the information society is open and interconnected through networks that transcend time and space, without hindrances or restrictions. Consequently, most countries are threatened by the specter of cybercrime.[5]

3- Difficult to Prove Crime: Cybercrime distinguishes itself from traditional crime by being committed in an intangible virtual environment through imperceptible electronic pulses and digital oscillations. Its traces vanish with a simple click. Even the method used to commit it differs, which can make the detection of cybercrime challenging.[6]

THIRDLY: FORMS OF CYBERCRIME

The forms of cybercrime are numerous and varied, as they are not subject to specific criteria for classification due to the constant evolution of their networks and the services they provide.

1- Crimes against Individuals:

This involves crimes that infringe upon individuals' privacy, where traditional laws may not be applicable. These offenses are committed through technology. Despite the development of

[4] Hussain bin Saeed bin Saif Al-Ghafri, "Al-Juhud Ad-Dawliyah Fi Mawajahat Al-Internet" (International Efforts in Facing the Internet), p. 2, available at the following link:https://knowledgemanagements.files.wordpress.com/2014/09/d8a7d984d8aad8b9d8a7d988d986-d8a7d984d8afd988d984d98a-d981d98a-d985d983d8a7d981d8add8a9-d8acd8b1d8a7d8a6d985-d8a7d984d8a7d986d8aad8b1.pdf.

[5] Naïma Daoudi, Electronic Crime (Characteristics, Areas of Use, and Important Methods of Combating it), Mahd Al-Lughat Journal, Faculty of Foreign Languages, Hassiba Ben Bouali University in Chlef, Algeria, Volume 02, Issue 01, 2020, p. 48

[6] Brahimi Jamal, Criminal Investigation in Cybercrimes, Ph.D. Thesis in Law, Faculty of Law and Political Science, Department of Law, Mouloud Mammeri University - Tizi Ouzou, 2018, p. 195.

individual and societal life through the use of the virtual space, it has become a formidable weapon in the hands of criminals to access individuals' personal information. Several types of computer crimes against individuals have emerged, including privacy breaches and violations of intellectual property rights.

2- Financial Crimes :

With the evolution of the internet, methods of electronic payment and transactions have evolved, becoming an integral part of financial transactions. During these online financial exchanges, several electronic crimes have arisen, such as theft, hacking, illegal electronic fund transfers, and magnetic card fraud. The illegal creation of card keys and bank accounts is now possible through internet channels.[7]

3- Crimes against National Security :

The most significant electronic crimes that threaten national security include:

A- Electronic espionage: This type of crime relies on advanced technologies and is no longer limited to military or political information but now extends to economic, commercial, and cultural domains. This type of crime emerged particularly after the events of September 11th in the United States.[8]

B- Organized crime : Criminal organizations have exploited the opportunities offered by communication means and the internet to plan, execute, and direct their criminal activities with ease.

C- Intellectual security-related crimes : Intellectual security is one of the most dangerous crimes committed online, as the internet offers opportunities to influence the beliefs and traditions of entire societies, making them vulnerable to intellectual manipulation and facilitating the creation of chaos.[9]

THE SECOND TOPIC : LA COOPERATION SECURITAIRE ET JUDICIAIRE DANS LA LUTTE CONTRE LA CYBERCRIMINALITE

It is imperative for states to collaborate in combating this new type of crime, which is no longer limited to a single country or community but crosses borders and harms multiple countries and societies, exploiting the significant evolution of modern technological means of communication and transportation. Strengthening cooperation between countries, taking effective measures to limit, eradicate, and punish the perpetrators is essential.

FIRSTLY: SECURITY COOPERATION IN COMBATING CYBERCRIME

Practical reality has shown that states cannot effectively combat crime alone, given the tangible and impressive developments in all areas of life, especially in communications and

[7] Khaled Mamdouh Ibrahim, "Electronic Crime," University House, Alexandria, 2001, p. 76.

[8] Linda Sharashba, "International and Regional Policies in Combating Electronic Crime: International Trends in Combating Electronic Crime," Studies and Research, Ziane Achour University, Djelfa, Algeria, Volume 01, Issue 01, 2009, p. 242.

[9] Ahmed Ben Khalifa, "The Electronic Crime and Mechanisms to Confront It," Al-Imtiyaz Journal for Economic and Management Research, Amar Thelidji University, Laghouat, Algeria, Volume 01, Issue 01, June 2017, Page 158.

information technologies. The International Criminal Police Organization (INTERPOL) serves as a model of security cooperation to combat organized crime. As the world's largest police organization, INTERPOL was founded in 1923 and is tasked with assisting law enforcement agencies of its 186 member countries in combating all forms of crime worldwide. INTERPOL has advanced infrastructure for technical and on-the-ground support, enabling police forces from around the world to address the growing challenges of 21st-century crime. The organization focuses on six priority areas: corruption, drugs, organized crime, advanced technology-related financial crime, fugitives, threats to public security and terrorism, and human trafficking.

INTERPOL is one of the affiliated agencies of the United Nations and operates under its auspices and supervision. It was created by a decision of the UN General Assembly and aims to strengthen and encourage international cooperation in police security, assisting agencies of member states in cooperating and collaborating in the fight against crime, particularly transborder and organized crime. Data and information related to criminals and crimes are collected and exchanged through National Central Bureaus of International Police located in the regions of member countries. Furthermore, cooperation involves aiding in the apprehension of criminals with the assistance of police forces from partner countries and providing available information within their region, especially for complex crimes across multiple countries, including online crimes.[10]

Moreover, INTERPOL has decided to establish a specialized center in Singapore for combating cybercrime, which develops investigative techniques and employs around 300 experienced technology police officers.[11]

SECONDLY: JUDICIAL COOPERATION IN COMBATING CYBERCRIME

International judicial cooperation is the primary mechanism for combating crime in its various dimensions. It involves the assistance and cooperation that authorities of one state provide to another state to pursue and punish criminals for their acts, implementing preventive measures to combat non-national forms of crime, and gathering evidence in various ways, which takes time and requires resources that the authorities of a single country generally lack unless supported by the legal authorities of other countries.[12]

Judicial cooperation is, therefore, the main mechanism for combating transnational crime in its various dimensions, especially concerning cybercrime. In the case of electronic crimes, the effectiveness of investigation and judicial prosecution often requires the assistance of authorities

[10] Hussein bin Saeed Al-Ghafari, Criminal Policy in Confronting Internet Crimes: A Comparative Study, 1st Edition, Arab Renaissance Publishing and Distribution House, Cairo, 2009, pp. 639-640.

[11] Ben Omar Al-Hajj Issa, Interpol as an International Police Institution for Combating Transnational Organized Crime, Journal of Legal and Political Studies, Faculty of Law and Political Science, University of Laghouat, Algeria, 2016, p. 259.

[12] A contribution by Mohamed Issa Boua, the need to update mechanisms of international cooperation in combating cybercrime, presented within the framework of the First Maghreb Conference on Informatics and Law, held from 28th to 29th October 2009, at the Higher Studies Academy - Tripoli, Libya, page 07

in the country where the crime was committed or where criminal activity transited en route to its target, or where evidence of the crime is available. For example, a criminal might have nationality in one country, use computers in another country to commit the crime, the effects of which are felt in a third country.

Judicial Cooperation in Combating Cybercrime takes several forms:

1- International Judicial Assistance: International judicial assistance is defined as any legal procedure undertaken by a state to facilitate proceedings in other states for a specific crime.[13]

Algerian legislation has enshrined the principle of mutual international judicial assistance in Law No. 04/09 on special rules for the prevention and combat of crimes related to information and communication technologies. Article 16 of this law considers that, in the context of international investigations and judicial inquiries aimed at collecting electronic evidence, international judicial assistance can take various forms, including:

- Exchange of information.
- Transfer of proceedings.
- International letters of request.

2- Extradition of Criminals: International law considers the extradition of criminals as one of the forms of international cooperation to combat crime and criminals, and to protect societies from their threat to security and stability. This ensures that criminals do not go unpunished and do not act with impunity. The procedure for the extradition of criminals is defined as the act by which the state where a person accused or convicted of a crime has taken refuge hands them over to the competent state for trial or execution of the sentence.

Extradition and judicial assistance are carried out under an agreement between two states and based on the conditions and procedures determined by that agreement.

The application of the principle of extradition and judicial assistance is used in cases where borders prevent the prosecution of criminals, including electronic crimes whose effects manifest in other countries.[14]

As stipulated in Article 24 of the Budapest Convention of 2001, the conditions for the extradition of criminals were defined, with a comprehensive agreement between both states for extensive cooperation aimed at conducting investigations or procedures related to criminal offenses involving networks and informational data, as well as collecting electronic evidence of these crimes.

Similarly, the Algerian legislator affirmed the principle of extraditing criminals in accordance with Article 82 of the Constitution, which states: "No one shall be extradited outside the national territory except under an extradition law and its application." Therefore, the Algerian legislator constitutionally acknowledged this principle, as also endorsed within the law on criminal procedures in articles 694 and subsequent ones.

[13] Salem Mohamed Sulaiman Al-Ojli, International Criminal Responsibility Provisions in Domestic Legislation, PhD thesis, Faculty of Law, Ain Shams University, Cairo, 1997, page 425.

[14] Amir Faraj Youssef, "Electronic and Information Crimes: International and Local Efforts to Combat Computer and Internet Crimes," Al-Wafa Legal Library, Alexandria, Egypt, 2011, p. 428.

THE SECOND TOPIC : OBSTACLES TO INTERNATIONAL COOPERATION IN COMBATING CYBERCRIME

Investigating electronic crimes and prosecuting their perpetrators are hindered by numerous obstacles and challenges that could compromise the detection and proof of crimes, and even lead to negative outcomes.

FIRSTLY: LEGISLATIVE GAPS AND CONFLICTS OF INTEREST BETWEEN STATES:

Differences between the legal systems of states pose a major obstacle to international cooperation in the fight against cybercrime. These differences lead to problems of law enforcement and practical challenges, especially since most state legal systems do not clearly define the concept of cybercrime, and their lack of specific legal framework for these crimes makes international cooperation difficult.[15]

SECONDLY: DIVERSITY AND DIVERGENCE OF LEGAL PROCEDURAL SYSTEMS:

Due to the diversity and divergence of legal procedural systems, investigation, inquiry, and prosecution methods that have proven effective in one country may be ineffective or even inapplicable in another, as is the case with electronic surveillance, surveillance-based extradition, covert operations, and other similar procedures. Thus, what is considered legal in one country may be illegal in another, which can result in frustration for the originating state due to the recipient state's authorities' inability to use what it deems an effective tool. Moreover, the judicial authorities of the recipient state may not allow the use of any evidence collected in a manner deemed illegal by that state, even if that evidence was obtained within the jurisdiction and legally.[16]

Conclusion:

This study has demonstrated that cybercrimes have become a concern for states, as they are vulnerable to attacks, infiltrations, and online extremist groups. This type of criminal activity can be committed from anywhere in the world, and the associated risks are increasing every day. Modern technologies alone are not sufficient to protect individuals from online criminal activities, which have caused significant harm to individuals, organizations, and states.

Many countries have taken measures to address cybercrime, especially in terms of international security and judicial cooperation. However, these efforts are still insufficient, and more endeavors are required to confront this serious threat.

Recommendations:

[15] Adel Abdel-Aal Ibrahim Kharashi, "Challenges of International Cooperation in Combating Cybercrimes and Ways to Overcome Them," p. 234, available at the following link: https://jfslt.journals.ekb.eg/article_14124_9940c95e1f087a055130abff802ddbd8.pdf

[16]

- Call for strengthening international and national cooperation by coordinating agencies responsible for combating cybercrime, exchanging experiences, and providing training to ensure effectiveness.

- Encourage states to expedite their adherence to international agreements against cybercrime.

- Train law enforcement agencies, experts, investigative authorities, and judges to be capable of handling such cases.

- Establish governmental oversight of content disseminated through the Internet, especially terrorist extremist ideologies, using specific programs, and the ability to block such sites.

- Transfer technologies used in advanced countries to combat online crime to countries that have not yet acquired these technologies.

- Raise awareness in society through various media about the dangers of cybercrime, with the participation of scientists, experts, religious leaders, educational, social, and cultural institutions in this field.

Bibliography List setting:

- Books:

1- Said Atiq, Internet Crimes, Dar Al-Nahda, Egypt, 2000.

2- Mohammed Saïd Abdel-Majeed, Computers and Crime, 1st Edition, Librairie Isra for Printing and Publishing, Egypt, 2006.

3- Younes Arab, Computer Crimes and the Internet, Union of Banks, 2001.

4- Khalid Mamdouh Ibrahim, Electronic Crime, Dar Al-Jameia, Alexandria, 2001.

5- Hussein bin Saïd Al-Ghafari, Criminal Policy Facing Internet Crimes, Comparative Study, 1st Edition, Dar Al-Nahda Al-Arabiya for Editing and Distribution, Cairo, 2009.

6- Amir Faraj Youssef, Electronic and Informational Crime, International and National Efforts to Combat Computer and Internet Crimes, Wafa Al-Qanouniya Library, Alexandria, Egypt, 2011.

- University Theses:

1- Brahimi Jamal, Criminal Investigation in Electronic Crimes, PhD thesis in Science, Specialty: Law, Faculty of Law and Political Science, Department of Law, University Mouloud Mammeri - Tizi Ouzou, 2018.

2- Salem Mohammed Sulaiman Al-Ojli, International Criminal Responsibility Sentences in National Laws, Doctoral Thesis, Faculty of Law, Ain Shams University, Cairo, 1997.

- Articles and Scientific Contributions:

1- Horia Gouigha, Economic Dimensions of Electronic Crime, Review of Economic Reforms and Integration in the World Economy, Higher School of Commerce, Algeria, Volume 14, Number 02, 2020.

2- Naïma Daoudi, Electronic Crime (Characteristics, Areas of Use, and Main Methods of Combat), Mahd Al-Lugat Review, Faculty of Foreign Languages, Hassiba Ben Bouali University - Chlef, Algeria, Volume 02, Number 01, 2020.

3- Linda Charachba, International and Regional Policy in Combating Electronic Crime: International Trends in Combating Electronic Crime, Studies and Research, Ziane Achour University, Djelfa, Algeria, Volume 01, Number 01, 2009.

4- Ahmed Ben Khalifa, Protection of Prince Abdelkader, Electronic Crime, and Mechanisms of Combat, Review of Excellence for Research in Economics and Management, Amar Thelidji University, Laghouat, Algeria, Volume 01, Number 01, June 2017.

5- Ben Ammar El Hage Issa, Interpol as a Mechanism for International Police in Combating Transnational Crime, Review of Legal and Political Studies, Faculty of Law and Political Science, Laghouat University, Algeria, 2016.

6- Bawa L'maali Mohammed Issa, The Necessity of Modernizing Mechanisms of International Cooperation in Combating Cybercrime, intervention within the framework of the first Maghreb conference on computers and law, held from October 28 to 29, 2009, Academy of Advanced Studies - Tripoli, Libya.

- Websites:

1- Hussein bin Said bin Saeed Al-Ghafari, International Efforts to Confront the Internet, available at the electronic link:

https://knowledgemanagements.files.wordpress.com/2014/09/d8a7d984d8aad8b9d8a7d988d986-d8a7d984d8afd988d984d98a-d981d98a-d985d983d8a7d981d8add8a9-d8acd8b1d8a7d8a6d985-d8a7d984d8a7d986d8aad8b1.pdf.

2- Adel Abdel Al-Ibrahim Khirashi, Problems of International Cooperation in Combating Cybercrime and Means of Overcoming Them, available at the electronic link:

https://jfslt.journals.ekb.eg/article_14124_9940c95e1f087a055130abff802ddbd8.pdf.