International Cooperation Mechanisms to Combat Cybercrime

آليات التعاون الدولي لمواجهة الجرائم السيبرانية

Ismahane KHARMOUCHE [1*]

[1] **Mohamed Lamine Debaghine University Setif 2, Algeria**

i.kharmouche@univ-setif2.dz

Date of transmission: 15/03/2024 date of acceptance: 08/05/2024 date of publication: 01/06/2024

****

Abstract :

Information technology is the tool of our time to keep pace with the development and progress occurring in the entire world, as it is the most powerful intellectual tool to bring about change in humans and the surrounding environment. It has, however, negative effects that have facilitated the rapid spread of cybercrime in accordance with the nature of the expeditious development of this technology. In fact, what has contributed to its spread is the inability of legislative texts to keep pace with this swift development, which necessitated the need for immediate intervention to confront this type of crime because of its danger to individuals and countries at the same time, and to develop mechanisms to coordinate cooperation at the international level as crimes that transcend the geographical borders of countries .

Keywords : Cybercrime, cybercriminal, international cooperation

ملخص:

تكنلوجيا المعلومات أداة العصر لمواكبة التطور و التقدم الحاصلين في العالم بأسره ، فهي الأداة الفكرية الأقوى لإحداث التغير في الإنسان و البيئة المحيطة به، غير أن لها تأثيرات سلبية ساهمت في إنتشار الجريمة السيبرانية بشكل سريع يتلاءم وطبيعة التطور السريع لهذه التكنولوجيا ، و ما ساهم في إنتشارها عدم قدرة النصوص التشريعية على مواكبة هذا التطور السريع ، الأمر الذي إستلزم ضرورة التدخل الفوري لمواجهة هذا النوع من الجرائم لما له من خطورة على الفرد و الدول في نفس الوقت ، ووضع آليات لتنسيق التعاون على المستوى الدولي بإعتبارها جرائم تتخطى الحدود الجغرافية للدول.

الكلمات المفتاحية: الجريمة السيبرانية ، المجرم المعلوماتي ، التعاون الدولي.

* Corresponding Author

Ismahane KHARMOUCHE

Introduction :

The overwhelming deluge of the information revolution and entering the digital age at the beginning of the 21st century has led to the emergence of cyber threats and crimes that have become a great challenge for countries and governments, especially with the increasing spread of the information network and the Internet and the important data it contains and the need often to share this data. In a world without borders, cyber security has become a matter of great importance not limited to a specific country, but a global concern for all countries. This has prompted the need for concerted efforts to reach the greatest amount of data and information protection and this has led to the adoption of many legislations at the internal level of countries and at the international level as well as the international level.

Therefore, through this paper, we will try to shed light on cybercrime and the mechanisms of international cooperation to confront it

Topic:

Cybercrime is different from traditional crimes and is characterized by a kind of specificity, especially since it is transnational, and the coordination of international efforts to cooperate to address it requires conditions governed by special controls, so the question that arises is**:**

What are the mechanisms of international cooperation to confront and combat cybercrime**?**

In order to address this issue, we will address this topic in two sections

The first discusses the concept of cybercrime, and the second discusses international cooperation to combat cybercrime.

First section

The concept of cybercrime

The information revolution has changed many legal concepts in criminal law due to the emergence of modern values of a special nature, and with the lack of legal texts on this type of crime, we will try through this research to address the most important definitions of cybercrime, its characteristics, and the most common types of cybercrime, in a first requirement and then the elements of cybercrime in a second requirement.

First requirement

Characteristics and types of cybercrime

First part: Definition of cybercrime

A cybercrime is generally defined by legal scholars as an incident committed in violation of the penal code.

As for cybercrime, there are those who define it as any unlawful behavior related to the automated processing or transmission of data.

It is also the crime resulting from the introduction of false data into systems and the misuse of the outputs, in addition to other acts that constitute a more technically complex crime, as it is every criminal act that uses the computer as the main tool in its commission**.**

The TRIPS Agreement of 1994 considered any infringement of information systems as a crime punishable by law, which is included in the fifth section of this agreement, and urged the member states of this agreement to enact laws to criminalize all types of attacks on information systems[1].

In addition, the Tenth United Nations Congress on the Prevention of Crime and Punishment of Offenders, held in Vienna in 2000, defined it as : Any crime that can be committed by a computer system, a computer network or within a computer system, and includes all crimes that can be committed in an electronic environment.

The Council of Europe has recognized the existence of cybercrime in every case in which computer data, records or programs are altered, erased, written, or any other interference in the field of data completion or processing**.**

These crimes are characterized by speed and continuous development of the means of committing them, as well as the absence of physical violence against humans in comparison with traditional crimes during their implementation because they are cross-border, including those directed against the computer or information and communication technology systems for the purpose of damaging, destroying or modifying them.

There are also cybercrimes in which the computer is the tool or means of committing fraud, identity theft, credit card and asset theft, forgery, embezzlement, intellectual property theft, extortion, deviant behavior and sexual exploitation. [2]

---

[1] Mohamed Ali Al-Arian, Cybercrime, Dar Al-Jamiaa, Alexandria University, Egypt, 2011, p. 25

[2] Mona Al-Ashkar Jabbour, Cybersecurity is the Obsession of the Age, Arab Center for Legal and Judicial Research, League of Arab States, Cairo, 2012.

Second part: Characteristics of Cybercrime

Cybercrime has a number of characteristics that differ from those known in traditional crimes, as it has a global dimension, is carried out with minimal effort - the click of a button - and does not require the presence of violence, and can be summarized as follows:

Firstly: Transnational Crimes

Cybercrime often occurs in more than one country, crossing geographical borders, so when the crime occurs, the perpetrator is in one country, the victim is in another, and the damage is in a third country.

Secondly: Difficulty in detecting crimes

This is because they do not leave a trace that is easy to trace, in addition to not discovering the victim until a period of time after the commission of the criminal act. [1]

Thirdly: Crimes that are difficult to prove

Where the perpetrator uses complex and fast technical means in many cases, it does not take a few seconds, in addition to the ease of protecting and manipulating the evidence, and most importantly, the judiciary in many countries does not accept information technology evidence that consists of circuits, magnetic fields and electrical pulses that are not perceptible to the natural human senses. [2]

Fourthly: Easy to commit crimes

They are soft crimes, and some have called them white-collar crimes [3], as when the necessary technology is available to the perpetrator, committing the crime becomes easy and does not require time or effort**.**

Fifthly: Weakness of the security and judicial agencies towards it

This is due to the lack of technical expertise, as these crimes require high and advanced technology to detect and search for them.

---

[1] Nahla Abdel Qader Al-Momeni, Cybercrime, Dar Al-Thaqafa for Publishing and Distribution, Amman Jordan, 2016, p 52.

[2] Nahla Abdel Qader Al-Momeni, ibid, p. 55.

[3] Naela Adel Mohammed Qoura, Economic Computer Crimes, A Theoretical and Applied Study, Halabi Law Publishing, Beirut, 2014, p. 61.

Third part: Types of Cybercrime

Among the most famous types of cybercrimes are those that are carried out by attacking the components of the information system and programs in order to achieve a specific purpose, and among the most common of these crimes we find:

Firstly: The crime of modifying the information software

The software is modified by manipulating it for the purpose of embezzling money through information systems, such as what happened in one of the American banks when one of the programmers in the accounts department modified a software program in his own way, where he added 10 cents for internal account management expenses on every 10 dollars, one dollar on every account more than 10 dollars, and credited the excess expenses to his own account called "Zzwick" and managed to get hundreds of dollars per month, and this crime was discovered by the bank by accident**.** [1]

Secondly: The crime of tampering with a computer software

This is achieved by implanting an unauthorized sub-program in the original program that allows access to the basic elements of the original program**.**

Thirdly: The crime of attacking operating software

This is done by providing software with a set of additional instructions that make it easy to circumvent the information system, such as what was done by an insurance company in the United States of America in Los Angeles [2] by a programmer and his computer to design a fictitious digital software that manufactures insurance policies for fictitious people, numbering 64,000 insurance policies.

Second requirement: Elements of Cybercrime

Cybercrimes are created by the presence of an electronic device, which may be mostly a computer, which is used to carry out a criminally prohibited act issued by a defective will and for which the legislator establishes a penalty, and the act is described as criminally prohibited if the law includes a provision that criminalizes it, and in light of this, cybercrimes are based on three elements, the legal element, the material element and the moral element.

---

[1] Ayman Abdullah Fikri, Cybercrime: A Comparative Study in Arab and Foreign Legislation, Law and Economics Library, Saudi Arabia, 2014, p. 615.

[2] Hizam Al-Quraiti, Cybersecurity and Information Security Protection, Dar Al-Fikr Al-Jami'i, Alexandria, 2022, p. 43.

First part: The legal element of cybercrime:

The sources of criminalization and punishment are generally limited to legislation, as the legislator in most countries issues many laws related to the protection of information and network systems, including images of these attacks and the penalties prescribed for them, and since the idea of legislation is to protect the interests and social values in society and maintain the security of the state and protect it from any external aggression, whatever its source, most countries adopt modern legislation represented in issuing special laws containing regulatory and guiding provisions related to how to manage and exploit information systems and protect them, in addition to containing a criminal penalty to ensure that individuals respect these provisions.

Second part: The material element of cybercrime:

The material element of a crime in general is the external act that a person performs and is criminalized by the law, this element is considered the basis of the crime factually, it is the criminal act or the failure to perform an act required by law, and both are subject to punishment if it results in a result criminalized by the law, and cybercrimes, like all crimes, are based on three elements, behavior, result and a causal relationship linking the behavior and the criminal result**.**

The criminal behavior is the performance of acts of a technical nature that may include a moral multiplicity of more than one crime with the same behavior in some of them or limited to the physical behavior of the cybercrime by electronic means and the result is achieved by the occurrence of the crime based on that behavior.

For example, the perpetrator [1] prepares the computer to make the crime happen by downloading hacking programs, or he may prepare these programs himself, or he may need to prepare pages with indecent content and upload them to the host machine, or the criminal may prepare a viral program in preparation for its transmission.

Third part: Moral Element of Cybercrime

It is not sufficient for a cybercrime to exist and deserve punishment for it, merely the availability of its apparent material or the act constituting the material element of it, but it is additionally necessary for the act to be the fruit of a sinful will expressed by the moral element of the crime**.**

[1] Haitham Abdul Rahman Al-Bakli, Electronic Crimes Against Display between Sharia and Law, Dar Al-Qalam for Publishing and Distribution, Cairo, 2010, p. 21;

Therefore, the moral element is considered one of the necessary elements for the realization of the information crime, and it means the criminal will and the sinful intent associated with the act, whether it takes the form of criminal intent and is then characterized as an intentional crime or it takes the form of an unintentional error and is then classified as an unintentional crime, the moral element means the general criminal intent and is associated with the psychological state of the offender and the relationship between the material of the crime and the personality of the offender**.**

Second section

International Cooperation Mechanisms to Confront Cybercrime

Cybercrime is characterized by the fact that it is transnational, and there may be countries and governments involved in its occurrence, so the procedures for following up and preserving evidence constitute a great challenge, which requires international cooperation and coordination of the various departments specialized in collecting evidence across many countries, as cooperation allows direct and rapid communication between the agencies of the various departments of these countries, and this is done by establishing specialized offices to collect information about the perpetrators of the act related to the Internet and disseminate this information.

Therefore, in the first requirement, we will address the manifestations of international security and judicial cooperation to combat cybercrime, and then we will address international cooperation for the extradition of cyber criminals in the second requirement.

First requirement: Manifestations of international security and judicial cooperation to combat cybercrime

We address this requirement in two parts, the first part deals with the role of the International Criminal Police Organization in combating cybercrime, and the second part deals with the role of letters rogatory in combating cybercrime.

First part: The role of the International Criminal Police Organization in combating cybercrime

This organization was established in 1946, with its administrative headquarters in France, with 182 member states. [1]

[1] Yasser Mohamed Abdel-Al, E-Management and the Challenges of the Digital Society, Publications of the Arab Administrative Development Organization, Cairo, 2016, p. 252.

This organization seeks to emphasize and coordinate cooperation between international police agencies located in the territories of member states, and cooperate in apprehending criminals with the help of internal security agencies of member states, and provide them with the information available to them at the level of their territory, especially for transnational information crimes that are complex in several countries.

The organization's efforts culminated in the establishment of regional communication centers in Tokyo, New Zealand, Nairobi and Azerbaijan to facilitate the passage of messages and information about criminals.

In 1991, the Council of Europe established a European police force in Luxembourg to coordinate the work of national police agencies in European countries and to prosecute perpetrators of cross-border crimes, including computer-related crimes.

At the Arab level, the Arab Criminal Police Bureau was established to secure, develop and advance cooperation between police agencies in member states in the field of combating crime and prosecuting criminals within the framework of the laws and regulations in force in each country.

These different agencies contribute to the tracking of cybercriminals by coordinating cooperation among them to track and capture evidence and conduct cross-border searches of logical computer components, information systems, and communication networks in search of evidence of cybercrime.

Second part: International judicial cooperation to combat cybercrime

Prosecuting the perpetrators of cybercrimes and bringing them to justice in order to punish them, requires taking measures outside the borders of the state where the criminal act or part of it was committed in many cases, such as inspecting Internet sites abroad, seizing hard disks or searching computer systems, all these procedures collide with the issues of geographical borders, jurisdictions and providing mutual legal assistance.

International judicial assistance is whereby a country takes all necessary measures to facilitate the task of prosecution in another country in connection with the prosecution of a cybercrime offense . This assistance takes several forms.[1]

[1] Mohamed Ramadan Bara, Criminal Law Commentary, General Provisions of Crime and Punishment, 1st edition, National Center for Research and Scientific Studies, Cairo, 2017, p. 144.

Firstly: The exchange of information between state administrations

This is through the provision of information, data, documents and evidentiary materials requested by a foreign judicial authority while considering a crime related to the charges against its nationals or citizens abroad and the actions taken against them, and the exchange may include the judicial record of offenders. [1]

II : Transfer of proceedings

This is through the taking of criminal proceedings by a state, based on an agreement or treaty of cooperation, while investigating a crime committed in the territory of another state and in the interest of this state, with the condition that there is dual criminalization of this crime in both states, in addition to the legality of the proceedings, meaning that they do not violate the law in both states, and these proceedings must be of great importance and play an important role in reaching the truth.

Thirdly: International letters rogatory

It is a request to take a judicial procedure of the criminal proceedings, submitted by the requesting state to the requested state, in order to adjudicate a matter before the judicial authorities in the requesting state, which is unable to carry out all procedures individually [12], so it requests help in order to facilitate criminal procedures between states in order to ensure the necessary investigations to bring the accused to trial and overcome the obstacle of territorial sovereignty that prevents the foreign state from practicing some judicial acts within the territory of other states, such as hearing witnesses or conducting a search and others.

A letter rogatory request is sent through diplomatic channels, for example, a request to obtain evidence is usually the matter of the public prosecution, which is documented by the competent national court in the requesting state and then passed through the Ministry of Foreign Affairs to the embassy of the recipient state to send it to the competent judicial authorities in the recipient state.

In line with the speed factor in the fight against information-related crimes and the great development in the field of communication and communication technology, many countries have resorted to concluding many agreements related to international judicial cooperation between different administrations, which

[1] Mohamed Amine El-Roumi, Computer and Internet Crimes, University Publications House, Alexandria, 2018, p. 33.

[2] Yousef Al-Masry, Computer and Internet Crimes, 1st edition, Dar Al-Adl, 2011, p. 87

contributed to gaining time and shortening procedures through direct communication between the authorities concerned with the investigation. [1]

Second Requirement: International cooperation for the extradition of cyber criminals

This type of cooperation between countries and governments emerged as a result of the developments that occurred in all fields related to communications and information technology, in order to combat crime and hold perpetrators accountable, in order to protect societies and maintain their security and stability.

In this requirement, we will deal with three parts. The first part deals with the concept of the cyber extradition system, the second part talks about the conditions for extraditing a cybercriminal, and the third part explains the procedures related to the extradition of a cyber criminal.

First part: The concept of cyber extradition

A cybercriminal is any person who commits an act that is punishable by law and this act is characterized as a crime in most countries of the world, especially countries that cooperate with each other.

The act in this type of crime differs from other criminals because he is the most capable and knowledgeable about the new information systems, he is highly skilled in using and exploiting modern technological means in order to harm others, and the damage he causes may exceed the borders of his country's territory, and this is often the case. [12]

The extradition of a cybercriminal means that a state extradites a person present in its territory to another state at its request for the purpose of prosecuting him for a crime he is alleged to have committed or to execute a judgment against him.

It may happen that a judicial verdict is issued against a person, but before the execution begins, the criminal flees to another country, and the country in which the verdict was issued requests to receive the fugitive criminal from the country to which he fled.

The 2001 Budapest Convention on Cybercrime [3] addressed methods of international cooperation with regard to the principles of extradition and mutual

---

[1] Yousef Al-Masry, ibid, p88.

[2] Mohamed Abdel-Moneim Abdel-Khaliq, Internet Crimes, 2nd edition, Arab Renaissance House, 2015, p. 97.

[3] Official website of the Council of Europe: https://rm.coe.int/budapest-convention-in-arabic/1680739173

assistance between states, and also attempted to standardize the terminology associated with cybercrime in order to facilitate its management.

Second part: Conditions for extradition

In order to extradite a cybercriminal to a country, several conditions must be met:[1]

Dual criminalization, i.e., the act committed is criminalized in the two countries, the country requesting extradition and the country from which extradition is requested, where the act is criminalized regardless of the legislative form that is punished, without regard to the description or legal characterization that is given to the act.

It is inadmissible to extradite nationals or extradite beneficiaries of the right of political asylum, as it is well established in the international community and prevails in various national legislations of states and international conventions based on the principle of non-extradition of nationals and grantees of the right of political asylum in states.

It is also inadmissible to extradite those who have been prosecuted for the same crime for which their extradition is requested, as when the person whose extradition is requested has already been tried and criminalized for the same act committed, he may not be extradited for the same crime, and this condition provides the greatest amount of judicial protection for the person whose extradition is requested.

This is so that the person is not subjected to double punishment and is tried twice for the same cybercrime.

Third Part: Procedures for the extradition of a cybercriminal

These procedures relate to both the requesting state and the requested state.

As the requesting state must express its desire to receive the wanted person, and this request must be in writing, as the request may not be submitted orally, and the extradition request is accompanied by a set of documents indicating that the wanted person has committed the extraditable offense and some specifications of the person to be extradited, and the extradition process goes through several steps, as the competent judicial authorities in the requesting state are authorized to prepare the extradition request. As the competent judicial authorities in the requesting country are authorized to prepare the extradition request and deliver it to the higher authorities in the country represented by the Ministry of Justice, the latter of which sends the request and the attached file to the Ministry of Foreign

[1] Mohamad Morsi Zahra, Computers and Law, Kuwait Foundation for the Advancement of Sciences, Specialized Book Series, second edition, 2019, p. 144

Affairs, which, through diplomatic channels, sends the file to its embassy in the country from which extradition is requested. [1]

As for the requested country, the extradition procedure at its level also goes through the following stages: [2]

Receiving the request, taking investigative measures, collecting evidence and arresting the wanted person, which are matters within the jurisdiction of the State Police Department.

Interrogating the arrested person, remanding him in custody or releasing him with or without bail, and preventing him from leaving the territory of the state until the request for his arrest is resolved, which is a matter within the jurisdiction of the public prosecution in the state.

Examining the request by the competent court and deciding on the subject matter by accepting or rejecting it after the court verifies the availability of the formal conditions in the requesting state, such as the existence of the extradition file in full and containing all the documents that must be attached to it, certified by the competent authorities, in addition to the availability of objective conditions, such as the condition of dual criminality and the non-expiration of the public case or penalty and ensuring that there is no impediment to extradition stipulated by law. If all the formal and objective conditions are met, the extradition of the person subject to the request will be ordered by a final decision issued by the competent judicial authority, including the type of crime on the basis of which the person was extradited and it is worth noting that the decision of the competent judicial authority is not binding on the state and is of an advisory nature and has discretionary power under the law to extradite the person or not.

Conclusion:

The information, network and cyber systems are of strategic importance, which makes the forms of attack on them very dangerous because they threaten the cultural, economic and even security structure of countries, which has led to the recognition of its dangerous nature by all countries and the attempt to shed light on its risks and the necessity of taking all measures and adopting all means in order to strengthen protection and prevention of this type of crime, which affects the private life of the individual in many cases, leaving a growing sense of the dangers of adopting this technology despite the urgent need to use it in line

[1] Brenton Chress and Others : Maiana Village Parkway ,Alameda : Syb ex inc ,Mstering Network Security,2003 .

[2] Lehto Martti ,Neittaanmak .Cyber Security : Analytics,TECHNOLOGY and Automation .Swtzerland : Springer International Publishing ,2015.

with the global scientific development. Some cybercrimes affect the national security of countries within the framework of the so-called information war or electronic ethics, specifically espionage crimes and crimes of appropriation of information transferred outside the borders.

Cybercrime is spreading and expanding, which threatens the security of individuals and states alike, so it is necessary to:

- Review both national and international legislation related to cybercrime, with a particular emphasis on intellectual property law, commercial law, and civil law, as well as to create electronic systems that are difficult to penetrate.
- Intensify efforts at the internal level of countries by adopting and passing legislation periodically in line with the nature of the speed and evolution of the spread of this type of crime.
- Coordinate efforts at the international level and make the procedures for extradition and rendition of cyber criminals more flexible.
- Adopting more effective international agreements to criminalize attacks on information systems, and working to facilitate the involvement of countries in them.

Bibliography

Books:

1- Mona Al-Ashkar Jabbour, Cybersecurity is the Obsession of the Age, Arab Center for Legal and Judicial Research, League of Arab States, Cairo, 2012 .
2- Nahla Abdel Qader Al-Momeni, Cybercrime, Dar Al-Thaqafa for Publishing and Distribution, Amman Jordan, 2016.
3- Naela Adel Mohammed Qoura, Economic Computer Crimes, A Theoretical and Applied Study, Halabi Law Publishing, Beirut, 2014.
4- Ayman Abdullah Fikri, Cybercrime: A Comparative Study in Arab and Foreign Legislation, Law and Economics Library, Saudi Arabia, 2014.
5- Hizam Al-Quraiti, Cybersecurity and Information Security Protection, Dar Al-Fikr Al-Jami'i, Alexandria, 2022
6- Haitham Abdul Rahman Al-Bakli, Electronic Crimes Against Display between Sharia and Law, Dar Al-Qalam for Publishing and Distribution, Cairo, 2010.
7- Yasser Mohamed Abdel-Al, E-Management and the Challenges of the Digital Society, Publications of the Arab Administrative Development Organization, Cairo, 2016.

8- Mohamed Ramadan Bara, Criminal Law Commentary, General Provisions of Crime and Punishment, 1st edition, National Center for Research and Scientific Studies, Cairo, 2017.
9- Mohamed Amine El-Roumi, Computer and Internet Crimes, University Publications House, Alexandria, 2018.
10- Yousef Al-Masry, Computer and Internet Crimes, 1st edition, Dar Al-Adl, 2011
11- Mohamed Abdel-Moneim Abdel-Khaliq, Internet Crimes, 2nd edition, Arab Renaissance House, 2015.
12- Mohamad Morsi Zahra, Computers and Law, Kuwait Foundation for the Advancement of Sciences, Specialized Book Series, second edition, 2019.
13- Mohamed Ali Al-Arian, Cybercrime, Dar Al-Jamiaa, Alexandria University, Egypt, 2011.
14- Brenton Chress and Others : Maiana Village Parkway ,Alameda : Syb ex inc ,Mstering Network Security,2003 .
15- Lehto Martti ,Neittaanmak .Cyber Security : Analytics,TECHNOLOGY and Automation .Swtzerland : Springer International Publishing ,2015.

Legal texts:

1- Official website of the Council of Europe: https://rm.coe.int/budapest-convention-in-arabic/1680739173