FIGHTING CYBERCRIME WITH IN THE FRAMEWORK OF INTERNATIONAL ORGANISATIONS: EFFECTIVENESS AND CHALLENGES.

DR. HAKIMABOUKEHIL[1], DR. BOUKREDINE HIBA[2]
[1]Lecturer Class A, Faculty of Law and Political Science, Specialisation: Public International Law,Mohamed CherifMessaadia University of Souk Ahras(Algeria).
[2]Lecturer Class A, Faculty of Law and Political Science, Specialisation: International Humanitarian Law, University BadjiMokhtarof Annaba (Algeria).
The Author's E-mail: hamimaboukehil23@gmail.com[1], boukredinehiba@ymail.com[2]
Received: 20/06/2024 Published: 15/01/2025

Abstract:
The widespread use of modern technologies has led to the emergence of many new crimes, including cybercrime, which pose significant risks to both individuals and society. Given the international nature of this serious crime and the intelligence level of its perpetrators, international organisations, regardless of their differences, are striving alongside states to combat this type of crime. This is achieved either by specifying in their charters acts that are considered cybercrimes, by holding specialised conferences or by activating methods of international cooperation that are considered essential, especially after the ineffectiveness of national laws in eradicating or even reducing these crimes has been demonstrated. However, states and international organisations face several challenges in achieving their goals, which reduce their effectiveness.

Keywords: Cybercrime, combating, international organisations, effectiveness, challenges.

INTRODUCTION:

Cybercrime has become one of the most serious crimes with a negative impact on all economic, social, political and security areas. Its danger has increased, especially with the development of communication technologies and the vast flow of information easily and quickly across distant areas, using modern technology and the ability to store and retrieve it in a very short time.

It is therefore imperative that States and international organizations make a concerted effort to address the dangers posed by this serious crime and to prosecute its perpetrators, as it is not confined within the borders of a single State but has permeated most countries of the world. This is due to the failure of domestic efforts to combat it, given its rapid spread, the concealment of evidence of its commission and the possibility of committing it at a distance. As a result, it has become a real threat to the security of individuals and governments, leading us to ask the following question: To what extent can international organisations play an effective role in combating cybercrime? Or what role do international organisations play in suppressing and preventing cybercrime?
In order to answer this question, we have decided to explore the topic in the following way:
- Chapter One: The conceptual framework of cybercrime.
- Chapter Two: The role of global and regional international organisations in combating cybercrime.

Chapter One: The Conceptual Framework of Cybercrime

Cybercrime first appeared in technologically advanced countries and subsequently spread to other nations, which have devoted considerable space in studies to define its concept. This has led to the establishment of several terms to denote it, such as "computer crimes," "high-tech crimes," "information crimes," and "internet crimes"[1]. In this chapter, we will address the concept of cybercrime in the first section and the types of cybercrimes in the second section.

Section One: The Concept of Cybercrime

Cybercrime is considered a serious social phenomenon, linked in its nature and magnitude to various transformations in society across all fields. Accordingly, we can say that definitions of cybercrime vary according to the terms used to describe it, as some see it as a result of the evolution of crime associated with information technology. Others believe that the different names

relate to the subject it addresses[2]. Therefore, we will attempt through this section to arrive at a definition that aligns with the nature of cybercrime in the first branch, and then we will move on to the characteristics of this crime in the second branch.

Branch One: Definition of Cybercrime:
Cybercrime is regarded as an emerging type of crime, and efforts to establish a specific definition for it have varied, with legal scholars not agreeing on a defined definition. This is supported by the argument that this type of crime is merely a traditional crime committed through modern electronic means[3].

1. Linguistic Definition:
- Crime:Derived from the term " جرم" (jurm), referring to sin and wrongdoing[4].
- Cyber: Refers to the automated processing of information and translates from the French term, meaning technology for gathering, processing, and transmitting information via computers[5].

2. **Legal Definition:**
- Most legislations have not provided a definition for the automated processing of information, delegating this task to legal scholars and the judiciary. However, some have provided definitions for information systems rather than automated processing systems[6]. The Algerian legislator has adopted the term "violation of data systems" to denote cybercrime, considering the information system itself and its components as the subject of the crime. A definition of cybercrime is found in Article 2 of Law No. 90/04, issued on August 5, 2009, which includes specific rules for the prevention and combating of crimes related to information and communication technologies.

3. Terminological definition:
- Numerous definitions have been provided by scholars from different disciplines and cultures to understand the intended meaning of the term “cyber”. Legal scholar “Mireui” defined it as: “Cybercrime is the illegal act involving a computer.” Lawyer Rose Blatt defined it as: “The illegal act of copying, altering, deleting, or accessing information stored in or transmitted by a computer.[7]”
- Professor Catalan described information as “a message expressed in a way that makes it transmittable or reportable to others”. Some others defined it as “a symbol or set of symbols that can convey meaning”. Lawyer Serleriz defined it as: “Any pattern of crime recognised in criminal law, as long as it is related to information technology”[8].

Section Two: Characteristics of cybercrime
Cybercrime is characterised by its unique nature, which stems from its association with computers and their advanced technology. This requires that criminal policy focus on these characteristics in order to formulate appropriate legal texts to combat this emerging type of crime. These characteristics include

1. Severity of cybercrime: The speed and capacity of computers to process information pose significant risks to the lives of individuals and their personal secrets, as well as to the economies of institutions and the security and economic policies of countries[9].
2. Intellectual basis: This type of crime is based on intellect rather than violence[10].
3. Lack of visible evidence: Cybercrime is often hidden and elusive and evolves faster than legislation due to rapid technological advances, such as the Internet[11].
4. Destruction of evidence: The perpetrator has the ability to destroy what could be used as evidence for a conviction[12].
5. Discovery by accident: Most, if not all, cybercrime is discovered by accident during the investigation.
6. Concealment: Cybercrime is often committed covertly, leaving no written trail, which makes it difficult to detect as it leaves no physical evidence.
7. Transnational nature: Cybercrime transcends borders and is committed in multiple locations, which may be affected simultaneously by a single cybercrime.
8. Modern methods: The means of committing cybercrime are innovative, requiring a computer or other device capable of automated information processing, such as hacking tools used to steal funds.

Section Three: Types of cybercrime

The manifestations of cybercrime are diverse and constantly evolving, reflecting advances in science and technology through the use of modern technological devices in all aspects of individual life. Unfortunately, it is difficult to categorise them comprehensively. There are crimes against individuals, crimes against property, and crimes against the state, which we will discuss in this section.

First: Crimes against individuals

Crimes against individuals or personal rights are those that threaten or violate personal rights, including "murder, assault, abortion, and honour crimes". These crimes can be committed using computers or the Internet. Examples of computer crimes against individuals include:[13]

- Computer-assisted murder and causing death.
- Intentional solicitation of murder over the Internet.
- Using the Internet to promote prostitution.
- Access to personal data of individuals.
- Harassment and bullying via secure communication channels.
- Spreading obscenity and violating public decency online, including the depiction of minors engaged in sexual activity.

Second: Cybercrime against property

Crimes against property threaten or violate financial rights. Major applications of these crimes within cybercrime include:[14]

- Data theft and credit card fraud.
- Crimes resulting from theft and financial violations of bank accounts and financial transaction centres through system breaches.
- The transfer of accounts to the hackers' accounts, a type of crime that is on the increase.
- Software piracy and theft of computer services[15].
- Forging emails or documents, records and identities.
- Using computers to obtain financial cards, or using them for others without authorisation, or destroying them.
- Entering false or forged data into computer systems.

Third: Cybercrime against the government

These are crimes committed against the public interest that threaten or violate rights of a general nature. Practical experience has revealed cybercrimes that fall into this category, including:[16]

- False reports of cybercrime.
- Tampering with and influencing legal evidence.
- Crimes aimed at disrupting government operations.
- Cyber terrorism.
- Failure to report cybercrime.
- Dissemination of data from unknown sources.

Chapter Two: The role of international and regional organisations in the fight against cybercrime

Since time immemorial, international communities have enacted laws and regulations to confront and combat all criminal acts, particularly cybercrime. International cooperation in the context of this serious crime is considered one of the most important issues that has attracted the attention of most countries due to its importance at both international and regional levels. This is due to several reasons, including the impossibility of countries living in isolation from each other without establishing international cooperative relations, as well as maintaining balanced relations to achieve common international interests.

Therefore, we can see that the international community has confronted this criminal phenomenon with a series of laws by establishing numerous global and regional agreements and treaties. In the first section, we will discuss the fight against cybercrime within the framework of global organisations, while the second section will be devoted to the fight against cybercrime within regional organisations.

Section One: Combating cybercrime within the framework of global international organisations

Due to the vast scope of cybercrime, international organisations, regardless of their differences, have sought to work with countries to combat this type of serious crime, either by specifying acts

that are considered cybercrimes in their charters or by holding specialised conferences. In this section, we will examine, among other things, the role of the United Nations in combating cybercrime in the first subsection, the role of Interpol in the second subsection, and the role of the World Intellectual Property Organisation (WIPO) in the third subsection.

Subsection One: The role of the United Nations in combating cybercrime

The United Nations is one of the most important forms of international cooperation in the fight against crime in general and cybercrime in particular. In this context, the UN plays an important role in laying the foundations for this cooperation through international agreements. At its Eighth Congress on the Prevention of Crime and the Treatment of Offenders, the UN adopted a special resolution on cybercrime, stating that international action to combat cybercrime requires Member States to take a number of measures, such as:[17]

- Updating laws and their criminal purposes, including measures to ensure the proper application of existing criminal laws.
- Seizing the proceeds of illegal activities.
- Implementing security and preventive measures while respecting individual privacy and human rights.
- Protect state interests and the rights of Internet victims.

On this basis, it can be said that the increase in crimes committed via the Internet has led the United Nations to convene several conventions on combating the misuse of technology for criminal purposes since 2000, emphasising the urgent need to enhance coordination and cooperation among countries in combating the misuse of information technology for criminal purposes.

Thus, the United Nations has paid considerable attention to the protection of electronic activities and the fight against all attacks against them, as reflected in the Fifteenth Congress of the International Association of Penal Law on Computer Crime in 1994, which specified the criminalised acts that constitute cybercrime, such as fraud and computer-related deception through destruction of data and unauthorised access. It also established many procedural rules to combat these crimes, such as searches and interception of communications[18].

Section Two: INTERPOL's Role in Combating Cybercrime

For any country to co-exist with others, a certain level of security and order is required. Crime is a major problem in many countries, affecting governments, professionals and individuals alike. As mentioned above, a state cannot eradicate crime on its own, especially with the rapid and astonishing development in various fields, especially in communication and information technology. The emergence and rapid expansion of the Internet has given rise to new forms and patterns of crime, including cybercrime, which poses a significant threat to the international community. This has created the need for an international body to take responsibility for combating or at least mitigating these risks, which can only be achieved through cooperation between police forces in different countries, given the transnational nature of these crimes, particularly in terms of exchanging information relating to crimes and tracking down criminals[19].

This is where the efforts of INTERPOL, the largest international police organisation founded in Lyon, France, in 1923, come into play. In 2004, INTERPOL set up a special unit to combat technology crime and worked with the G8 countries to develop strategies to combat such crimes. These strategies include:[20]

- Establishing a secure 24/7 communications centre between police forces in member countries.
- Using modern tools to combat these crimes, such as a centralised database of pornographic images provided by member countries using the Excalibur automated image analysis and comparison programme.
- Providing member police forces with cybercrime guidelines and training on how to combat and investigate cybercrime.

Section Three: The World Intellectual Property Organisation (WIPO)

The World Intellectual Property Organisation (WIPO), as one of the agencies of the United Nations, has focused on promoting innovation and developing the management of intellectual property associations. It has also emphasised the need for legal protection of software and databases in the information field, having concluded that such protection cannot be adequately provided by global agreements, in particular the "Berne" and "Paris" Conventions, which urge member states to develop their legislation, particularly copyright laws[21]. Under the Berne Convention, computer programs, whether in source or object code, are protected as literary works[22].

Article 3 of the Agreement Establishing WIPO states: "The purposes of the Organisation shall be: to contribute to the establishment of international rules for the protection of intellectual property rights; to promote the protection of intellectual property throughout the world through cooperation among States and, where appropriate, with other international organisations; and to provide for administrative cooperation among its members.[23]"

Section Two: Combating cybercrime within regional international organisations

Regional international organisations also seek to combat this type of serious crime, of course through their charters or by holding various conferences. This section will look at some of these regional organisations in the fight against cybercrime, starting with the European Union in the first subsection, followed by the African Union in the second, and finally the Arab League in the third.

Subsection One: The European Union - The Budapest Convention

We will also discuss the European Treaty on Combating Cybercrime, where the European Union and the Council of Europe have made significant efforts, culminating in the adoption of the Budapest Convention on Cybercrime[24]. This Convention addresses the international nature of cybercrime and its trans-national nature, helping countries to combat it and track down its perpetrators. It also outlines best practices for investigating cybercrime, with signatories committing to work closely together to combat it. In addition, the Convention details the substantive criminal law relating to cybercrime and its types, including terrorism and credit card fraud[25]. The Budapest Convention requires member states to take into account international human rights treaties when enacting domestic legislation related to cybercrime, such as the 1950 European Convention on Human Rights and Fundamental Freedoms and the 1966 International Covenant on Civil and Political Rights. Member States must also rely on standards to determine jurisdiction over the offences listed in the Convention, represented by the principles of territoriality and relativity, territorial jurisdiction and nationality[26].

Section Two: The African Union Initiative on Cybersecurity and Personal Data Protection

The Malabo Convention addresses a very serious issue: cybersecurity. It encompasses the fight against cybercrime, the protection of personal data and the supervision of electronic transactions. This is why the African Union is working directly to improve cybersecurity and collect national cybersecurity data. The effectiveness of the "Malabo" Convention is evident in the fact that it encourages international efforts to combat cybercrime and obliges member states to implement its provisions through a monitoring mechanism to ensure compliance[27].

Section Three: The Arab Convention against Cybercrime ("Information Technology Crimes")

The Arab Convention Against Cybercrime calls for enhancing cooperation among Arab states in combating information technology crimes in order to reduce their risks and protect the security of Arab states and the safety of their societies and individuals[28]. Like other international communities, Arab societies face transnational threats from cybercrime. The Arab League has consistently worked to strengthen legal, judicial and security cooperation among its members in combating crime and achieving criminal justice. This is being achieved through the coordination of their criminal policies and the establishment of legal mechanisms for organising Arab cooperation, as evidenced by their contributions and participation in all stages of the drafting of the United Nations Convention against Transnational Organised Crime through the proposals submitted at meetings of governmental experts[29].

CONCLUSION:

In conclusion, scientific and technological advances have greatly helped the international community to globalise information and simplify many services and operations. However, this progress is sometimes exploited to the detriment of the international community through the commission of serious and transnational crimes, such as cybercrime. Legislation must therefore keep pace with these developments and overcome the obstacles to international cooperation, while at the same time seeking to at least reduce these crimes.

In addition, international organisations, whether global or regional, have played and continue to play an important and prominent role in combating these serious crimes or at least reducing their prevalence.

REFERENCES:

- Al-Razi, IbnAbiBakr Muhammad Mukhtar Al-Sihah. Dictionary of Arabic Language. Dar Al-Maajim, Lebanon, Beirut, 1989.
- Amel, Qara. Cybercrime.Master's Thesis, University of Algiers, Faculty of Law and Political Science, Ben Aknoun, Algeria, 2002.
- Ayadi, Farida. Cybercrime in Algerian Legislation. Algerian Journal of Legal, Economic, and Political Sciences, University of Algiers 1, Faculty of Law, No. 2, 2018.
- Hamshashi, Amina. The Nature of Cybercrime. Presentation at the National Conference on Cybercrime at Mustafa Stambouli University, Mascara.
- Jendli, Warda. International Cooperation to Combat Cybercrime: Effectiveness and Challenges. Journal of Law and Political Science, Vol. 10, No. 2, 202.
- Khaled, Mamdouh. Cybercrime Security. New Publishing and Distribution House, Cairo, Alexandria, 2008.
- Kharshi, Othman. Extradition of Criminals as a Mechanism to Combat Cybercrime. Journal of Legal and Political Research, No. 10, University of MohamedBoularas, Saida, Algeria, 2018.
- Linda, Sharabsha. International and Regional Policy in Combating Cybercrime. Studies and Research Journal, Djelfa, No. 1, 2009.
- Maâchi, Samira. Cybercrime: An Analytical Study of the Concept of Cybercrime. Al-Mufakkir Journal, Mohamed Kheider University of Biskra, Faculty of Law and Political Science, No. 17, 2018.
- Nabilla, HibaHarwal. Procedural Aspects of Internet Crimes in the Evidence Gathering Stage: A Comparative Study. Dar Fikr Al-Jami, 2007.
- Naima, Fadila. Crimes Committed via the Internet and Legislative Means to Limit Them. Presentation at the National Conference on Information Security: Threats and Protection Methods, Previous Reference.
- Rbaïi, Hussein. Methods of Research and Investigation in Cybercrimes. Doctoral Thesis, Faculty of Law and Political Science, Specialization in Penal Law and Criminal Sciences, 2015.
- Talouz, Khelwat.Electronic Crimes: Their Combat System and the Challenges Reducing the Use of Modern Technology. Presentation at the National Conference on Information Security: Threats and Protection Methods, November 3-4, University of MouloudMammeri, TiziOuzou, Faculty of Arts and Languages.
- The Arab Convention on Combating Cybercrime was approved on December 12, 2010, by the Council of Arab Interior Ministers during their joint meeting at the General Secretariat of the League of Arab States in Cairo.
- The Budapest Convention was signed on 8/11/2001, ratified on 23/11/2001, and came into force in 2004, signed by 30 countries in the Hungarian capital "Budapest," including EU members, Canada, Japan, South Africa, and the USA. Naima, Fadila. Previous Reference.
- Yakar, Al-Taher. Cybercrime Between National Legislations and International Agreements. Al-Sada Journal for Legal and Political Studies, University of DjilaliBounaama, KhemisMiliana, Vol. 9, No. 1, 2022.

Footnotes:

[1]- Ayadi, Farida. Cybercrime in Algerian Legislation. Algerian Journal of Legal, Economic, and Political Sciences, University of Algiers 1, Faculty of Law, No. 2, 2018, p. 227.
[2]- Maâchi, Samira. Cybercrime: An Analytical Study of the Concept of Cybercrime. Al-Mufakkir Journal, Mohamed Kheider University of Biskra, Faculty of Law and Political Science, No. 17, 2018, p. 400.
[3]- Khaled, Mamdouh. Cybercrime Security. New Publishing and Distribution House, Cairo, Alexandria, 2008, p. 41.
[4]- Al-Razi, IbnAbiBakr Muhammad Mukhtar Al-Sihah. Dictionary of Arabic Language. Dar Al-Maajim, Lebanon, Beirut, 1989, p. 89.
[5]- Ayadi, Farida. Previous Reference, p. 228.
[6]- Same Reference, p. 228.
[7]- Rbaïi, Hussein. Methods of Research and Investigation in Cybercrimes. Doctoral Thesis, Faculty of Law and Political Science, Specialization in Penal Law and Criminal Sciences, 2015, p. 26.
[8]- Kharshi, Othman. Extradition of Criminals as a Mechanism to Combat Cybercrime. Journal of Legal and Political Research, No. 10, University of Mohamed Boularas, Saida, Algeria, 2018, pp. 919-920.

[9]- Maâchi, Samira. Previous Reference, p. 410.
[10]- Amel, Qara. Cybercrime.Master's Thesis, University of Algiers, Faculty of Law and Political Science, Ben Aknoun, Algeria, 2002, p. 25.
[11]- Ayadi, Farida. Previous Reference, p. 224.
[12]- Amel, Qara. Previous Reference, p. 25.
[13]- Hamshashi, Amina. The Nature of Cybercrime. Presentation at the National Conference on Cybercrime at Mustafa Stambouli University, Mascara, p. 454.
[14]- Talouz, Khelwat.Electronic Crimes: Their Combat System and the Challenges Reducing the Use of Modern Technology. Presentation at the National Conference on Information Security: Threats and Protection Methods, November 3-4, University of MouloudMammeri, TiziOuzou, Faculty of Arts and Languages, pp. 294-255.
[15]- Hamshashi, Amina. Previous Reference, p. 454.
[16]- Same Reference, p. 455.
[17]- Naima, Fadila. Crimes Committed via the Internet and Legislative Means to Limit Them. Presentation at the National Conference on Information Security: Threats and Protection Methods, Previous Reference, p. 256.
[18]- Jendli, Warda. International Cooperation to Combat Cybercrime: Effectiveness and Challenges. Journal of Law and Political Science, Vol. 10, No. 2, 202, p. 324.
[19]- Yakar, Al-Taher. Cybercrime Between National Legislations and International Agreements. Al-Sada Journal for Legal and Political Studies, University of DjilaliBounaama, KhemisMiliana, Vol. 9, No. 1, 2022, p. 15.
[20]- Nabilla, HibaHarwal. Procedural Aspects of Internet Crimes in the Evidence Gathering Stage: A Comparative Study. Dar Fikr Al-Jami, 2007, p. 153.
[21]- Naima, Fadila.Previous Reference, p. 258.
[22]- Linda, Sharabsha. International and Regional Policy in Combating Cybercrime. Studies and Research Journal, Djelfa, No. 1, 2009, p. 246.
[23]- Jendli, Warda. Previous Reference, p. 325.
[24]- The Budapest Convention was signed on 8/11/2001, ratified on 23/11/2001, and came into force in 2004, signed by 30 countries in the Hungarian capital "Budapest," including EU members, Canada, Japan, South Africa, and the USA. Naima, Fadila. Previous Reference.p. 295.
[25]- Linda, Sharabsha. Previous Reference, p. 247.
[26]- Yakar, Al-Taher. Previous Reference, p. 23.
[27]- Jendli, Warda.Previous Reference, p. 326.
[28]- The Arab Convention on Combating Cybercrime was approved on December 12, 2010, by the Council of Arab Interior Ministers during their joint meeting at the General Secretariat of the League of Arab States in Cairo.
[29]- Yakar, Al-Taher. Previous Reference,p. 17.