

Combating cybercrime in international law

مكافحة الجرائم الإلكترونية في القانون الدولي

ZAADI Mohamed Djelloul¹
m.zaadi@univ-bouira.dz

Received: 20/09/2025

تاريخ النشر: 2025/12/15

published: 15/12/2025

تاريخ الاستلام: 2025/09/20

Article abstract:

Cybercrime represents one of the most important contemporary challenges that members of the international community had to raise, given the danger it poses by virtue of the close link between it and the technological development that was embodied in particular in the expansion of the use of internet. From this point of view, no one is safe from the effects of this crime, from the simplest individual to the largest institutions, and even government. These practices include all areas of life, from the simplest to the most complex. The fait accompli explains the strenuous efforts made at the international and national levels to put an end to this phenomenon, and at the same time impose on countries to cooperate with each other in various fields to raise the challenge it pose to the safety and security of international community.

Key words : Cybercrime; Cyberspace; International treaties; International cooperation; Berne Convention.

ملخص المقال:

تمثل الجريمة الإلكترونية أحد أهم التحديات المعاصرة التي كان على أعضاء المجتمع الدولي رفعها، وذلك بالنظر إلى الخطورة التي تنطوي عليها بحكم الارتباط الوثيق بينها وبين التطور التكنولوجي الذي تجسد بشكل خاص في توسع إستعمال شبكة الأنترنت. ومن هذا المنطلق فلا أحد في مأمن من آثار هذه الجريمة من أبسط فرد إلى أكبر المؤسسات، بل وحتى الحكومات؛ إذ تشمل هذه الممارسات كافة مجالات الحياة، إنطلاقاً من أبسطها، إلى أكثرها تعقيداً.

يفسر الأمر الواقع الجهود الحثيثة المبذولة على الصعيدين الدولي و الوطني لوضع حد لهذه الظاهرة، وفرض في نفس الوقت على الدول التعاون فيما بينها في مختلف المجالات لرفع التحدي الذي تمثله على سلامة و أمن المجتمع الدولي.

كلمات مفتاحية: الجريمة الإلكترونية؛ الفضاء السيبراني؛ الاتفاقيات الدولية؛ التعاون الدولي؛ إتفاقية برن.

1. akli m'hand oulhadj university-bouira Algeria

Introduction

In recent years, the world has witnessed a qualitative leap in the field of modern technologies, perhaps most notably the widespread use of the internet, whose application has become inevitable in various aspects of life, including the simplest ones. Its use has increased in the economic, social, and cultural spheres. This development has not always been synonymous with a positive outlook. On the contrary, the qualitative leap in this field has been accompanied by the development of criminal behavior, which has found in this means a tools of easy access to individuals' data and a means of violating the privacy of their lives, and even more than that, a means of stealing their money and threatening their lives. Thus, crime has become more powerful thanks to modern technology.

Most criminal law experts agree that combating cybercrime is one of the most significant challenges facing the international community, given its departure from traditional forms of crime. Furthermore, the fact that this type of crime is committed in cyberspace makes identifying the perpetrator and addressing the actions involved difficult, if not impossible, to achieve. This requires innovation and creativity from relevant authorities to keep pace with the evolution of criminal behavior in such cases.

The rise of this type of crime has drawn the attention of various members of the international community, regardless of their technological advancements. These communities have worked to find a radical response to put an end to this phenomenon, which is not confined to the territorial borders of a particular State, but rather encompasses all States, regardless of their level of technological development. This has been embodied on the ground at the legislative level, with international efforts multiplied to enact international treaties and conventions that address the issue of cybercrime, identifying its forms and the most effective means of combating it and limiting it to the narrowest possible limits.

Importance of the study:

The current study's importance can be derived from a number of points:

- The widespread prevalence of cybercrime, as it is a cross-border crime, given that cyberspace is not restricted by specific borders. It is also easy for anyone to engage in such practices. All a person needs to do is acquire a computer, connect it to the internet, and download specific programs to be able to commit this crime;

- The rapid development of practices associated with cybercrime has paralleled the development of modern technologies, which have flourished in recent years, with the proliferation of electronic applications and programs that can be downloaded from various virtual sites;

- The intangible nature of this type of crime, as there is no crime scene, no instrument of crime, and not even a tangible weapon;

Study Objectives:

The current study aims to achieve a set of objectives, perhaps the most important of which are:

- Identifying the features of cybercrime within the framework of international legal texts, thus shedding light on its characteristics and distinguishing it from other similar practices;
- Identifying the elements required to commit this type of crime, given its specific nature;
- Identifying the types of practices in which cybercrime is embodied in reality;
- Illustrating the approach adopted internationally to address the phenomenon of cybercrime.

The problematic:

Cybercrime has been the subject of controversy and debate at various levels, both legally and doctrinally, which leads us to ask the following problematic:

To what extent are the measures adopted internationally to combat the phenomenon of cybercrime effective?

Scientific methodology:

This study relied on a number of scientific methods, perhaps the most important of which is the descriptive approach, which is particularly relevant within the theoretical framework related to the definition of cybercrime in the various international treaties and conventions enacted in this regard. It also examines the measures taken to combat this cross-border phenomenon, as well as the forms in which practices associated with cybercrime are embodied. The historical method was also used to demonstrate the development of this phenomenon, while the analytical method was used to study the provisions contained in international treaties, and criticize their content.

Study Division:

We decided to divide the current study into two complementary axes. In the first, we address the conceptual framework of cybercrime, listing the definitions attributed to this concept, along with its associated characteristics and the types that branch off from it. The second axis, meanwhile, is devoted to the measures included in the legal system designed to combat cybercrime, whether those contained in relevant international treaties or those emanating from the work of the United Nations.

1. The concept of cybercrime

Recent years have witnessed a significant development in the methods used to commit crimes. These crimes are no longer confined to traditional methods that rely on familiar tools such as bladed weapons or firearms. Today, they are committed using advanced technological methods such as computers, smartphones, software, and electronic applications.

Given the importance of this topic, efforts have increased to shed light on this concept, both on the technical and legal level (1.1), which in turn led to a distinction between two distinct types of practices associated with this phenomenon (1.2).

1.1. Definition of Cybercrime:

Cybercrime represents one of the most significant contemporary forms of crime, and local authorities in any country seek to combat it through various means. In their quest to achieve this goal, they face a number of difficulties, perhaps the most significant of which is the ambiguity surrounding this concept, given its similarity to other concepts. This has sparked a movement at the doctrinal and legislative levels to shed light on its meaning (1.1.1), and subsequently define its characteristics (1.1.2).

1.1.1. The significance of Cybercrime:

The concept of cybercrime did not emerge directly, nor was it first referred to under this name. The concept of “computer crime,” or “crime committed by computer,” was proposed by a group of experts from the Organization for Economic Cooperation and Development in Paris in 1983. They defined it as: “Any illegal, unethical, or unauthorized behavior that affects the automated processing of data and/or the transmission of data” (Cernomoret & Andrei, 2023, p. 12).

Definitions attributed to cybercrime are diverse and varied, depending on the perspective used to define cybercrime. Some define it based on its technical nature, such as Professor (Olukunle Oladipupo and others), who views it as a criminal act that uses a computer as its primary tool in its preparation, and execution, and its purpose is to threaten interests of other individuals and institutions, whether public or

private (Amoo, Akoh, Temitayo, Oleuvatoyin, Femi, & Benjamin, 2023, p. 207), therefore, this approach attributes to the means, technology and knowledge that the criminal relies on a fundamental position in committing the criminal act, and this is what is confirmed by the jurist (JIANG PING), who limits it to: a crime of a material nature, represented by every unlawful act or behavior, through the use of electronic media, which causes the victim to bear or be able to bear a loss, and the perpetrator to obtain or be able to obtain any gain, and these crimes aim to illegally access confidential data that is not permitted to be viewed, transferred, copied or deleted, or to threaten and blackmail the persons and entities concerned with that information, or to destroy the data and computers of others by means of viruses (Ping, 1995, p. 33). This is confirmed by (Ishan Atrey), who believes that every illegal act requires a great deal of knowledge of computer technology to commit it, on the one hand, and to pursue and investigate it, on the other hand (Atrey, 2023, p. 185).

1.1.2.Characteristics of Cybercrime:

Cybercrime is distinguished from other traditional crimes by a number of aspects, perhaps the most important of which are that which relates to the identification of the person that committed the crime (1.1.2.1), or that which relates to the area in which the crime was committed (1.1.2.2), or the scope of the latter (1.1.2.3), or the difficulties faced by the authorities concerned in confronting this type of crime (1.1.2.4), as follows:

1.1.2.1.Regarding the perpetrator of the crime:

This person is often trained in the field of computer science and possesses advanced knowledge in the field, such as an engineer in this field. Therefore, not just anyone could engage in this type of activity (E.F.G, 2016, p. 3).

1.1.2.2.In terms of the scope of the crime:

While traditional crimes affect individuals in their property, money, and even their persons, cybercrimes also affect these areas, but in cyberspace, by intercepting and hacking their data and violating the privacy of their lives through the photos and videos they store on their computers and smartphones (Chowbe, 2011, p. 7).

1.1.2.3.The transnational nature of cybercrime:

Because cyberspace is borderless, the commission of cybercrime is also borderless. A person from Algeria may hack the data of another person or company located in the United States using their computer, even without moving from one location to another (Hadi, 2023, p. 1584).

1.1.1.4.The difficulty of combating cybercrime:

This is primarily due to the technical nature of this type of crime. It is difficult to prove the commission of this crime because it does not require the use of violence, but rather is carried out using electronic programs. It requires a high level of technical knowledge for the competent authorities to examine it. Furthermore, it is difficult to detect the perpetrators due to its cross-border nature, in addition to the ease with which evidence can be erased (Nuredini, 2014, p. 597).

1.2.Types of Cybercrime:

The scope of cybercrime is broad, given its penetration into various aspects of life, including economic, social, cultural, and even security-related issues. As such, this crime has attracted the attention of criminologists, who, in their analysis of this phenomenon, have distinguished between two distinct types of practices that manifest themselves in real-life situations: crimes targeting individuals, such as data hacking

(1.2.1), and crimes that affect society as a whole and are specific to State security, such as cyberattacks (1.2.2).

1.2.1. Crimes targeting individuals:

Recent years have witnessed a proliferation of social media sites. Originally designed to bring people together, whether friends or family members, these platforms have quickly become targets for illegal and unethical practices that often damage the reputation and honor of individuals. Police departments record daily complaints related to slander, defamation, and libel on social media, along with more serious forms of harassment, threats, and stalking. This is in addition to identity theft, which involves the creation of fake accounts that help perpetrators deceive and lure individuals into the trap of exploitation (Bhandari, 2024, pp. 119-120).

1.2.2. Crimes against State Security:

Electronic tools, including software and applications, have become just as deadly and dangerous as bombs, mines, and missiles. Evidence has demonstrated on more than one occasion the use of cyberattacks prior to the outbreak of conventional armed conflict. These tools are typically used to deprive an adversary of essential resources for waging war, such as targeting power plants and communications networks. These tools, in turn, deprive the opposing party of the means to coordinate its defense or offensive operations against the adversary (Islam, 2017, p. 103).

The dangers of these practices are embodied in other forms, perhaps the most significant of which is the propaganda disseminated by some terrorist organizations to attract new members to bolster their ranks, as was done by the Islamic State in Iraq and Syria (ISIS) beginning in 2011 (Lux, 2018, p. 19). Organized criminal organizations also resort to such methods, which allow them to easily plan, pass on, direct, and execute criminal schemes on the ground. They are also used to facilitate espionage operations undertaken by some individuals to achieve military, political, or economic objectives on behalf of a competing company (Broadhurst, peter, mamoun, brigitte, & steve, 2014, pp. 5-6).

It is worth noting in this regard that cybercrime is widely used in relation to financial crimes, the latter of which affects individuals and the State simultaneously. It is embodied on the ground in its simplest forms in stealing credit card numbers and transferring sums of money illegally, while it is manifested in its most complex forms in the crime of theft and robbery of bank funds, whose internal systems are hacked, and customer data is modified and affected (Nicholls, aditya, & nhien-an, 2021, pp. 6-20).

2. Addressing cybercrime in international law

Given the serious harm caused by cybercrimes, public authorities have increasingly focused on this type of practice. These authorities have worked to develop means to combat it. However, most of these measures have limited their effectiveness due to the cross-border nature of the practices involved, requiring concerted efforts from various countries to confront them. This is a conclusion reached by members of the international community in international treaties and conventions concluded in this field (2.1), or resulting from the work of the United Nations in various relevant conferences and meetings that followed (2.2).

2.1. In related international treaties and conventions:

Cybercrime is primarily considered a cross-border crime. As such, it is not surprising to note the active international efforts to combat it, whether through the adoption of preventive measures or the imposition of penalties on perpetrators, whether isolated individuals or organized groups. Indeed, members of the

international community have undertaken numerous initiatives in this regard, perhaps the most important of which is the Berne International Convention for the Protection of Literary and Artistic Works (2.1.1), or even within the framework of the 2001 Budapest Convention on the Prevention and Punishment of Cybercrime (2.1.2).

2.1.1. The Berne Convention for the International Protection of Literary and Artistic Works:

The Berne Convention represents one of the most important legislative mechanisms designed to effectively protect authors' rights. The founders of this convention were concerned with the harm authors suffer from infringement of the rights to their literary and artistic works. Although this convention was enacted in 1886, its provisions were subject to amendments from 1896 until 1971 to keep pace with developments in this field (Gervais, 2011, pp. 154-156).

The drafters of this convention devoted a special section to computer-related crimes, and in its preamble, they recognized the need to develop international means and methods to encourage cooperation between States in the criminal field to combat this phenomenon (works, 1979, p. preambular para.1). While they included in the practical paragraphs of this convention measures that are supposed to put an end to this type of practice, they began its provisions by emphasizing the need to develop States' efforts to combat this phenomenon and to move from an individual, isolated approach to a multilateral approach (works, 1979, p. Article 2 para.7), in addition to intensifying the efforts of member States to combat cybercrime in all its forms by defining their relevant legal framework, particularly by including a detailed list of crimes that fall under this description, and amending the capabilities available to security services in each State related to investigation and prosecution, in addition to the extradition of criminals through the conclusion of bilateral treaties. In this regard, it is noteworthy that the Organization of States in the Convention emphasizes preventive measures, given the close link between these practices and respect for human rights and fundamental freedoms (works, 1979, p. Article 6).

2.1.2. The 2001 Budapest Convention on Combating Cybercrime and Communications:

This convention has been widely ratified by members of the international community, aware of the seriousness of cybercrime. The most important feature of the approach adopted in this instrument is its preference for deterrent measures over preventive measures. The convention aims to align the elements and components of the criminal law applicable in any country with the specificity of cybercrime, including the procedural aspect of criminal prosecution of those involved in such acts, as with other crimes. It also aims to establish effective and rapid cooperation between countries (Europe, 2025, p. para.8). Indeed, with regard to the criminal code applicable in any member State, the Convention recommends defining 9 crimes classified into 4 different categories, specifying responsibility for each one, in addition to the corresponding penalties. The Convention defines the following crimes: unlawful intrusion and access (Europe t. C., 2001, p. article 2); unlawful interception (Europe t. C., 2001, p. Article 3); data interference (Europe t. C., 2001, p. Article 4); system interference (Europe t. C., 2001, p. Article 5); misuse of equipment or devices (Europe t. C., 2001, p. Article 6); computer-related photography or forgery (Europe t. C., 2001, p. Article 7); computer-related fraud (Europe t. C., 2001, p. Article 8); crimes related to the exploitation of children in pornographic materials (Europe t. C., 2001, p. Article 9); and crimes related to copyright and related rights (Europe t. C., 2001, p. Article 10).

At the procedural level, the second section of Chapter Two of the Convention requires the application of the common conditions and safeguards applicable to all procedural measures normally applied to similar

crimes, when the crime is committed using a computer system or when the evidence related to it is in electronic form. These measures must include:

- Expedited preservation of stored data, including traffic data, and partial disclosure thereof;
- Ordering the production of data;
- Searching for and confiscating computer data;
- Collection of traffic data in real time;
- Intercepting content data (Europe t. C., 2001, p. Article 14).

These measures are consistent with the nature of cybercrime, characterized by its flexibility, difficulty in detection, and ease of falsification and even concealment (Clough, 2014, p. 704).

2.2. In the initiatives of the United Nations Organization:

The United Nations represents one of the primary bodies dedicated by the members of the international community to protecting international peace and security. It was no surprise that the issue of combating cybercrime captured the attention of its members. The global international organization has organized numerous events to study and analyze this cross-border phenomenon and enact the necessary measures to effectively combat it.

Reference in this regard is, of course, to the work and decisions emanating in this regard from the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Prisoners, held in Havana in 1990, on computer-related crimes (2.2.1), and then the meeting of the Working Group on Cooperation, held in Vienna on 27 and 28 October 2015 (2.2.2).

2.2.1. The 1990 Havana Conference:

The conference's drafters addressed the issue of combating cybercrime in the second section of the document that emerged from it. In the preamble to the document, the conference participants acknowledged that the misuse of communication technologies has spread nationally and internationally, and that this has the potential to negatively impact all areas of life due to the interconnectedness created by the widespread use of the Internet (the United Nation Organization, 1990, p. preambular paras 1 and 2).

The legal framework adopted in this regard consists of preventive measures, including the need for local authorities in each country to adopt legislation to combat cybercrime, and the establishment of mechanisms to ensure the implementation of this framework on the ground, in addition to raising public awareness of the risks posed by, for example, social networking sites, or the neglect of effective protection of personal data in cyberspace, particularly through the inclusion of passwords and the downloading of programs that prevent hacking of systems (the United Nation Organization, 1990, p. Active Para. 2(a) and (b)). On the deterrent level, one of the most important points mentioned in the conference was that expanding the scope of criminal law applicable in any country is not sufficient to address the challenges posed by this phenomenon, particularly through the creation of new crimes. Rather, it is necessary to identify each form in which cybercrime is embodied, and to program the penalties applied to each one, as we indicated above (the United Nation Organization, 1990, p. Active Para. 4).

2.2.2. Meeting of the Working Group on Cooperation, held in Vienna on October 27 and 28, 2015:

The document resulting from this meeting represents one of the most important steps taken to combat this phenomenon. In its decision 2/2, the Conference of the Parties to the United Nations Convention against Transnational Organized Crime decided to establish a meeting in Vienna on October 27 and 28, 2015, to study various topics related to cooperation in criminal matters, particularly those related to cybercrime. The

added value of this meeting lies in its composition by a group of experts focused on the most intricate aspects of the crime. They pointed out that the challenge of this phenomenon can be overcome by covering all its aspects, starting with the terminological aspect, where they show, for example, that the use of the terms digital evidence and electronic evidence does not affect any country's policy in combating this phenomenon, as long as they are used naturally in the legislative systems of these member States. However, the participants highlighted the barrier of jurisdiction and how to determine the country competent to consider this type of crime, which is hindered by another obstacle represented by requesting relevant information from internet service providers or requesting that they store data with them, and the procedural and legal requirements necessary for that (cooperation, 2015, p. Paras. 4 and 5).

One of the most important recommendations made in this area is the need to support technical assistance efforts, including those undertaken by the United Nations Office on Drugs and Crime, aimed at developing training programmes to improve the capabilities of local law enforcement personnel, including those authorized to carry out the duties of liaison officers, and judges specialized in adjudicating this type of practice, and to enhance their knowledge in this field at the technical and legislative levels, especially with regard to the conditions for the admissibility of evidence before courts in this area (cooperation, 2015, pp. Part II. Recommendations, Para.2(f)).

Conclusion:

It is evident from what was mentioned above that cybercrime, like other crimes, requires a set of conditions to be criminalized and removed from the realm of international law. However, its specific nature, resulting from the means by which it is committed, makes it a phenomenon that national legislators cannot effectively combat without external assistance from their counterparts in other countries. Recent years have demonstrated that cybercrime has become one of the most widely used practices by criminal organizations, which seek to generate the greatest profits while employing the least possible resources.

The above study leads to a number of conclusions, perhaps the most important of which are:

-Cybercrime is one of the most difficult crimes to detect, given its intangible environment, in addition to the fact that most countries lack the technical means to combat this phenomenon;

-Cybercrime is a cross-border crime, and as such, it is impossible for local authorities in a given State to effectively combat this phenomenon without resorting to the assistance and cooperation of foreign authorities in other countries;

-Despite the diversity and multiplicity of legal texts adopted internationally to combat the phenomenon of cybercrime, their impact remains limited as long as their effectiveness and efficacy depend on the willingness of member States to cooperate in this area.

Through the above-mentioned, legal gaps were highlighted, which can be filled through the following:

-The need to establish special units tasked with combating cybercrimes of all kinds. This, in turn, requires national legislation to adopt a special budget to support this type of program;

-The need to update the various existing international treaties and conventions to take into account current developments in the field of cybercrime;

-The necessity of concluding international treaties to combat cybercrime. This would be an inevitable step towards coordinating international efforts at various levels, whether on the ground, through raids and

seizures carried out by authorities in various countries, for example. This would also be positive at the judicial level, as judicial bodies pursue prosecutions against individuals involved in such practices.

-The necessity of incorporating research into the core of the policy adopted to combat cybercrime, by supporting laboratories and research centers in developing research programs that help countries protect their internal systems from practices associated with cybercrime, such as hacking, etc.

Sources and references

- Amoo, O. O., Akoh, A., Temitayo, O. A., Oleuvatoyin, A. F., Femi, O., & Benjamin, S. A. (2023). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *world journal of advanced research and reviews*, 21(02).
- Atrey, I. (2023, July). Cybercrime and its legal implications: analysis the challenges and legal frameworks surrounding cybercrime, including issues related to jurisdiction, privacy, and digital evidence. *International journal or research and analytical review*, 10(03).
- Bhandari, R. (2024, April). Cyber law and cybercrime- A comprehensive study. *international journal of novel research and development (IJNRD)*, 9(4).
- Broadhurst, R., peter, g., mamoun, a., brigitte, b., & steve, c. (2014, march). Organization and cybercrime: An analysis of the nature of groups engaged in cybercrime. *international journal of cyber criminology*, 8(1).
- Cernomoret, S., & Andrei, N. (2023). *Comparative analysis of cybercrime in the criminal system*. Budapest, Paris, Calgary: AdJURIS International academic publisher.
- Chowbe, V. (2011, February). The concept of cyber-crime: nature and scope. *SSRN electric journal*.
- Clough, J. (2014). A world of difference: The Budapest convention on cybercrime and the challenges of harmonization. *monash university law review*, 40(3).
- cooperation, t. w. (2015). *Part III Summary of deliberations-A. Gathering and sharing electronic evidence-Paras. 4 and 5*. conference of the parties of the United Nations convention against transnational organized crime, conference of the parties of the United Nations convention against transnational organized crime. vienna: conference of the parties of the United Nations convention against transnational organized crime.
- E.F.G, A. (2016, August). Challenges to enforcement of cyber-crimes laws and policy. *Journal of internet and information systems*, 6(1).
- Europe, C. o. (2025). *Convention on Cybercrime*, . Explanatory report, Strasbourg.
- Europe, t. C. (2001, November 23rd,). the convention on cybercrime. *the convention on cybercrime*(,N°185). Budapest, Budapest, -Hungary: European treaty Series,.
- Gervais, D. J. (2011). Golan v. Holder: A look at the constraints imposed by the Berne convention. *Vanderbilt university law school*, 64(147).
- Hadi, Z. H. (2023). cross-border cybercrime. *Russian law Journal*, XI(3).
- Islam, M. S. (2017, June). Cyber warefare and international humanitarian law: a study. *International Journal of ethics in social sciences*, 5(1).
- Lux, L. M. (2018). defining cyberterrorism. *revista chilena de derecho y tecnologia*, 7(2).
- Nicholls, J., aditya, k., & nhien-an, l.-k. (2021, december 8). financial cybercrime: a comprehensive survey of deeplearning approaches to tackle the evolving financial crime landscape. *IEEE access*, PP.
- Nuredini, A. (2014, August). Challenges in combating the cyber-crime. *mediterranean journal of social sciences*, 5(19).
- Ping, J. (1995). Exploring computer crime. *Policing studies*(4).
- the United Nation Organization. (1990, 27 August- 7 september 27 August- 7 september). Eighth united Nations congress on the prevention of the crime and the prevention of crime and the treatment of offenders. *Eighth united Nations congress on the prevention of the crime and the prevention of crime and the treatment of offenders*. Havana, Havana, Colombia.
- works, B. c. (1979, september 28). Berne convention for the protection of literary and artistic works. *Berne convention for the protection of literary and artistic works*. berne, berne, switzerland.