LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S6(2025)

ELECTRONIC CRIMES IN INTERNATIONAL LAW: INTERNATIONAL EFFORTS TO COMBAT THEM AND CURRENT CHALLENGES

Dalal Sadiq Ahmed[1], Ilham Hashim Abdulghani[2], shaymaa majeed rashed[3], Ahmed Y. Alasadi[4]

[1]Northern Technical University, Polytechnic College Kirkuk
[2] Middle Technical, University (MTU)
[3] RenewableEnergy Research Center / Northern Technical University
[4]College of Nursing, University of Al-Ameed, Karbala PO Box 198, Iraq.

dalal-sadiq@ntu.edu.iq[1]
ilhamhashems@mtu.edu.iq[2]
shymaa.m@ntu.edu.iq[3]
ahmedyaa@alameed.edu.iq[4]

Abstract:
There is no longer any economic, social, Industrial, or administrative field in which information technology does not play a central role in performance and development. As a result of this progress in the world of informatics, new patterns of crime have emerged and expanded, attracting international attention to combating them due to their extremely dangerous negative impacts. This has necessitated serious efforts to confront such crimes. Many countries have enacted laws criminalizing these acts and prescribing penalties for them; however, these individual efforts have revealed legislative gaps and practical shortcomings In the mechanisms for combating such crimes. This Is natural given the unique nature of cybercrimes, which transcend geographical borders on the one hand, and are characterized by rapid technological advancement and wide-scale spread across all aspects of life on the other. Consequently, the developments in the field of Information technology have made international cooperation essential to addressing cybercrimes. It is no longer a matter of choice but rather an Inevitable necessity in the absence of alternative solutions.

Keywords: International efforts, International cooperation, Internet, computer, cybercrimes, difficulties, challenges.

1 Introduction:

The emergence of the computer and the Internet is considered one of the most remarkable achievements of modern science and among the most influential on human life. Information and communication technology has brought about numerous benefits In various fields such as economy, education, medicine, and others. Alongside these achievements, however, a new group of experts has emerged—individuals possessing the skills needed to exploit these technologies In committing crimes. This has led to the transformation of traditional crime Into new forms that rely on modern technology, with such crimes now being carried out in innovative ways previously unknown.

The rapid development of information technologies has enabled these criminals to expand the scope of their offenses, posing a significant threat to information systems. They are now capable of paralyzing both civilian and military systems, disabling electronic equipment, Infiltrating banking systems, disrupting air traffic, and crippling power stations—using “information bombs” transmitted through a computer keyboard from great distances, leaving no trace by which they could be tracked. Thanks to these modern technologies, criminals can reach any place they desire via the internet and communicate with anyone worldwide, making the world seem like a small village.

Therefore, it has become essential for different legislations to keep pace with this remarkable rise In cybercrimes. Addressing such crimes requires nontraditional legal frameworks to confront the diverse forms of computer crime, including unauthorized access to networks, data destruction, document forgery, attacks on banks, spreading rumors, pornography, and other cyber offenses. States and the International community have recognized the seriousness of these crimes, their ease of commission, and their direct impact—making the fight against them a top priority for governments and the global community alike. Since internet crimes are transnational in nature, International cooperation In combating them Is one of the most Important mechanisms In criminal policy. It plays a key role In harmonizing national legislations and strengthening mutual legal and judicial assistance between states In detecting these crimes and prosecuting their perpetrators. For this reason, the Intervention of the International community has become a necessity In addressing this type of crime.

2 – International Efforts to Combat Cybercrime in International Law

Cybercrime is a criminal activity In which computer technology is used, directly or indirectly, as a tool or a target to commit the Intended criminal act. Due to the special nature of computer data, being intangible, and because of the problems raised by the judicial application of criminal law provisions to computer crimes, and In order to prevent offenders from escaping justice as a result of Insufficient or inadequate laws to address these newly emerging crimes, and to safeguard the principle of legality—which stipulates that there is no crime and no punishment without a legal provision—and in light of the prohibition of analogy In substantive criminal law, many countries around the world have enacted specific criminal laws or amended their penal codes. These laws ensure the confrontation of computer crimes that target computer data, Information, and software.

Accordingly, it has become essential for countries to cooperate In combating this new type of crime, whichh is no longer confined to a particular state or directed at a specific community. Instead, it transcends borders, inflicting harm on multiple countries and societies by exploiting the rapid advancement of modern technological means in communication and transportation. The International community has responded to this criminal phenomenon with a set of legislations through treaties and conventions[(1)].

2.1. The Role of International Conventions in Combating Cybercrime"

- **General Frameworks for International Cooperation in Combating Cybercrime**

The rapid acceleration of technological progress and the emergence of cyberspace have triggered a comprehensive revolution that has affected various aspects of life, making electronic services an indispensable element. However, these modern technologies have also provided a fertile environment for some to engage in unlawful activities. Since cyberspace transcends geographical borders and does not recognize state sovereignty, it has become difficult for any single country to establish an adequate legal framework to confront these emerging crimes. Hence, the need arises to develop the international legislative system, along with devising new pathways and mechanisms for international cooperation—whether through enhancing traditional

[(1)] Mahmoud Mohamed Safaa El-Din Ali Shershar, International and Legislative Efforts to Combat Internet Crimes, Faculty of Law, Menoufia University, no publication year, p. 527.

tools or by creating advanced mechanisms that keep pace with the rapid evolution of these crimes and contribute effectively to addressing and combating them(1)

- **Judicial Cooperation**

Investigations and judicial proceedings in cybercrime cases require tracking criminal activity at all stages, from its source to the moment of execution, while identifying the locations affected. Since these elements may be spread across several countries, prosecuting perpetrators of such crimes necessitates effective judicial cooperation among the competent authorities in those countries. This enables the expansion of jurisdiction and helps overcome the cross-border nature of these crimes.

- **Security Cooperation**

It is clear that geographical borders and the issue of territorial jurisdiction constitute major obstacles to criminal procedures related to prosecuting offenders, especially in cybercrimes of a transnational nature. A perpetrator may be a citizen of one country, executing his attack from the territory of another, while the effects of his crime appear in a third country.(2)

Here emerges the urgent need to unify efforts and exchange data and information related to cybercrimes, in order to uncover the identity of perpetrators. It is impossible for any single country to eradicate this phenomenon alone. Security authorities cannot pursue criminals outside their national borders, which allows perpetrators to escape prosecution as soon as they leave a country's territory(3).

In this context, three main forms of security cooperation can be identified:

1. Establishment of specialized offices tasked with gathering information on cybercriminals and sharing it among states, with the aim of enhancing cooperation between judicial and security authorities, tracking offenders through data exchange, and providing technical support and expertise when needed.
2. Cooperation through INTERPOL: The International Criminal Police Organization works to strengthen cooperation among police forces in member states to combat crime effectively, by collecting and exchanging data on criminals and crimes via national central bureaus of international police in each state, as well as coordinating the arrest of criminals with the assistance of security agencies across member states(4).
3. Joint security operations, involving the direct pursuit of cybercrimes through tracking and seizing digital evidence, conducting cross-border searches of information systems, devices, and networks in search of proof. Such operations require intensive international cooperation at both the security and technical levels, and they also contribute to developing the capacities and expertise of personnel in the field of cybercrime combating.

- **International Judicial Assistance**

International judicial assistance is defined as all judicial procedures carried out by one state in order to facilitate trial proceedings in another state regarding a specific crime. The general principles governing the obligation of mutual legal assistance can be

(1) Qazran, Mustafa. International Mechanisms to Combat Cybercrime, Sawt Al-Qanoun Journal, Vol. 8, No. 2, Algeria, 2022, p. 1225.

(2) Hussein Al-Ghafari. International Efforts in Confronting Cybercrime, published on www.cip.org.sa/vb/sharthread.php3697, accessed 22-09-2025.

(3) Hilali Abd Al-Lah Ahmed. The Budapest Convention on Cybercrime, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 2007, p. 327.

(4) Hilali Abd Al-Lah Ahmed, ibid., p. 328

inferred from paragraph 1 of Article 25 of the Budapest Convention on Cybercrime, which stipulates that such assistance should be available to the greatest possible extent, be comprehensive and broad, and minimize obstacles.(1)

Judicial assistance takes several forms, including:

1. Information exchange: This involves sharing data, documents, and evidence requested by a foreign judicial authority during the examination of a crime prosecuted against one of its nationals or the nationals of another state. It also includes sharing the criminal records of offenders in such crimes. There are many applications of this, such as those in paragraphs 6 and 7 of Article 1 of the UN Model Treaty on Mutual Assistance in Criminal Matters, and paragraphs 3 and 4 of Article 8 of the UN Convention against Transnational Organized Crime.
2. Transfer of proceedings: This means that a state, pursuant to a convention or treaty, undertakes a set of criminal procedures regarding a crime committed in the territory of another state, in the interest of that state. This is subject to conditions, the most important of which is dual criminality—that the act must be criminalized in both the requesting and the requested states. The requested procedures must also be lawful under its legal system and sufficiently serious to contribute to uncovering decisive facts about the crime. Many treaties recognize this, including the UN Model Treaty on the Transfer of Proceedings in Criminal Matters, Article 21 of the UN Convention against Transnational Organized Crime, and Article 23 of the Budapest Convention on Cybercrime.

In all cases, where dual criminality is applied, it should be done flexibly to ensure the facilitation of judicial assistance(2).

3. International letters rogatory: This refers to judicial procedures within criminal proceedings aimed at deciding a specific matter before the judicial authority, when the requesting state cannot do so on its own. Judicial letters rogatory facilitate criminal procedures between states by ensuring the necessary investigations are conducted to bring offenders to trial, thus overcoming the obstacle of territorial sovereignty that prevents foreign states from conducting judicial activities on another state's territory (such as investigations, inspections, searches, or witness hearings). Such requests are usually transmitted via diplomatic channels, but in order to simplify and expedite procedures, many states have begun appointing a central authority—often the Ministry of Justice—to receive requests directly(3).

In the field of judicial cooperation, it can be concluded that such cooperation constitutes one of the most important mechanisms for combating cybercrime. However, most conventions addressing this issue have dealt with cybercrime superficially and without depth. Hence, there is a pressing need for conventions that keep pace with the rapid developments in information and communication technologies, particularly since speed is an essential factor in confronting cybercrime. This trend can be observed in a number of conventions concluded at both the international and regional levels, which have addressed cybercrime as a principal and exclusive matter.(4)

(1) Hilali Abd Al-Lah Ahmed, ibid., p. 332.
(2) Qazran, Mustafa, ibid., p. 1228.
(3) Qazran, Mustafa, ibid., p. 1228.
(4) Qazran, Mustafa, ibid., p. 1228.

2.2 International Cooperation in Training to Combat Cybercrime

The emergence of new forms of crime, represented by cybercrimes such as hacking and other technological crimes, has placed a burden on justice institutions of all kinds due to the distinctive characteristics of cybercrimes compared to traditional crimes. Therefore, security agencies must bear full responsibility toward these crimes and achieve justice. To achieve this, these agencies, in all their forms, must possess a high degree of competence and skill in uncovering the ambiguity of such crimes and identifying perpetrators with great speed and accuracy. This can only be achieved through training, which highlights the importance of international cooperation in this field.(1)

- **The Importance of Training Officials in Cybercrime Enforcement Agencies**

Training in the field of combating cybercrime has become an investment tool that administrative organizations usually resort to in order to achieve their objectives. It is a vital element for building renewed expertise and skills. In fact, training has come to play an important role in modern human life(2).

Attention to training in its various technical aspects has increased and become a necessity in the lives of most people—whether for the trainee or for the organization providing the training. Whether the organization is civilian, military, governmental, or private, or whether it works in the justice sector or elsewhere, training is one of the basic elements for enhancing human resource efficiency, boosting productivity, and achieving comprehensive development. The purpose of training is to introduce fundamental changes in the behavior of trainees, reflected in how they perform their assigned tasks more effectively after the training process(3).

Training is also the most practical and effective means of benefiting from the skills and experiences of others through qualified individuals. The training referred to here is specialized technical training that equips individuals with advanced technical expertise in the field of cybercrime. Such expertise cannot be achieved without specialized training that takes into account the trainee's personal capabilities, including academic qualifications and intellectual capacity to absorb the training(4).

It is often easier to train specialists in information technology and communication networks than to train law enforcement officers such as police or prosecutors. Some experts argue that trainees should have no less than five years of experience in IT-related fields such as programming, systems design and analysis, network management, and computer operations. The training curriculum must include an explanation of risks, threats, vulnerabilities, and potential breaches of information networks and computer systems. It should also cover concepts and definitions related to the traits of cybercriminals and the motives behind committing cybercrimes. Training programs should be tailored according to their type—whether through seminars, workshops, or study groups—and should foster active interaction among

(1) Sulaiman Abu Namer, Combating Cybercrime within the Framework of International Law, Master's Thesis, Faculty of Law and Political Science, Department of Law, Mohamed Khider University of Biskra, Algeria, 2020, p. 37.
(2) Ghanem Mardhi Al-Shammari, Cybercrimes, 1st Edition, Dar Al-Thaqafa, Amman, Jordan, p. 115.
(3) Adel Abdel-Aal Ibrahim Kharashi, Challenges of International Cooperation in Combating Cybercrime and Ways to Overcome Them, 1st Edition, Dar Al-Jami'a Al-Jadida, Alexandria, 2015, p. 23.
(4) Ghanem Rady Al-Shammari, op. cit., p. 22.

participants to analyze case studies and exchange scientific expertise on handling and using computers.

Training can be individual or team-based, with groups of trainees working together as teams. Teams should undergo practical experiences, including exposure to real-world cybercrime cases previously investigated, ensuring variety in these cases to provide participants with the necessary expertise. Such training requires specialized institutions with sufficient expertise to carefully select trainees who possess strong technical knowledge, scientific background, and distinctive personal qualities(1).

Training must also be continuous, as cybercrimes evolve rapidly. Security agencies responsible for investigations should enlist IT specialists and experts, for example, through police academies that recruit IT graduates as officers trained in both law and technology. Similarly, law faculties should integrate computer science into their curricula, ensuring that graduates acquire both legal and technological knowledge(2).

- **Aspects of International Cooperation in Training Criminal Justice Officials**

Justice institutions in many countries are often unprepared to confront computer-related crimes and other rapidly evolving modern crimes. Since no country can succeed in addressing such emerging crimes alone without cooperation and coordination, there has been a call for international collaboration in this field, particularly regarding mutual legal assistance, extradition of criminals, and training of justice officials. Several international and regional conventions have explicitly stressed the importance of cooperation between states in training and knowledge exchange, such as Article 9 of the Draft Arab Convention on Combating Transnational Organized Crime.

For example, in Egypt, the Public Prosecution organizes and participates in seminars, conferences, and workshops, both locally and internationally. In addition, prosecution members at various levels are sent abroad to participate in training programs in cooperation with other prosecution bodies and international organizations, enabling them to learn about the latest systems in this field. Such meetings and seminars also facilitate the exchange of opinions, experiences, and ideas, encouraging collaboration among states and treaty partners in resisting such crimes(3).

Training programs and seminars benefit the participating organizations by allowing them to present vital topics, highlight their leadership role, and build trust with other stakeholders, which encourages further cooperation. They also enhance trainees' skills, knowledge, and ability to work effectively with international bodies, ultimately benefiting their home institutions(4).

One of the most significant experiences in this field is that of the United States. The U.S. is keen on providing technical assistance and training to enhance the criminal justice capabilities of other governments—supporting their police, prosecutors, and judges to become more effective in combating crime. Such assistance not only facilitates building a framework for international law enforcement cooperation but also strengthens the ability of foreign governments to address cybercrime domestically before it crosses borders.

---

(1) Ghanem Rady Al-Shammari, op. cit., p. 22.
(2) Sulaiman Abu Namer, op. cit., p. 38.
(3) Bourbaba Souria, International Cooperation in Combating Cybercrime, Journal of International Law for Research Studies, Issue 1, July 2019, p. 98.
(4) Sulaiman Abu Namer, op. cit., p. 40.

The Office of Overseas Prosecutorial Development, Assistance, and Training (OPDAT), affiliated with the U.S. Department of Justice, is tasked with providing the necessary support to strengthen criminal justice institutions and judicial administration abroad. Additionally, the International Criminal Investigative Training Assistance Program (ICITAP) often provides support to police agencies in developing countries worldwide.

Currently, the U.S. Department of Justice offers assistance to judicial systems in Africa, Asia, Eastern and Central Europe, among others. U.S. law enforcement agencies also provide training to their counterparts in other countries, either domestically or abroad, through specialized training agreements. For example, agreements with Hungary and Thailand allow American experts to train foreign law enforcement officers in innovative investigative methods and encourage the exchange of ideas with counterparts worldwide(1).

3. Current Challenges in Combating Cybercrime

Despite the efforts made to curb crimes committed over the Internet, whether by legislators or by investigative and judicial authorities, both internationally and domestically, these efforts face several obstacles and challenges. Chief among them Is the immaterial nature of crimes committed online, as well as the specific characteristics of the evidence derived from such crimes. The difficulties of detecting and proving Internet-related crimes are not the only factors that hinder the fight against them; there are also other challenges, particularly those related to the judicial aspect—such as determining the applicable law and Identifying the competent court to prosecute the perpetrators, who, in most cases, are individuals located outside the state's borders(2).

3.1 Difficulties Facing the Achievement of International Cooperation

- The absence of a unified law on cybercrime

The lack of a general consensus among states regarding the forms of misuse of information systems and the Internet that should be criminalized poses a major challenge. What may be permissible under one legal system could be considered criminal and prohibited under another. This divergence stems from differences in environments, customs, traditions, religions, and cultures across societies, which in turn leads to variations In legislative policies(3).

- The absence of effective mechanisms linking systems together

There must be a communication framework that enables investigative authorities to establish contact with foreign entities in order to collect specific evidence or critical Information.

- The diversity and differences In procedural legal systems

This is due to variations In methods of Investigation, prosecution, and trial from one state to another with respect to electronic surveillance, controlled delivery, undercover operations, and similar measures. A particular method of evidence collection or Investigation deemed legal in one country may be unlawful in another.(4)

- Jurisdictional issues in cybercrime

(1) Sulaiman Abu Namer, op. cit., p. 41.

(2) Mahmoud Mohamed Safaa El-Din Ali Shershar, previously cited reference, p. 565.

(3) Jamil Abdel-Baqi Al-Saghir, The Internet and Criminal Law: The Substantive Provisions of Internet-Related Crimes, Dar Al-Nahda Al-Arabiya, Cairo, 2001, p. 72

(4) Reference: Mahmoud Naguib Hosni, Commentary on the Code of Criminal Procedure, Dar Al-Nahda Al-Arabiya, Cairo, 1988, p. 823.

Jurisdiction refers to the authority granted by law to the judiciary to examine specific types of cases as determined by the legislator. Generally, jurisdiction is vested in the trial court, empowering it to adjudicate disputes(1).

Differences in laws and legal systems can lead to conflicts of jurisdiction in cybercrime cases, which are by nature transnational. Such conflicts may take the form of positive jurisdictional conflict—where multiple authorities claim jurisdiction over the same case—or negative jurisdictional conflict—where both decline jurisdiction on the grounds of lack of competence.(2)

For example, if a crime Is committed within the territory of one state by a foreign national, that crime falls within the jurisdiction of the first state on the basis of the principle of territoriality. If the perpetrator broadcasts obscene or pornographic material from one country, and it Is accessed In another, both states may assert jurisdiction—one under territoriality and the other under the principle of personality. Furthermore, if the crime threatens the security of a third state, jurisdiction may be established under the principle of protection(3).

- The principle of dual criminality In extradition

This condition within the extradition framework presents an obstacle to international cooperation in cybercrime cases, particularly as many states do not criminalize such acts. It also remains difficult to determine whether traditional provisions under the law of the requested state apply to Internet-related offenses. This complicates the implementation of international extradition treaties, obstructing evidence collection and the prosecution of offenders.(4)

- Mutual legal assistance through judicial cooperation

International judicial assistance often faces significant hurdles, such as delays in responses due to insufficiently trained personnel, language barriers, or procedural differences. Judicial cooperation may also conflict with the sovereignty of states, as each state typically retains exclusive jurisdiction over disputes arising within its territory(5).

- Lack of training for administrative leadership

Another challenge lies In the unwillingness or Inability of leadership figures to undergo training in information technology. Individual differences among trainees further hinder effective skills acquisition in IT and telecommunications. Some may lack any knowledge in the field, while others may already possess advanced expertise.(6)

- The international dimension

Electronic crime evidence may be stored in a computer located In a country different from where the offense was committed. Offenders can conceal their identity and transmit materials through multiple countries across continents before reaching recipients. This ability to navigate electronically through diverse networks and

(1) Jamil Abdel-Baqi Al-Saghir, previously cited reference, p. 73.
(2) Jamil Abdel-Baqi Al-Saghir, previously cited reference, p. 74.
(3) Adel Abdel-Aal Ibrahim Kharashi, previously cited reference, p. 62.

(4) Adel Abdel-Aal Ibrahim Kharashi, previously cited reference, p. 62.
(5) Mohamed Sami Abdel-Hamid, International Organization, Dar Al-Matbouaat Al-Jame'iya, Alexandria, 2002, p. 153.
(6) Mohamed Sami Abdel-Hamid, previously cited reference, p. 153.

databases complicates judicial efforts, as such crimes fall under the jurisdiction of multiple states governed by different laws and rules.

-The absence of bilateral or multilateral treaties

The lack of international agreements facIlitating cooperation in combating cybercrime, or the inadequacy of existing ones, poses another obstacle. Given the rapid technological advancements In computing and the Internet, cybercrime evolves at an equally rapid pace, outstripping legislative responses and straining state security authorities. This gap undermines effective international cooperation—a concern addressed by the United Nations and several European countries(1).

3.2 Difficulties Specific to Cybercrime

- **Cybercrimes are "clean crimes".**

They leave no trace of violence or bloodshed, making It difficult to establish proof. Instead, they Involve the alteration or deletion of numbers and data stored In computer memory, without leaving any tangible external evidence.

1. **The invisibility of electronically stored data.**

Data stored digitally is not visible or perceptible to the naked eye.

2. **Encryption of data**.

Both stored and transmitted data are often encrypted, particularly when transferred across communication networks.

3. **Ease of erasing or concealing evidence.**

Digital evidence can be deleted or hidden with relative ease(2).

4. **Perpetrators' use of security measures.**

Cybercriminals typically conceal their crimes and erase traces by manipulating databases, computer logs, or software without leaving evidence. Since electronic storage is invisible and data is encoded in digital language—unreadable to humans unless displayed on a screen—this presents a significant challenge in proving the crime(3).

Additionally, cybercriminals often hide their Identities or impersonate others to avoid detection In case their crimes are uncovered. Numerous programs allow users to mask their Identities when sending emails or browsing websites, making it more difficult for investigators to track them.

5. **Concealment by victims.**

Another obstacle to discovering cybercrimes Is the reluctance of victimized entities—often banks, financial Institutions, large corporations, or industrial enterprises—to report such Incidents. Instead, they tend to keep them hidden to protect their reputation and avoid loss of trust(4).

6. **Lack of expertise among law enforcement authorities.**

Criminal justice requires government bodies, particularly those tasked with investigating and prosecuting crimes, to assume responsibility for identifying

(1) Linda Sharabsha, International and Regional Policies In Combating Cybercrime: International Trends in Combating Cybercrime, Algeria, 2009, p. 250

(2) Mahmoud Mohamed Safaa El-Din Ali Shershar, previously cited reference, p. 568.

(3) Amjad Hassan Morshed Al-Dajjah, Strategies for Combating Cybercrime, Master's Thesis, Institute of Strategic Research and Studies, Omdurman Islamic University, Sudan, 2014, p. 59.

(4) Mahmoud Mohamed Safaa El-Din Ali Shershar, previously cited reference, p. 569.

offenders, apprehending them, and ensuring their prosecution. However, insufficient technical expertise among such authorities hampers this process.

7. **Obstruction of access to evidence.**

Cybercriminals are typically professionals who do not act Impulsively but rather plan their crimes carefully, using technical and intellectual skills to ensure success. They often surround themselves with protective technical safeguards that complicate the process of identifying and apprehending them.

8. **The vast amount of data to be examined.**

Investigations often require authorities to sift through massive volumes of digital data, which significantly delays and complicates the process.(1)

4 Conclusions:

1. The necessity of international cooperation: Cybercrimes transcend national borders, making international cooperation among states essential to ensure coordination between national legislations and to strengthen joint legal and judicial measures for prosecuting offenders.
2. Gaps in national legislation: Despite the efforts of many countries to enact laws combating cybercrimes, the lack of uniformity in legislation and differences in legal standards between states create gaps that reduce the effectiveness of law enforcement and judicial procedures.
3. Technological development and difficulty of prosecution: The rapid advancement of technology and its use in committing crimes make it difficult to track offenders, as methods and tools are constantly evolving, necessitating the continuous development of legal and technical mechanisms to keep pace with these changes.
4. The importance of building human and institutional capacities: Combating cybercrimes requires specialized training for judges, police, and technical experts, in addition to activating specialized international institutions, to ensure effective handling of these crimes and enhance legal deterrence.
5. Balancing technical, legal, and human rights challenges: Beyond technical and legal challenges, there are difficulties related to privacy, data protection, and human rights, requiring the development of mechanisms that balance crime prevention with the protection of citizens' fundamental rights, while promoting international cooperation and the exchange of expertise.

List of Sources and References

1. Mahmoud Mohamed Safaa El-Din Ali Shershar (no publication year), "International and Legislative Efforts to Combat Internet Crimes", Faculty of Law, Menoufia University, p. 527.
2. Qazran, Mustafa (2022), "International Mechanisms to Combat Cybercrime", Sawt Al-Qanoun Journal, Vol. 8, No. 2, Algeria, p. 1225.
3. Hussein Al-Ghafari (accessed 22-09-2025), "International Efforts in Confronting Cybercrime", published on www.cip.org.sa/vb/sharthread.php3697.
4. Hilali Abd Al-Lah Ahmed (2007), "The Budapest Convention on Cybercrime", Dar Al-Nahda Al-Arabiya, Cairo, Egypt, p. 327.

(1) Mahmoud Mohamed Safaa El-Din Ali Shershar, previously cited reference, p. 569.

5. Sulaiman Abu Namer (2020), "Combating Cybercrime within the Framework of International Law", Master's Thesis, Faculty of Law and Political Science, Department of Law, Mohamed Khider University of Biskra, Algeria, p. 37.
6. Ghanem Mardhi Al-Shammari (no publication year), "Cybercrimes", 1st Edition, Dar Al-Thaqafa, Amman, Jordan, p. 115.
7. Adel Abdel-Aal Ibrahim Kharashi (2015), "Challenges of International Cooperation in Combating Cybercrime and Ways to Overcome Them", 1st Edition, Dar Al-Jami'a Al-Jadida, Alexandria, p. 23.
8. Bourbaba Souria (2019), "International Cooperation in Combating Cybercrime", Journal of International Law for Research Studies, Issue 1, July, p. 98.
9. Mahmoud Mohamed Safaa El-Din Ali Shershar (no publication year), previously cited reference, p. 565.
10. Jamil Abdel-Baqi Al-Saghir (2001), "The Internet and Criminal Law: The Substantive Provisions of Internet-Related Crimes", Dar Al-Nahda Al-Arabiya, Cairo, p. 72.
11. Mahmoud Naguib Hosni (1988), "Commentary on the Code of Criminal Procedure", Dar Al-Nahda Al-Arabiya, Cairo, p. 823.
12. Mohamed Sami Abdel-Hamid (2002), "International Organization", Dar Al-Matbouaat Al-Jame'iya, Alexandria, p. 153.
13. Linda Sharabsha (2009), "International and Regional Policies in Combating Cybercrime: International Trends in Combating Cybercrime", Algeria, p. 250.
14. Amjad Hassan Morshed Al-Dajjah (2014), "Strategies for Combating Cybercrime", Master's Thesis, Institute of Strategic Research and Studies, Omdurman Islamic University, Sudan, p. 59.