

Dr. Islam Serour

Egyptian State Lawsuits Authority

International cooperation in pursuing cybercrime perpetrators, according to the United Nations Convention against Cybercrime

■ **Correspondence:** Dr. Islam Serour
Egyptian State Lawsuits Authority

■ **DOI:** 10.54873/jolets.v5i2.234

■ **E-mail:** counselor.islam.suroor@gmail.com

■ **Citation:** Islam Serour
International cooperation in pursuing cybercrime per-
petrators, according to the United Nations Convention
against Cybercrime, Volume 05, Issue 02 October 2025

Abstract:

This study examines the United Nations Convention against Cybercrime and its implications for strengthening international cooperation in combating offenses committed through information and communication technology (ICTs). With the growing reliance on ICTs, cybercrime has become increasingly complex, transnational, and organized, often involving multiple jurisdictions and criminal networks. This trend underscores the urgent need for harmonized legal frameworks and coordinated enforcement mechanisms at the international level.

This research highlights the Convention's role in enhancing states' capacity to address cybercrime by establishing common standards for investigation, prosecution, and extradition. A central focus is the principle of dual criminality, which facilitates mutual legal assistance and underpins the effectiveness of bilateral extradition treaties. The Convention also emphasizes the necessity of cross-border collaboration among law enforcement agencies to ensure that perpetrators are effectively pursued and brought to justice.

The findings suggest that the Convention provides a valuable foundation for reducing the global impact of cybercrime by promoting legal consistency, fostering trust between states, and supporting judicial cooperation. However, its effectiveness depends on the states' commitment to adopting and implementing its provisions comprehensively.

Accordingly, this study recommends that governments strengthen domestic legal frameworks, invest in capacity building, and actively engage in international partnerships. By doing so, states can better address the evolving threats posed by cybercrime, protect victims, and safeguard the integrity of digital ecosystems.

Keywords: Cybercrime, Information and Communication Technologies, International Cooperation, Dual Criminality, Extradition.

1. Introduction

International cooperation is an essential tool to confront traditional forms of transnational crime as well as new types of crime, such as cybercrime, which require an immediate and rapid response from the countries where the perpetrators of these crimes are present or fleeing to, as traditional methods of judicial cooperation in criminal matters no longer meet the requirements of a quick investigation of such types of crimes¹.

Although crime is a phenomenon in human societies, each society has its own characteristics regarding the spread of crime and its types. As methods of committing crime develop with the development of life in its various aspects and with the development of modern technology in our current era, traditional crimes are committed in different ways than they were previously known. This led to the emergence of a new type of crime, known as cybercrime, which is committed using information and communication technology systems.

This prompted the United Nations General Assembly to realize the importance of establishing an international convention to combat cybercrime and its firm conviction that the United Nations Convention against Cybercrime will work to enhance international cooperation to combat crimes committed using ICT systems and to exchange evidence in electronic form on serious crimes, which will constitute an effective tool and a legal framework for international cooperation in preventing and combating cybercrime and to ensure the collection and timely and legal exchange of evidence in electronic form in relation to a wide range of crimes that may be committed using ICT systems, including money laundering, corruption, terrorist acts, trafficking in persons, smuggling of migrants, the illicit manufacture and trafficking of

1 Gercke, M. Understanding cybercrime, phenomena, challenges and legal response, Telecommunication Development Sector, ITU publication, Switzerland, 2012, p.267, available at: https://www.unodc.org/e4j/data/_university_uni/_understanding_cyber-crime_phenomena_challenges_and_legal_response.

firearms, their parts and components and ammunition, illicit drug trafficking, and illicit trafficking in cultural property, which falls within the scope of crimes committed by organized crime gangs.

Cybercrime is a sophisticated form of transnational crime. The increasing involvement of organized crime groups further exacerbates the complexity of this crime, which occurs in the boundless cyberspace. Cybercriminals and their victims can be located in different regions worldwide. The effects of the crime can extend across societies around the world, highlighting the need for an urgent, dynamic, and international response, as well as a mechanism for international cooperation to collect and preserve information for investigations and procedural cooperation for the extradition of the perpetrators of these crimes².

The present study utilizes a doctrinal legal research methodology, characterized by the examination of primary legal sources, such as the United Nations Convention against Cybercrime and other international treaties, including the Budapest Convention, Hague Convention, and Model Treaty on Extradition.

Additionally, it involves analyzing secondary legal literature, including academic theses, articles, reports, and commentaries by renowned scholars.

This study aims to interpret the provisions of the Convention, define legal concepts such as cybercrime, dual criminality, and extradition, and synthesize existing legal arguments and frameworks to achieve this goal.

2. The nature and scope of Cybercrimes according to the International Convention

Cybercrimes pose a serious threat to global security and the digital economy, requiring significant efforts to mitigate them

2 See the website of the United Nations Regional Office on Drugs and Crime for the Middle East and North Africa: <https://www.unodc.org/romena/ar/cybercrime.html>

and maintain security and safety in cyberspace. These crimes are characterized by being carried out quickly and without physical evidence, which makes it difficult to investigate them and hold those responsible accountable. Cybercrimes also include several types of cyber-attacks and breaches, such as cyber fraud, cyber hacking, cyber-attacks, cyber espionage, cyber abuse, cyber extortion, and others.

Given the complexity of the use of terms in expressing the crime related to information and communications technology, it was essential to understand the nature of information and communications technologies and the definition of cybercrime before delving into the study of what is related to the regulation contained in the International Agreement on International Cooperation.

2.1 Definition of Cybercrime

Cybercrime can be defined as any criminal activity carried out using computer and electronic technologies, targeting cyber systems, networks, and electronic data³. It also includes hacking into systems, stealing, destroying, and disrupting information, as well as fraud, espionage, abuse, blackmail, and other criminal activities carried out using computer and electronic technologies.

Cybercrime is also known simply as “a crime committed using computers and the Internet.”⁴.

It should be noted here that most reports, guides, or publications on cybercrimes begin with a definition of the terms “computer

3 See the article entitled “The Concept of Cybercrimes, Their Types, Methods of Commitment, and Ways to Combat Them,” published on the “Wafeer Knowledge and Medicine” Arabic platform on the Internet: https://doafeer.net/concept_cybercrimes_types_committing_combating/

4 Dr. Khalid bin Suleiman Al-Ghathbar and Dr. Eng. Muhammad bin Abdullah Al-Qahtani, Information Security in a Simplified Language, Center of Excellence for Information Security, King Saud University, Pub. 1429 AH, p. 20.

crimes” and “cybercrimes.”⁵. In this context, different approaches have been adopted to develop a precise definition of both terms in recent decades.⁶

As the research mainly focuses on international cooperation in Pursuing Cybercrime Perpetrators, we will first review the definition of each before providing an overview.⁷ Without delving into details.

Therefore, the term “cybercrime” or “electronic crime” is narrower than computer-related crimes (“computer crimes”) as it must involve the Internet⁸. Computer-related crimes (computer crime) include crimes that are not connected to the Internet but only affect independent computer systems.

5 See, in this context: Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, *International Journal of Law and Information Technology*, 2002, Vol. 10, No. 2, page 144, available at: <https://archive.org/details/TheEmerging-ConsensusOnCriminalConductInCyberspace/page/n95/mode/2up>

6 Regarding approaches to define and categorize cybercrime, see, for example, Cybercrime, Definition and General Information, Voce I & Morgan A 2023. *Cybercrime in Australia 2023*. Statistical Report no. 43. Canberra: Australian Institute of Criminology available at: <https://doi.org/10.52922/sr77031>; Explanatory Report to the Council of Europe Convention on Cybercrime, No. 8; Gordon/Ford, On the Definition and Classification of Cybercrime, *Journal in Computer Virology*, Vol. 2, No. 1, 2006, page 13-20; Chawki, Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/; Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf; Cybercrime, Report of the Parliamentary Joint Committee on the Australian Crime Commission, 2004, page 5, available at: [Reports on Annual Reports – Parliament of Australia](#); Hayden, Cybercrime’s impact on Information security, Cybercrime and Security, IA-3, page 3; Ian Brown and Christopher Marsden Information Security and Cybercrime, research paper, available at: https://www.researchgate.net/publication/228226770_Information_Security_and_Cybercrime; Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, *CJI* 2002, Vol. 18, available at: [Cybercrime: Facts & Figures Concerning This Global Dilemma | Office of Justice Programs](#); Forst, Cybercrime: Appellate Court Interpretations, 1999, page 1, available at: [Cybercrime: Appellate Court Interpretations : Martin L. Forst : Free Download, Borrow, and Streaming : Internet Archive](#).

7 Nhan/Bachmann in Maguire/Okada (eds), *Critical Issues in Crime and Justice: Thought, Policy, and Practice*, Third Edition, SAGE Publications, Inc., 2019, Chapter 14 Critical Issues in Cybercrime, page 211 available at: [Sage Academic Books - Critical Issues in Crime and Justice: Thought, Policy, and Practice](#).

8 Regarding this relationship, see also: Sieber in *Organised Crime in Europe: The Threat of Cybercrime*, Situation Report 2004, page 86 <https://doi.org/10.1007/s12117-005-1036-6>.

Whereas, during the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions were developed in the framework of a related workshop: one covering cybercrime in the narrow sense (cybercrime) which is any illegal conduct directed by electronic processes that target the security of computer systems and the data processed by them; and the other covering cybercrime in the broader sense (computer-related crime) which is any illegal conduct committed by or in connection with a computer system or network, including crimes such as the illegal possession, display or distribution of information by means of a computer system or network⁹.

Also, the common definition of cybercrime states that it encompasses any activity where computers or networks serve as the tool, target, or venue for criminal acts, but this broad interpretation presents several challenges.

For instance, it implies that traditional crimes, like murder, would be classified as cybercrime if a keyboard were used to assault the victim¹⁰.

A further broader definition is also contained in Article 1.1 of the Stanford Draft International Convention to Enhance Protection from Cybercrime and Terrorism (“Stanford Draft”)¹¹. It indicates

9 Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: <https://digitallibrary.un.org/record/432653?v=pdf>.

10 See, for example: Carter, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: <https://www.ojp.gov/pdffiles1/Digitization/156176NCJRS.pdf>; Charney, Computer Crime: Law Enforcement’s Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 et seq.; Goodman, Why the Policy don’t care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

11 The Stanford Draft International Convention was developed as a follow-up to a conference hosted at Stanford University in the United States in 1999. The text of the

that cybercrimes are actions related to cyber systems¹².

Some definitions also attempt to provide more comprehensive definitions, taking into account the goals or intentions to define cybercrimes more precisely¹³. Such as this definition: “computer-mediated activities that are considered illegal or unlawful by certain parties and that can be conducted over international cyber networks.”¹⁴.

In light of the last definition, which is similar to the meaning given in many of the references referred to above, cases in which firearms or explosives are used... and in which electronic devices or computers are used to commit ordinary crimes are excluded, but such a definition risks excluding some crimes that are considered cybercrimes in international laws and agreements such as the Commonwealth Model Law on Computer-Related Crime and Computer-Related Crime or the Council of Europe Convention on Cybercrime.¹⁵

Stanford Draft is available at: <https://web.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf>.

12 Article 1, The Stanford Draft International Convention, Definitions and Use of Terms: For the purposes of this Convention: 1. “cybercrime” means conduct, with respect to cyber systems, that is classified as an offense punishable by this Convention; [...]

13 See: Hayden, Cybercrime’s impact on Information security, Cybercrime, and Security, IA-3, page 3.

14 Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37

15 Council of Europe Convention on Cybercrime (CETS No. 185), available at: <http://conventions.coe.int>. For more details about the offences covered by the Convention, see below: § 6.2.; Gercke, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 et seq.; Gercke, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et seq.; Aldesco, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: <http://elr.ils.edu/issues/v23-issue1/aldesco.pdf>; Jones, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; Peter CSONKA, THE

Also, Cybercrime is defined in various academic and legal frameworks with overlapping yet distinct emphases on its nature and scope. Academically, cybercrime is widely recognized as criminal activities that depend significantly on the use of digital technology or cyberspace¹⁶.

Legally, definitions of cybercrime are complicated by jurisdictional differences and evolving technology, but international efforts such as those by the United Nations strive to harmonize legal frameworks to address cybercrime consistently.

These legal definitions generally characterize cybercrime as offenses that involve computers or networks as tools, targets, or places where criminal activity occurs, covering crimes such as unauthorized access, data theft, and cyber fraud.¹⁷

Academic literature further notes that conceptualizing cybercrime remains challenging due to variability in terminology and legislation across jurisdictions. Systematic literature reviews have sought to consolidate existing definitions and propose classification frameworks to understand cybercrime and related deviance better.

COUNCIL OF EUROPE'S CONVENTION ON CYBER-CRIME AND OTHER EUROPEAN INITIATIVES, *International Review of Penal Law* (Vol. 77), available at: <https://shs.cairn.info/revue-internationale-de-droit-penal-2006-3-page-473?lang=-fr> ; Broadhurst, Development in the global law enforcement of cyber-crime, in *Policing: An International Journal of Police Strategies and Management*, 29(2), 2006, page 408 et seq.; Adoption of Convention on Cybercrime, *International Journal of International Law*, Vol. 95, No. 4, 2001, page 889 et seq.

16 For example, one comprehensive review emphasizes that cybercrime is not merely a technical issue but involves human offenders and should be understood as crime that uses digital technology in a significant way, incorporating research from social sciences alongside legal studies to conceptualize it, see: Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, 14(1), 52–60. <https://doi.org/10.1080/17440572.2012.759508>.

17 Allahrakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, 2(5), 28–36. <https://doi.org/10.59022/ijlp.191>

These efforts underscore that cybercrime encompasses a wide spectrum of offenses, including, but not limited to, hacking, identity theft, cyberstalking, online fraud, cyberterrorism, and the spread of malicious software.¹⁸

Moreover, specialized academic work acknowledges the emergence of organized cybercrime, comparing it to traditional organized crime structures, and emphasizes the novelty and complexity of criminal enterprises operating in cyberspace.¹⁹

Emerging technologies such as AI and IoT have introduced new categories of cyber offenses, requiring legal definitions to adapt dynamically to include technology-driven crimes.

In sum, detailed academic and legal definitions of cybercrime share common ground in recognizing it as criminal conduct that significantly involves digital technology, yet highlight the continued evolution and multidimensional challenges of defining and legislating against such offenses comprehensively and uniformly across global contexts.

The diversity of methods involved in cybercrimes and related issues highlights difficulties in defining “computer crime” and “cybercrime”, as the term “cybercrime” covers a broad range of offenses, including traditional computer crimes and network-based crimes, and due to their differences, no single standard can encompass all acts across various legal systems, excluding crimes facilitated solely by devices.

However, the absence of a single definition isn’t critical since “cybercrime” isn’t a legal term. Many simplify the definition by focusing on the means of using computers and the Internet, Such

18 Phillips, K., Davidson, J. C., Caneppele, S., Burkhardt, C., Aiken, M. P., & Farr, R. R. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, 2(2), 379–398. <https://doi.org/10.3390/forensicsci2020028>

19 Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, 14(1), 52–60. <https://doi.org/10.1080/17440572.2012.759508>

as in the International Convention on Combating Cybercrime, which aims to improve international cooperation against crimes committed through information and communication technology, emphasizing the means rather than the intentions or perpetrators.²⁰

2.2 Criminal Uses of ICT

Cybercrimes are broadly categorized into two types: violent or potentially violent crimes and non-violent crimes. Violent cybercrimes such as cyberterrorism, threats, cyberstalking, and child pornography pose physical threats and are a priority. Most cybercrimes are non-violent because of the nature of cyberspace interaction without physical contact. Its anonymity and 'unreal' environment attract offenders. Non-violent cybercrimes include cyber theft, cyber fraud, and destructive cybercrimes.²¹

The term "cybercrime" encompasses a broad range of criminal activities involving information technology. The UN Convention against Cybercrime lists crimes such as money laundering, corruption, terrorism, human trafficking, migrant smuggling, illegal firearm manufacturing and trafficking, drug trafficking, and illicit cultural property trafficking, all facilitated through ICT systems.²² It also lists the forms of committing these crimes in more detail under Articles 7 to 17.

This is in eleven criminal forms, as follows: (1) Illegal access (Article 7), (2) Illegal interception (Article 8), (3) Interference with

20 See, United Nations resolution on combating the use of information and communications technologies for criminal purposes: Report of the Third Committee: General Assembly, seventy-ninth session, adopting the draft resolution United Nations Convention against Cybercrime, through the following link: <https://digitallibrary.un.org/record/4068812?ln=en&v=pdf>

21 Chawki, Cybercrime in France: An Overview, 2005, available at: www.crimere-search.org/articles/cybercrime-in-france-overview

22 See, United Nations resolution on combating the use of information and communications technologies for criminal purposes: Report of the Third Committee: General Assembly, seventy-ninth session, adopting the draft resolution United Nations Convention against Cybercrime, through the following link: <https://digitallibrary.un.org/record/4068812?ln=en&v=pdf>

electronic data (Article 9), (4) Interference with an information and communications technology system (Article 10), (5) Misuse of devices. (Article 11), (6) Information and communications technology system-related forgery (Article 12), (7) Information and communications technology system-related theft or fraud (Article 13), (8) Offences related to online child sexual abuse or child sexual exploitation material (Article 14), (9) Solicitation or grooming for the purpose of committing a sexual offence against a child (Article 15), (10) Non-consensual dissemination of intimate images (Article 16), and (11) Laundering of proceeds of crime (Article 17).

The Convention also added, under the text of Article 4, that the acts criminalized according to the other applicable United Nations conventions and protocols must be considered by the States Parties as criminal offenses under domestic law when committed through the use of information and communications technology systems, if the act committed according to its material form constitutes a crime in itself according to the rules of the other convention or the applicable protocols, as the Convention currently under study is not what criminalizes those acts, but rather added what relates to the means of committing the crime to be the basis of cybercrimes committed using information and communications technology systems. In the second section, we will discuss in detail the scope of application of the Convention and the crimes contained therein.

3. International Cooperation within the scope of the United Nations Convention against Cybercrime

The UN Convention against Cybercrime is the second global treaty, following the Budapest Convention from 2001 under the Council of Europe. In December 2019, efforts to establish a UN convention faced division. Some countries, including Russia and China, supported it, while others, like Australia, Japan, the UK, and the US, opposed. Australia and allies prefer the Budapest Convention, which promotes cooperation on cybercrime and

includes protections and standards, but remains a European treaty. Many non-European countries participated, yet Russia did not sign, and the treaty was seen as limited and unrepresentative.²³

This prompted the United Nations to move towards the necessity of concluding an international agreement regulating this type of crime as a first step towards establishing bilateral agreements for procedural cooperation between member states and combating these crimes more comprehensively. We will discuss aspects related to international cooperation in light of the provisions of the international Convention, beginning by defining the scope of application.

3.1 Scope of application of the Convention and acts criminalized under its provisions:

Article 3 of the Convention clarifies the scope of its application, except as otherwise provided, as follows:

- (a) The prevention, investigation, and prosecution of the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation, and return of the proceeds from such offences;
- (b) The collecting, obtaining, preserving, and sharing of evidence in electronic form for the purpose of criminal investigations or proceedings, as provided for in articles 23 and 35 of this Convention.

23 Gatra Priyandita, The UN Cybercrime Convention: a victory for State Sovereignty, an article published 16 Aug 2024, in ASPI Australian Strategic Policy Institute, <https://www.aspistrategist.org.au/the-un-cybercrime-convention-a-victory-for-state-sovereignty/>

In addition, the Convention addresses eleven forms of crimes committed using information and communications technology systems and defines them as follows:

- 1. Illegal Access:** Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law when committed intentionally, the access to the whole or any part of an information and communications technology system without right²⁴.
- 2. Illegal interception:** Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the interception, made by technical means, of non-public transmissions of electronic data to, from or within an information and communications technology system, including electromagnetic emissions from an information and communications technology system carrying such electronic data²⁵.
- 3. Interference with electronic data:** Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the damaging, deletion, deterioration, alteration or suppression of electronic data²⁶.

24 Also, The UN Convention stated in Art.7 that: ‘A State Party may require that the offence be committed by infringing security measures, with the intent of obtaining electronic data or other dishonest or criminal intent or in relation to an information and communications technology system that is connected to another information and communications technology system.’

25 Also, The UN Convention stated in Art.8 that: ‘A State Party may require that the offence be committed with dishonest or criminal intent, or in relation to an information and communications technology system that is connected to another information and communications technology system.’

26 Also, The UN Convention stated in Art.8 that: ‘A State Party may require that the conduct described in paragraph 1 of this article result in serious harm.’

4. **Interference with an information and communications technology system:** Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the serious hindering of the functioning of an information and communications technology system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing electronic data.
5. **Misuse of devices:** Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

(a) The obtaining, production, sale, procurement for use, import, distribution or otherwise making available of:

(i) A device, including a program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention; or

(ii) A password, access credentials, electronic signature or similar data by which the whole or any part of an information and communications technology system is capable of being accessed;

with the intent that the device, including a program, or the password, access credentials, electronic signature or similar data be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention;

(b) The possession of an item referred to in paragraph 1 (a) (i) or (ii) of this article, with intent that it be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention.

Also, Art. 11 shall not be interpreted as imposing criminal

liability where the obtaining, production, sale, procurement for use, import, distribution or otherwise making available, or the possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with articles 7 to 10 of this Convention, such as for the authorized testing or protection of an information and communications technology system. According to the aforementioned articles, these criminal acts are Illegal Access, Illegal Interception, Interference with electronic data, and Interference with an information and communications technology system²⁷.

6. **Information and communications technology system-related forgery:** Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion or suppression of electronic data resulting in inauthentic data with the intent that they be considered or acted upon for legal purposes as if they were authentic, regardless of whether or not the data are directly readable and intelligible²⁸.
7. **Information and communications technology system-related theft or fraud:** Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by means of:
 - (a) Any input, alteration, deletion or suppression of electronic data;
 - (b) Any interference with the functioning of an information

27 The UN Convention stated in Art. 11 that: 'Each State Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (ii) of this article.'

28 The UN Convention stated in Art. 12 that: 'A State Party may require an intent to defraud, or a similar dishonest or criminal intent, before criminal liability attaches.'

and communications technology system;

(c) Any deception as to factual circumstances made through an information and communications technology system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do; with the fraudulent or dishonest intent of procuring for oneself or for another person, without right, a gain in money or other property.

8. Offences related to online child sexual abuse or child sexual exploitation material²⁹: Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right, the following conduct:

(a) Producing, offering, selling, distributing, transmitting, broadcasting, displaying, publishing or otherwise making available child sexual abuse or child sexual exploitation material through an information and communications technology system;

(b) Soliciting, procuring or accessing child sexual abuse or child sexual exploitation material through an information

29 According to Art. 14 of the UN Convention, the term “child sexual abuse or child sexual exploitation material” shall include visual material and may include written or audio content that depicts, describes, or represents any person under 18 years of age: (a) Engaging in real or simulated sexual activity; (b) In the presence of a person engaging in any sexual activity; (c) Whose sexual parts are displayed for primarily sexual purposes; or (d) Subjected to torture or cruel, inhumane, or degrading treatment or punishment, and such material is sexual in nature.

- Also, the state party may require that the material identified in paragraph 2 of this article be limited to material that: (a) Depicts, describes, or represents an existing person; or (b) Visually depicts child sexual abuse or child sexual exploitation.

- Also, the state party may, In accordance with their domestic law and consistent with applicable international obligations, take steps to exclude the criminalization of: (a) Conduct by children for self-generated material depicting them; or (b) The consensual production, transmission, or possession of material described in paragraph 2 (a) to (c) of this article, where the underlying conduct depicted is legal as determined by domestic law, and where such material is maintained exclusively for the private and consensual use of the persons involved.

and communications technology system;

(c) Possessing or controlling child sexual abuse or child sexual exploitation material stored in an information and communications technology system or another storage medium;

(d) Financing the offences established in accordance with subparagraphs (a) to (c) of this paragraph, which States Parties may establish as a separate offence.

9. **Solicitation or grooming for the purpose of committing a sexual offence against a child:** Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the act of intentionally communicating, soliciting, grooming, or making any arrangement through an information and communications technology system for the purpose of committing a sexual offence against a child³⁰, as defined in domestic law, including for the commission of any of the offences established in accordance with article 14 of this Convention.
10. **Non-consensual dissemination of intimate images:** Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the selling, distributing, transmitting, publishing or otherwise making available of an **intimate image of a person** by means of an information and communications technology system, without the consent of the person

30 A State Party may require an act in furtherance of the conduct described in paragraph 1 of Art. 15. Also, may consider extending criminalization in accordance with paragraph 1 of this article in relation to a person believed to be a child in addition to it may take steps to exclude the criminalization of conduct as described in paragraph 1 of this article when committed by children.

depicted in the image³¹³².

Also, a State Party may require the intent to cause harm before criminal liability attaches and may take other measures concerning matters related to the type of this crime in accordance with their domestic law and consistent with applicable international obligations.

11. Laundering of proceeds of crime: Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences when committed intentionally:

(a) (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of that person's actions³³;

(ii) The concealment or disguise of the true nature, source, location, disposition, movement, or ownership of or rights

31 For the purpose of the first paragraph of the article 16, "intimate image" shall mean a visual recording of a person over the age of 18 years made by any means, including a photograph or video recording, that is sexual in nature, in which the person's sexual parts are exposed, or the person is engaged in sexual activity, which was private at the time of the recording, and in respect of which the person or persons depicted maintained a reasonable expectation of privacy at the time of the offense. It may also extend the definition of intimate images, as appropriate, to depictions of persons who are under the age of 18 years if they are of legal age to engage in sexual activity under domestic law and the image does not depict child abuse or exploitation.

32 For the purposes of Article 16, a person who is under the age of 18 years and depicted in an intimate image cannot consent to the dissemination of an intimate image that constitutes child sexual abuse or child sexual exploitation material under Article 14 of this Convention.

33 As stated in Article 17 of the UN Convention, for purposes of implementing or applying paragraph 1 of this article:

(a) Each State Party shall establish as predicate offences relevant offences established in accordance with articles 7 to 16 of this Convention;

(b) In the case of States Parties whose legislation sets out a list of specific predicate offences, they shall, at a minimum, include in that list a comprehensive range of offences established in accordance with articles 7 to 16 of this Convention.

with respect to property, knowing that such property is the proceeds of crime;

(b) Subject to the basic concepts of the state-party legal system, it shall take all the necessary actions to criminalize the following³⁴:

(i) The acquisition, possession, or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

(ii) Participation in, association with, or conspiracy to commit, attempts to commit, and aiding, abetting, facilitating, and counselling the commission of any of the offences established in accordance with this article.

The eleven categories of crimes perpetrated through information and communications technology (ICT) systems, as mentioned above, encompass a comprehensive array of malicious activities that exploit digital environments.

These categories illustrate the multifaceted nature of cybercrime and emphasize the need for targeted legal measures within the domestic laws of State Parties to the United Nations Convention against Cybercrime.

Each offense pertains to a specific mode of attack or misuse of ICT systems. Collectively, these categories establish a robust legal framework that not only criminalizes direct attacks on ICT systems and data but also addresses the ancillary criminal behaviors that

³⁴ For the purposes of subparagraph (b), predicate offences include offences committed both within and outside the jurisdiction of the State Party concerned.

An example of this may be given in the case of the acquisition of property that is the proceeds of crime for an act committed outside the jurisdiction of the State in which the property was received, in which case that act is considered a criminal offence in itself regardless of the place where the predicate offence resulting in the acquisition of the transferred property was committed in the other State.

The article also indicated that offences committed outside the jurisdiction of a State Party constitute predicate offences only if the relevant act is a criminal offence under the domestic law of the State in which it was committed and would have been a criminal offence under the domestic law of the State Party implementing or applying this article had it been committed there.

facilitate or result from cybercrime.

This comprehensive approach promotes harmonized legislation across states, thereby enhancing international cooperation for investigation, prosecution, and extradition.

The detailed enumeration also helps clarify the scope of cybercrime for legal practitioners and policymakers, ensuring clarity in enforcement and judicial proceedings.

This structured categorization aligns with the Convention's objective of creating a common understanding and legal basis for effectively combating cybercrime, reflecting the evolving technological landscape and the diverse methods employed by offenders.

In the second section, we explain the mechanisms for international cooperation to prosecute the perpetrators of these crimes and for extraditing criminals in accordance with the provisions of the United Nations Convention Against Cybercrime.

3.2 International Cooperation to Prosecute and Extradite Perpetrators of Cybercrimes:

International cooperation is essential due to increasing criminal activities, terrorism, and crimes against humanity, both domestically and internationally, in the last decade of the 20th century. It reflects the global consolidation of criminal justice principles. The modern extradition system is a key form of this cooperation, demonstrating states' commitment to ensure criminals do not evade punishment after leaving the crime scene.³⁵

Extradition is no longer merely an act of international courtesy,

35 Islam Serour, *Extradition of Foreigners in Terrorism Cases, A Comparative Study in Light of International Conventions*, Dar al-Fath for Printing and Publishing, Alexandria, p 16. Also see: Boister, Neil, *An Introduction to Transnational Criminal Law*, 2nd Edition (2018; online edn, Oxford Law Pro), <https://doi.org/10.1093/law/9780198795995.001.0001>, accessed 20 Dec. 2025.

as some jurists have suggested. Instead, states have adopted it for various reasons. The arguments presented by opponents of this system are weak and collapse under scrutiny. Extradition is no longer regarded as an act that the state regrets and wishes to abolish; rather, states have come to recognize its advantages, organizing it through treaties or domestic legislation.

It can be said that the state has two main interests in accepting extradition requests: *firstly*, it works to avoid the disturbances caused by the presence of a criminal within its territories, and *secondly*, it ensures reciprocal treatment in the future.

The majority of legal scholars believe that extraditing a foreign fugitive to face trial in the state whose laws were violated is the best possible solution. The state where the crime occurred is always in the best position to collect evidence, bring in witnesses, and understand how the crime took place. Therefore, the interests of investigation and prosecution require that the foreign fugitive be extradited to the state where the criminal act occurred, especially if the act was part of a terrorist crime committed on its territory³⁶.

Extradition involves states cooperating to enforce justice and prevent territories from becoming safe havens for criminals. It fosters cooperation in combating crime, which is vital for maintaining security. Allowing criminals to escape undermines justice, making extradition a crucial aspect of the justice system.³⁷

36 Islam Serour, Extradition of Foreigners in Terrorism Cases, A Comparative Study in Light of International Conventions, Dar al-Fath for Printing and Publishing, Alexandria, (2024), p 22. Also see: Dugard, J., & Van Den Wyngaert, C. (1998). Reconciling Extradition with Human Rights. *American Journal of International Law*, 92(2), 187–212. <https://doi.org/10.2307/2998029>

37 Dr. Mahmoud Hassan Al-Arousi, A Study on the Extradition of Criminals in the Egyptian System and Comparative Legislation, Costatsoumas Press, 1951, p. 17, etc.

Achieving the *public interest* among states is a *strong justification for establishing the system of extradition*.³⁸ States can prosecute criminals for national security, grounded in international cooperation and solidarity. The UN's role in extradition aims to reduce organized crime and terrorism worldwide.³⁹

Also, activating international conventions to enhance cooperation against organized crime, terrorism, arms, and drug smuggling, while establishing global norms in criminal and humanitarian law for international justice⁴⁰.

The rise in wars and crimes worldwide has caused more terrorist acts, fugitives escaping prisons, and criminals crossing borders, highlighting the need for an extradition system.

The International Convention against Cybercrime is undoubtedly one of the United Nations conventions that is based on the pillar of achieving the public interest among states. It rests on the same foundations and objectives upon which international cooperation is based to limit the spread and pursue perpetrators of these crimes. This is particularly significant given the rapid expansion and the broad scope of these crimes, along with the multiple methods of committing them in the present time.

Chapter Five (Articles 35 to 52) of the International Convention explicitly affirms the general principles of international cooperation, setting out the general rules necessary for pursuing the perpetrators of such crimes and investigating them. Here, we present the aspects related to the extradition of cybercrime

38 Dr. Abdel Fattah Mohamed Siraj, *The General Theory of Extradition*, Dar Al Nahda Al Arabiya, Cairo, 1998, p. 25, etc.

39 Dr. Mohamed Abu Al-Fath Ibrahim, *Combating Organized Crime in Light of International Treaties*, PhD Thesis, Menoufia University, 2010, p. 182.

40 Dr. Faiza Younis Al-Basha, *Organized Crime in Light of International Agreements and National Laws*, Dar Al-Nahda Al-Arabiya, Cairo, 2001, p. 88-89 et seq.

perpetrators according to the provisions of the Convention as follows:

Article 35 of the Convention defines the General principles of international cooperation. We comment on this by stating that the Convention has explicitly addressed the principle of dual criminality (Article 35/3) in relation to international cooperation. The application of this provision becomes evident in the context of extraditing criminals, as dual criminality is one of the essential conditions for extradition. The principle of dual criminality means that the act serving as the basis for extradition must be considered a crime under the laws of both the requesting state and the state from which extradition is sought. This requirement is logical since the commitment of a state to extradite would be weak if the act were not criminalized under its own law⁴¹. Some states adopt this condition as a fundamental basis for the extradition process, and extradition would not be valid without it⁴².

The Tenth International Congress of Criminal Law⁴³, held in Rome in 1969, called for abandoning the dual criminality requirement if the circumstances of the requesting state necessitated deterring

41 A person may not be extradited for the execution of a criminal judgment issued against them by another state if the act that served as the basis for that conviction was not considered a crime under the law of the state from which extradition is requested at the time the judgment was issued. Refer to the application of this principle: *Vois cour d'appel d'Aix-en-Provence*, 24 Novembre 1999, D. 2000, p.245, note Renucci.

42 Dr. Mazhar Gebran Ghaleb Al-Masry, *International Cooperation in Combating Organized Crime*, master's thesis, Faculty of Law, Assiut University, Egypt, 2008, p. 176 et seq.

43 **International Congress of Criminal Law (Tenth Session), held in Rome in 1969, which stipulates the abandonment of the dual criminality requirement if the circumstances of the requesting state necessitate deterring criminals who violate the law across both the requesting and requested states.** Refer to the recommendations of the Tenth International Congress of Criminal Law, published in the *National Criminal Journal*, National Center for Social and Criminal Research, Vol. 13, Issue 1, March 1970, pp. 143–154, and available on the Egyptian Knowledge Bank (<http://www.ekb.eg>).

criminals who violate its laws and international law⁴⁴.

In this context, the principle of dual criminality serves both as a restriction and a protection for the requested individual. The restriction lies in the requirement for punishment in both the requesting and the requested states for the same offender. However, the necessity of punishment does not imply its identical nature, but rather that the act is criminalized to a similar degree without requiring identical classification⁴⁵.

This condition is integrated within the substantive requirements related to identifying the crimes that warrant extradition. The guarantee provided by this principle is closely linked to the principle of legality. It is evident that this fundamental principle, on which the dual criminality condition rests, represents the other side of the protection afforded to both the requesting and requested states, as well as the requested individual.

Examples of treaties that establish extradition include Article 8 of the Hague Convention⁴⁶. Similarly, the second article of the _____

44 Abdul Rahman Fathi Samhan, "Extradition of Criminals under the Rules of International Law," Dar Al-Nahda Al-Arabiya, Egypt, 2011, p. 272.

45 **The Principle of Legality (Legality Principle)** means that there is no crime and no punishment without a legal provision. This implies that no individual may be accused or subjected to any legal action for engaging in behavior unless that behavior is specifically punishable under the law and subject to criminal sanctions. **For further details, refer to:** Dr. Ahmed Fathi Sorour, *Constitutional Legitimacy and Human Rights in Criminal Procedures*, Dar Al-Nahda Al-Arabiya, Egypt 1993, p. 129 et seq. Also, Dr. Mahmoud Najib Hosni, *Explanation of the Penal Code – General Section – General Theory of Crime and the General Theory of Punishment and Preventive Measures*, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 4th Edition, 1983, p. 78.

46 **Article 8 of the Hague Convention on the Unlawful Seizure of Aircraft (1970)** – The Diplomatic Conference was attended by representatives of 27 countries, along with 12 international organizations. When the draft was put to a vote, it was approved by 74 countries, signed by representatives of 50 countries, and faced no opposition. The Convention was signed on December 16, 1970, and entered into force on October 14, 1971. By July 16, 1991, a total of 143 countries had ratified it, with Egypt joining on February 28, 1975. **For more details, refer to:** Dr. Ihab Mohamed Youssef, *Extradition Treaties and Their Role in Achieving International Cooperation*

United Nations Model Treaty on Extradition dated December 14, 1990, and Article 40 of the Arab League's Riyadh Agreement on Judicial Cooperation of 1983, affirm that "extradition is mandatory for those accused of acts punishable under the laws of both contracting parties requesting extradition and the one from which extradition is sought, with a custodial penalty of at least one year or a more severe penalty under the law of either party, regardless of the maximum or minimum punishment specified." For that, the Courts have refused extradition in several cases due to the lack of dual criminality in both the requesting and the requested states⁴⁷.

An application of the *dual criminality* principle can be seen in the ruling of the Supreme Court of New Zealand, which decided that "**Mr. Kim Dotcom** must be extradited to the United States to face the prescribed penalties for violating intellectual property rules

to Combat Terrorism, Ph.D. Thesis, Cairo, Egypt, Police Academy, 2003, p. 400, 441.

47 Article (40) of the Riyadh Arab Convention on Judicial Cooperation. Also, Article 3 of the 1952 Arab Convention concerning Persons Subject to Extradition states the following: 'Extradition shall be mandatory for the following persons:

A. Individuals accused of acts punishable under the laws of both contracting parties—the requesting party and the requested party—with a custodial sentence of at least one year or a more severe penalty according to the law of either party, regardless of the maximum or minimum penalties specified.

B. Individuals accused of acts that are not punishable under the laws of the requested contracting party or where the prescribed penalty for those acts under the law of the requesting contracting party does not have an equivalent in the law of the requested contracting party, provided that the individuals sought are nationals of the requesting contracting party or nationals of another contracting party that imposes the same penalty.

C. Those who have been convicted, either in person or in absentia, by the courts of the requesting contracting party, with a custodial sentence of at least one year or a more severe penalty for acts punishable under the law of the requested contracting party.

D. Those who have been convicted, either in person or in absentia, by the courts of the requesting contracting party for an act that is not punishable under the laws of the requested contracting party, or with a penalty that does not have an equivalent in its laws, provided that they are nationals of the requesting contracting party or nationals of another contracting party that imposes the same penalty.'

related to his former website, ‘*Megaupload*’.” The court addressed the defense argument, stating that:

*“Protecting intellectual property in public network communication does not constitute a crime in New Zealand.” The court responded that “violating intellectual property rules in this manner **could constitute a crime of breach of trust**, which is considered a crime in New Zealand and **for which extradition is permissible under the treaty with the United States.**”⁴⁸*

The Convention under study has followed the same approach as modern conventions concerning the regulation of international cooperation. We have previously clarified that the principle of **dual criminality**, in the context of international cooperation, is clearly evident in the process of extradition between states.

The Convention explicitly states that the condition of dual criminality is considered fulfilled, regardless of whether the laws of the requested state party classify the concerned crime within the same category as the requesting state party or use the same terminology, provided that the conduct underlying the crime for which assistance is sought is considered a criminal offense under the laws of both state parties.

This serves as a precise application of the established principle in international law regarding dual criminality. The Convention

48 *Case Study 5 (Dotcom et al. v. the United States)*, Justice Murray Gilbert of the High Court of New Zealand ruled that while he agreed with one of Dotcom’s defence attorney’s primary argument that “**online communication of copyright-protected works to the public was not a criminal offense in New Zealand**,” Dotcom and his co-defendants were still eligible for extradition based on their conduct which can be interpreted as the offense of conspiracy to defraud in terms of art II.16, referring to a particular section of the extradition treaty between New Zealand and the United States. For more information, website link: <https://www.unodc.org/e4j/en/organized-crime/module-11/exercises/case-studies.html>

further explains that it is not required for the crime to have the same classification in both states in terms of international cooperation, as long as the act is considered a criminal offense under the laws of both the requesting and requested states in pursuing cybercrime offenders.

This also maintains a balance between preserving state sovereignty on one hand and safeguarding human rights and the freedoms of the accused to a significant extent on the other hand, while also considering the application of certain human rights agreements, such as the United Nations Human Rights Convention⁴⁹.

Also, the new Convention provides a detailed outline of the procedures for the extradition of cybercrime offenders in accordance with its provisions. Article 37 of the Convention stipulates the regulations concerning Extradition and the procedures involved.

This article of the new Convention has incorporated all the procedural rules internationally agreed upon regarding extradition, explicitly providing for the possibility of extraditing criminals for all acts that are considered crimes under the Convention's application, provided that the crime for which extradition is requested is punishable under the domestic law of both the requesting and requested states. This represents a straightforward application of what is stipulated in Article 35(3) of the Convention concerning dual criminality in the context of international cooperation procedures under the new Convention.

Despite the text in that article stating that extradition applies to all acts as long as they are punishable under the domestic law of both the requesting and requested states, it also provides that a State

49 Islam Serour, Extradition of Foreigners in Terrorism Cases, A Comparative Study in Light of International Conventions, Dar al-Fath for Printing and Publishing, Alexandria, (2024), p 168.

Party whose law permits it may agree to extradite a person for any of the acts criminalized under this Convention, even if such acts are not punishable under its domestic law. This is considered consensual extradition and does not conflict with the principle of dual criminality stipulated in the Convention.

Furthermore, a state's accession to the Convention imposes upon it the obligation to regard acts that are considered crimes under its provisions as offenses that threaten international peace and security due to the widespread nature and impact of cybercrimes, and perpetrators must be pursued wherever they may be.

The new Convention states that when extradition is requested to carry out a final judgment of imprisonment or other detention related to a crime for which extradition is allowed, the requested State may approve it according to its law. If the request covers multiple crimes, extradition may be granted for at least one, even if not for all, due to sentencing considerations. If these crimes are linked to acts criminalized under the Convention, the requested State may apply this article if the extradition requirements are met. Some laws also specify a minimum duration or penalty for crimes to qualify for extradition.⁵⁰

The Convention rightly confirmed that any crime to which the Convention applies is considered among the crimes eligible for extradition under any existing extradition treaty between the State Parties.

It requires State Parties to include cybercrime in the list of extraditable offenses in all extradition treaties, thereby simplifying procedures and speeding up justice. The article also states that a State Party can use this Convention as the legal basis for extradition if domestic law demands an extradition agreement. It

50 Islam Serour, *Extradition of Foreigners in Terrorism Cases, A Comparative Study in Light of International Conventions*, Dar al-Fath for Printing and Publishing, Alexandria, (2024), p 146.

encourages states that require treaties for extradition to negotiate agreements with other Parties if they do not see the Convention as the legal basis.⁵¹

Also, the Convention aligns with international standards on extradition and respect for sovereignty. If a State does not extradite a national for a Convention crime, it must refer the matter without delay for prosecution, treating it as a domestic offense. States must cooperate on procedural and evidentiary issues to ensure effective prosecution. Additionally, if an extradition request for enforcing a judgment is denied because the person is a national, the requested State may consider enforcing the judgment if the law allows.

The Convention clarifies that extradition is not obligatory if the request is made to target someone based on gender, race, religion, nationality, ethnicity, political opinions, or if fulfilling the request

51 Some legal scholars have argued regarding the extent of a state's obligation to extradite in the absence of an extradition treaty, stating that: *"Some international law scholars view extradition as an act of cooperation in the realm of justice. When a state extradites a suspect or a convicted individual to another state, it is thereby extending a hand of assistance to that state, allowing it to apply its criminal law to the perpetrator of a specific crime. Naturally, extradition in itself is not considered a punishment, and the state carrying out the extradition is not exercising its right to punish. The judgment or decision on the incident and the resolution of the case that forms the basis of the extradition request is carried out through a comprehensive investigation of the crime upon which the extradition request is based, completing its validity and revealing the full and clear truth if conducted in the place where the crime occurred. In fact, the current state of international community organization still necessitates continuing to consider extradition as a requirement for safety, security, and global order, especially now that it has become easy for any criminal to cross the borders of the country where the crime was committed into another country, continuing to commit crimes, particularly if they are part of an organization or terrorist group involved in organized crime through criminal networks spread across several countries. This allows the perpetrator and their accomplices to escape justice outside the state and evade punishment, especially if the state where they reside applies the concept of territorial jurisdiction concerning crimes."* **For more on legal perspectives concerning the extent of a state's obligation to extradite, refer to:** Islam Serour, *Extradition of Foreigners in Terrorism Cases, A Comparative Study in Light of International Conventions*, Previous Reference, p. 76.

would harm their status.⁵²

One of the aspects that should be discussed concerning the extradition framework outlined in the Convention is its provision regarding financial crimes. The Convention explicitly states that State Parties may not refuse an extradition request solely on the grounds that the crime also involves financial matters.

According to international private law jurisprudence, these crimes are typically excluded from extradition and are referred to as economic and financial crimes. In its broadest sense, this term is defined as “any act or omission punishable by law or contrary to the state’s economic policy.”⁵³ The severity of economic crimes depends on the country’s political state, increasing during wartime. The concept is linked to the political system and the violated interest. Examples include tax evasion, currency counterfeiting, embezzlement, and crimes using ICT for financial goals. Notably, the dual criminality requirement is often unmet in financial crimes, complicating extradition, due to differing economic systems and legal definitions among states.⁵⁴

The exclusion of economic crimes from extradition is rooted in differing perceptions among states and can harm national economies. Many countries exclude these crimes to protect economic stability, ensuring the return of suspects and the enforcement of legal punishments.⁵⁵

The new Convention adopts a broader, modern approach to

52 Islam Serour, *Extradition of Foreigners in Terrorism Cases, A Comparative Study in Light of International Conventions*, Previous Reference, p. 184.

53 Dr. Zaki Mohamed Al-Najjar, “Economic Growth and Crime: Marginal Criminal Phenomena and Methods of Combating Them,” published in *Public Security Journal*, Egypt, Issue 166, Vol. 41, July 1999, p. 129.

54 Dr. Mahmoud Naguib Hosni, *Explanation of the Penal Code, “General Section”: The General Theory of Crime and the General Theory of Punishments*, Dar Al-Nah-da Al-Arabiya, Cairo, Egypt, 4th Edition, 1983, p. 78.

55 Islam Serour, *Extradition of Foreigners in Terrorism Cases, A Comparative Study in Light of International Conventions*, Previous Reference, p. 218.

extradition, stating that requests cannot be denied solely because the crime is financial. It specifies that cybercrimes involving financial issues, such as tax evasion, customs violations, or breaches of currency laws, are extraditable. This approach, adopted by the Convention, aligns with many other international conventions, such as the *International Convention for the Suppression of the Financing of Terrorism* of 1999⁵⁶.

Similarly, the *Model Treaty on Extradition*⁵⁷ follows the same approach, mandating extradition for crimes related to state revenues⁵⁸.

The framework established by the new Convention concluded with an emphasis on the importance of a treaty-based foundation for extradition, stating the necessity for State Parties to pursue the conclusion of bilateral and multilateral agreements or arrangements to implement the extradition of Cybercrime Perpetrators according to the United Nations Convention against Cybercrime and enhance the effectiveness of procedures taken by state parties for that aim.

56 **Article 13 of the International Convention for the Suppression of the Financing of Terrorism (1999)** states: “None of the offences set forth in Article 2 shall be regarded, for the purposes of extradition or mutual legal assistance, as a fiscal offence. Accordingly, States Parties may not refuse a request for extradition or for mutual legal assistance on the sole ground that it concerns a fiscal offence.” For the full text of the Convention, refer to the following link: [United Nations Treaty Collection - International Convention for the Suppression of the Financing of Terrorism \(1999\)](#).

57 **Refer to the *Model Treaty on Extradition* issued by the United Nations, available on the official United Nations documentation website:** [UNODC - Model Treaty on Extradition](#).

58 **Article 2, Paragraph 3 of the *Model Treaty on Extradition*** states: “Where extradition of a person is sought for an offence against a law relating to taxation, customs duties, exchange control or other revenue matters, extradition may not be refused on the ground that the law of the requested State does not impose the same kind of tax or duty or does not contain a tax, customs duty or exchange regulation of the same kind as the law of the requesting State.”

The full text of the *Model Treaty on Extradition* can be accessed at the following link: [UNODC - Model Treaty on Extradition](#).

4. Conclusion

This analysis clarifies the scope of cybercrimes under the Convention, defining cybercrime as criminal activities that use computer and electronic technologies to target cyber systems, networks, and data. The Convention aims to enhance international cooperation in combating specific ICT crimes and facilitating the exchange of electronic evidence. It focuses on the means used rather than the perpetrators' intentions or identity.

Additionally, the Convention outlines various crimes involving information technology, including money laundering, corruption, terrorism, human trafficking, firearm trafficking, narcotics, cultural property, and organized crime, listing eleven criminal activities to be criminalized by member states, regardless of their specific legal terminology.

According to chapter five of the convention, international cooperation was addressed, especially extradition under Article 37, emphasizing dual criminality and following established international customs.

It allows extradition even if the act isn't a crime domestically and considers the Convention itself as an extradition agreement if both states are signatories.

The scope also extends to financial crimes, stating extradition requests shouldn't be refused solely because the crime involves financial matters, reflecting modern views on financial and economic crimes related to cybercrime.

States are encouraged to facilitate the extradition of offenders involved in the financial aspects of cybercrime.

5. Findings and Recommendations

5.1 Findings

1. The United Nations Convention against Cybercrime is the first United Nations convention to combat cybercrimes related to information and communication technology.
2. Potential crimes associated with information and communication technology cannot be overcome without identifying these crimes and working towards strengthening domestic legal systems to criminalize acts connected to these mechanisms.
3. All crimes that fall within the scope of the Convention's application are subject to extradition and international cooperation in light of the implementation of its provisions, as well as crimes stipulated in any other agreements or protocols that were committed using information and communication technologies.
4. The system of extraditing criminals is a form of international cooperation based on the idea of international solidarity to suppress crimes and pursue their perpetrators across states, facilitated through judicial mechanisms and channels.
5. Political will is considered the cornerstone in determining whether or not criminals are extradited. Consequently, the effectiveness of international cooperation for the extradition of criminals, especially in the case of widespread cybercrimes, is directly linked to the political will of states in their relations with other states, as extradition and transfer for prosecution or punishment are matters related to state sovereignty.
6. The Convention stipulates that the principle of dual criminality must be considered in all international cooperation procedures.

7. Bilateral agreements between states are crucial for the success of extradition procedures for terrorists and cybercrime perpetrators.
8. Cybercrimes have negative effects on states and societies at political, economic, and social levels. Therefore, international cooperation must be strengthened to pursue offenders wherever they are and to activate the Convention's provisions on international cooperation, particularly in the context of extradition.
9. Even if states are keen on protecting their citizens, respecting their rights, and maintaining their dignity by adopting the principle of non-extradition of nationals to other states and opting for their prosecution within their own territory, if the committed crime is considered a cybercrime under the Convention's definition, the state is then obligated to impose penalties and deterrents on the perpetrators within its jurisdiction to combat such crimes and deter offenders, as well as establish strict criminal laws to confront and combat these crimes.

5.2 Recommendations

1. Domestic legal frameworks should be developed in accordance with international extradition regulations, while fully upholding human rights obligations and international standards pertaining to fair and impartial criminal proceedings.
2. A harmonized conceptual definition of cybercrime should be promoted at the international and regional levels, focusing on the criminal use of information and communication technologies, in order to enable collective deterrence and effective international cooperation.
3. National criminal legislation, particularly in the Arab region, should be modernized and continuously updated to reflect evolving methods of committing and financing cybercrimes,

ensuring that such acts are criminalized in a manner compatible with international obligations.

4. Regional and bilateral extradition agreements should be reviewed and aligned with the United Nations Convention on Cybercrime, to ensure their procedural adequacy, inclusiveness of cybercrime offenses, and effectiveness in facilitating extradition through clear channels and mechanisms.

5. States that decline extradition should be held to enhanced international accountability standards, including the effective application of the principle of *aut dedere aut judicare*, ensuring that cybercrime perpetrators are prosecuted domestically where extradition is refused in accordance with the Convention.

6. The principle of dual criminality should be applied in a flexible and functional manner in cybercrime cases, as prescribed by the Convention, in order to avoid procedural impediments arising from divergent legal classifications and terminologies among states.

REFERENCES:

1. **International Conventions and Treaties:**
 - **Arab Convention (1952) on Persons Subject to Extradition.** Available at:
<https://www.acerislaw.com/wp-content/uploads/2022/01/Arab-League-Convention-on-the-Enforcement-of-Judgments-1952.pdf>
 - **Council of Europe Convention on Cybercrime (CETS No. 185).** Available at:
<http://conventions.coe.int>
 - **Hague Convention on the Unlawful Seizure of Aircraft (1970).** United Nations Treaty Collection. Available at:
<https://treaties.un.org>
 - **International Convention for the Suppression of the Financing of Terrorism (1999).** United Nations Treaty Collection. Available at:
<https://treaties.un.org/doc/db/Terrorism/english-18-11.pdf>
 - **Model Treaty on Extradition.** United Nations Office on Drugs and Crime (UNODC). Available at:
https://www.unodc.org/pdf/model_treaty_extradition.pdf
 - **Riyadh Arab Convention on Judicial Cooperation (1983).** Available at:
<https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280527ea2>
 - **United Nations Convention against Cybercrime.** United Nations General Assembly, Seventy-ninth Session, Report of the Third Committee. Available at:
<https://digitallibrary.un.org/record/4068812?ln=en&v=pdf>
 - **Stanford Draft International Convention on Cybercrime (1999).** Stanford University. Available at:
<https://web.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf>

2. Books and Academic Theses:

- **Al-Arousi, Mahmoud Hassan.** *A Study on the Extradition of Criminals in the Egyptian System and Comparative Legislation.* Costatsoumas Press, Lebanon, 1951.
- **Al-Basha, Faiza Younis.** *Organized Crime in Light of International Agreements and National Laws.* Dar Al-Nahda Al-Arabiya, Cairo, 2001.
- **Al-Ghathbar, Khalid bin Suleiman & Al-Qahtani, Muhammad bin Abdullah.** *Information Security in a Simplified Language.* Center of Excellence for Information Security, King Saud University, 1429 AH.
- **Al-Masry, Mazhar Gebran Ghaleb.** *International Cooperation in Combating Organized Crime.* Master's Thesis, Faculty of Law, Assiut University, Egypt, 2008.
- **Boister, Neil.** *An Introduction to Transnational Criminal Law.* 2nd ed., Oxford University Press, 2018.
- **Hosni, Mahmoud Naguib.** *Explanation of the Penal Code – General Section: The General Theory of Crime and Punishment.* 4th ed., Dar Al-Nahda Al-Arabiya, Cairo, 1983.
- **Ibrahim, Mohamed Abu Al-Fath.** *Combating Organized Crime in Light of International Treaties.* PhD Thesis, Menoufia University, Egypt, 2010.
- **Samhan, Abdul Rahman Fathi.** *Extradition of Criminals under the Rules of International Law.* Dar Al-Nahda Al-Arabiya, Egypt, 2011.
- **Serour, Islam.** *Extradition of Foreigners in Terrorism Cases: A Comparative Study in Light of International Conventions.* Dar al-Fath for Printing and Publishing, Alexandria, 2024.
- **Siraj, Abdel Fattah Mohamed.** *The General Theory of Extradition.* Dar Al-Nahda Al-Arabiya, Cairo, 1998.
- **Sorour, Ahmed Fathi.** *Constitutional Legitimacy and Human Rights in Criminal Procedures.* Dar Al-Nahda Al-Arabiya, Cairo, 1993.

- **Youssef, Ihab Mohamed.** Extradition Treaties and Their Role in Achieving International Cooperation to Combat Terrorism. PhD Thesis, Police Academy, Cairo, 2003.

3. Journal Articles and Research Papers:

- **Allahrakha, N. (2024).** Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, 2(5), 28–36.
- **Brenner, S. (2004).** Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law and Technology*, 9.
- **Broadhurst, R. (2006).** Development in the Global Law Enforcement of Cybercrime. *Policing: An International Journal*, 29(2).
- **Brown, I., Edwards, L., & Marsden, C. (2009).** Information Security and Cybercrime.
- **Carter, D. (1995).** Computer Crime Categories. *FBI Law Enforcement Bulletin*.
- **Chawki, M. (2005).** Cybercrime in France: An Overview.
- **Dugard, J. & Van den Wyngaert, C. (1998).** Reconciling Extradition with Human Rights. *American Journal of International Law*, 92(2).
- **Gercke, M. (2006).** The Slow Wake of a Global Approach Against Cybercrime. *Computer Law Review International*.
- **Gercke, M. (2008).** National, Regional and International Legal Approaches in the Fight Against Cybercrime. *Computer Law Review International*.
- **Gercke, M. (2012).** Understanding Cybercrime: Phenomena, Challenges and Legal Response. *ITU*.
- **Goodman, M. & Brenner, S. (2002).** The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*, 10(2).
- **Lusthaus, J. (2013).** How Organised Is Organised Cybercrime? *Global Crime*, 14(1). Phillips, K. et al. (2022).

Conceptualizing Cybercrime. Forensic Sciences, 2(2).

- **Priyandita, G.** (2024). The UN Cybercrime Convention: A Victory for State Sovereignty. ASPI.

4. Online Platforms and Websites:

- Wafeer Knowledge and Medicine, “The Concept of Cybercrimes, Their Types, Methods of Commitment, and Ways to Combat Them.” Available at: [Wafeer Platform] (https://doafeer.net/concept_cybercrimes_types_committing_combating/)

5. Reports, Resolutions, and Official Documents:

- Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: <https://digitallibrary.un.org/record/432653?v=pdf>.
- Cybercrime, Report of the Parliamentary Joint Committee on the Australian Crime Commission, 2004, page 5, available at: [Reports on Annual Reports – Parliament of Australia](#)
- Explanatory Report to the Council of Europe Convention on Cybercrime, No. 1 available at: <https://docslib.org/doc/۲۹۶۴۳۲۲/explanatory-report-to-the-convention-on-cybercrime>
- Recommendations of the Tenth International Congress of Criminal Law, published in the National Criminal Journal, National Center for Social and Criminal Research, Vol. 13, Issue 1, March 1970, and available on the Egyptian Knowledge Bank (<http://www.ekb.eg>)
- Sieber in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004, page 86 <https://doi>.

- [org/10.1007/s12117-005-1036-6](https://doi.org/10.1007/s12117-005-1036-6)
 - The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: <https://digitalcommons.lmu.edu/do/search/?q=cybercrime&start=0&context=2236248&facet=>
 - United Nations resolution on combating the use of information and communications technologies for criminal purposes: Report of the Third Committee: General Assembly, seventy-ninth session. Available at: [UN Digital Library] (<https://digitallibrary.un.org/record/4068812?ln=en&v=pdf>)
 - United Nations Regional Office on Drugs and Crime for the Middle East and North Africa: <https://www.unodc.org/romena/en/cybercrime.html>
 - Voce, Isabella & Morgan, Anthony & Australian Institute of Criminology. (2023). Cybercrime in Australia 2023 / Isabella Voce, Anthony Morgan. Canberra, Australian Capital Territory: Australian Institute of Criminology, available at: <https://doi.org/10.52922/sr77031>
 - Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress, 2007, Updated January 29, 2008, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf
6. Legal Case Studies:
- **Dotcom et al. v. United States (Case Study 5).** UNODC. (<https://www.unodc.org/e4j/en/organized-crime/module-11/exercises/case-studies.html>)