Human Rights and Public Liberties Review
(H.R.P.L.R)

Vol° : 09- N° : 02 An :2024
p.p : 16 - 46

Mechanisms of international law to confront cyber terrorism

review of risks and ways to confront-

Dr- Boukourou manel

Constantine 1 University - Brothers Mentouri, constantine / Algeria

manel.boukourou@umc.edu.dz

Received: 31/08/2024 Accepted: 29/09/2024 Published:20/12/2024

Abstract:

The emergence of cyberterrorism as a new form of transnational international terrorism has led to the rise of new types of crimes committed by criminal groups or individuals in the digital space. These include hacking websites and infiltrating sensitive national information systems with the intent to disrupt, alter, or destroy data. This has driven the international community to seek effective legal and institutional mechanisms To stop these escalating threats.

Keywords : cyber terrorism; digital space, dangers, response mechanisms, legal framework, institutional framework

1. INTRODUCTION

Today, cyberterrorism has become a significant threat to international peace and security, especially with the major advancements in computer programs that allow for the rapid and covert infiltration and destruction of data anywhere in the world within seconds. Additionally, the proliferation of thousands of chat sites and social media platforms on the internet has turned the world, across its five continents, into a small village. All these technological advantages in cyberspace

*Corresponding author. –

provided by modern technology have become a major attraction for terrorist organizations from different parts of the world, regardless of the differences in the types of these groups and the diversity of their religious and ideological orientations, to enter this field and use it against hostile states and governments by spreading disinformation, eavesdropping on the conversations of influential figures in the state, and spreading panic or demanding ransom.

Cyberspace is also used for propaganda, psychological warfare, military and media recruitment, in addition to using the internet for fundraising and information gathering, coordinating terrorist attacks, and mobilizing sympathizers from various parts of the world. Furthermore, cyberspace is also used for direct attacks on cyber infrastructure, such as computers, networks, and stored information, to disrupt the functions of information systems, damage or destroy virtual and physical assets, block government ministry websites, and disrupt daily life by targeting critical infrastructure such as medical facilities, stock exchanges, banks, and international financial transactions, to erode trust in the economic system, disrupt and interfere with communication networks, prevent or delay the flow of funds, redirect deposits, shut down power plants, attack air traffic control systems, railway systems, or even shut down nuclear reactors and tamper with missile launch platforms, among other things.

All these terrorist operations can be carried out easily from anywhere in the world, covertly, without the perpetrator needing to be at the site of the attack. Moreover, cyberterrorist operations do not require massive financial resources due to the low cost of the internet. A single computer and a specialized individual are enough to launch harmful software by spreading viruses and erasing the memory of hostile devices quickly and

effortlessly, often in just minutes. Furthermore, cyberterrorist activities conducted through the network can remain anonymous and untraceable by using techniques that camouflage and falsify digital evidence and locations, making it easier to attack government and security sites without facing legal consequences.

An example of terrorist organizations that have established cyber armies is ISIS, which has enhanced its cyber capabilities with the "Caliphate Cyber Army," "Kalashnikov E-Security," and "The United Cyber Caliphate Hacker Group." These groups have successfully hacked into several government sites, including the UK's Ministry of Health, the Royal Malaysian Police, Malaysia Airlines, the French TV network TV5, and the U.S. Central Military Command.These modern threats have driven the international community to seek effective mechanisms to combat cyberterrorism. These efforts first became visible in 1981 when Interpol discussed the possibility of establishing an international convention to combat cybercrime. However, this idea has yet to be realized, leaving the United Nations Convention against Transnational Organized Crime of 2000 as the only existing instrument addressing cross-border crime. In addition, the 2001 Budapest Convention on Cybercrime by the Council of Europe aims to enhance international cooperation in this domain.

A global strategy for cybersecurity protection has also been adopted through various initiatives, most notably the International Multilateral Partnership Against Cyber Threats (IMPACT), which focuses on sharing and securing cybersecurity. Other modest initiatives have been implemented at national, bilateral, regional, and international levels to address cyber threats and facilitate the sharing of intelligence in new ways. The United Nations Office on Drugs and Crime (UNODC) team has organized a series of conferences since 2010, involving governments and international and regional

organizations to study the risks of using the internet for terrorist purposes and to explore countermeasures.

This study aims to understand the nature of cyberterrorism and the threats it poses to international security and peace, then to identify the most significant international efforts to counter this phenomenon in the context of the legal void addressing this new form of terrorism. This gap has made establishing an international legal and institutional framework to combat cyberterrorism and creating effective cooperation mechanisms for intelligence sharing and developing tracking and investigation technique for cybercrimes a major challenge for the international community today. Thus, the study's central question is framed as follows:

What role does international law play in countering the threats of cyberterrorism to global security and peace in light of the legal void that currently exists in combating this emerging crime and mitigating its risks?

To answer this question, the study is methodologically divided into two main sections :

- **The first section** : The conceptual framework of cyberterrorism.
- **The second section** : International mechanisms to combat cyberterrorism.

Section One : The Conceptual Framework of Cyberterrorism

Cyberterrorism is considered one of the most dangerous crimes threatening international security and peace, as it is a transnational crime that can easily target any military or civilian objective, endangering public safety and the stability of social and economic life in

any country around the world. This is why this section is dedicated to defining this type of terrorism and identifying its causes and risks.

1. Definition of Cyberterrorism and Its Characteristics:

Cyberterrorism is a modern phenomenon that has emerged from the information revolution in our contemporary world, using the internet as the stage for its crimes. This network does not recognize international borders and is difficult to subject to any legal oversight. Cyberterrorism involves a series of attacks carried out by a terrorist organization or hacker against a state, group, or several individuals residing in one or multiple countries. The purpose is to demand ransom, intimidate, or coerce governments or populations into accepting a political, social[1], or ideological agenda using electronic operations. These operations involve infiltrating unauthorized websites with the intent to disrupt, destroy, or take control of the available data. The cyberterrorist only needs a laptop screen and high-speed internet to attack any target worldwide, making it a cross-border crime with an inherently international nature.[2]

In this context, **Dr. Raghda Al-Bahi** defines cyberterrorism as "the illegal threat or attack by terrorists who launch attacks on computers,

[1] Bandar Aqab Darwish, Proof in Cyberterrorism Crimes, Master's thesis, Islamic Sciences University, Amman, Jordan, 2018, p. 16.

[2] - Abdul Rahman bin Abdullah Al-Sind, Means of Cyberterrorism and Their Rulings in Islam and Methods of Combating Them, World Conference organized by Imam Muhammad bin Saud Islamic University, 2004, p. 8.

information systems, software, and data with the aim of intimidating and coercing governments to achieve various objectives."[3]

However, Neil Walsh, Head of the Cybercrime Section at the United Nations Office on Drugs and Crime (UNODC), stated in an interview with Al Jazeera on June 5, 2019, that there is no unified definition of cyberterrorism due to political reasons, leaving the matter to national legislations and regional efforts. In this regard, the Council of Europe's Budapest Convention on Cybercrime, concluded in 2001, defines cyberterrorism as "illegal attacks or threats of attacks against computers, networks, or electronically stored information, aimed at revenge, extortion, or forcing governments, populations, or the international community as a whole to achieve political, religious, or social goals using various digital weapons," including:[4]

- **Cyber Viruses:** These are types of malicious software created by terrorists to alter the properties of digital files. Viruses replicate by copying their source code and regenerating themselves or by infecting a computer program, modifying or damaging its properties. Some of the most well-known include:Boot Sector - Web Scripting Virus -

[3] - Raghda Al-Bahy, Cyberterrorism: Concept, Characteristics, and Patterns, Egyptian Center for Thought and Strategic Studies, 2019, p. 01.

[4]- Computer Viruses. Wayland University. Available at: https://www.wbu.edu/wbu-online/current-students/computer-viruses.htm

Browser Hijacker -Resident Virus. - Direct Action Virus.- Polymorphic Virus. - File Infector Virus-Multipartite Virus.

- **Electronic Worms :**These are electronic programs sent via the internet to hack personal data or disrupt internet connections, aiming to disable critical facilities or institutions in a particular country.
- **Trojan Horse:**This is a code embedded in programs designed to delete data from any targeted institution. It is one of the fastest-spreading and most easily distributed weapons across any device.
- **Chips:**These are tools used to control a computer by connecting them to the source and then remotely controlling them.
- **Electronic Bombs:** These are electromagnetic pulses dropped onto a sensitive electronic site, causing an explosion that leads to the immediate erasure of data and information from any electronic device. This is known as an electromagnetic explosion caused by sudden fluctuations in the magnetic field.Among the most well-known types of malicious software spreading in cyberspace are **Ransomware Attacks**, which include two main types: encryption programs, which encrypt data, documents[5], and images on a computer, and blocking programs, which prevent access to the targeted device's files.Based on the above, cyberterrorism can be defined as

[5] -Mamdouh Abdelhamid Abdelmottaleb, *Crimes Using the World Wide Web (Internet Crime): A Security Perspective*, paper presented at the Conference on Law, Computers, and the Internet organized by the College of Sharia and Law in collaboration with the Emirates Center for Strategic Studies and Research and the Information Technology Center at the United Arab Emirates University, May 1-3, 2000, p. 42.

an illegal a[6]ct carried out by a terrorist organization or a group of individuals to intimidate, extort, or deceive using information networks to disrupt the functions of government websites, financial institutions, or administrative bodies. This is done through computer viruses to hack sites, disrupt daily life, and target infrastructure such as medical facilities, stock exchanges, financial systems, water or electricity supplies, or communication services.

Key Aspects of Cyberterrorism:

a. Security Aspect :

Terrorist groups commit digital crimes aimed at threatening the national security of states, such as disrupting communication networks, or economic life by attacking financial institutions, health facilities, military sites, or disrupting air and maritime navigation systems, and redirecting or launching missiles to other targets.

b. Political Aspect:

Cyberterrorist groups aim to spread fear for political purposes, intending to create chaos and disclose politicians' secrets.

Cyberterrorism is characterized by several features that distinguish it from traditional terrorism, which we will address below:

- **Cyberterrorism is a Recent Phenomenon:**

  Cyberterrorism differs from traditional terrorism through its tools, relying on electronic weapons that emerged and evolved due to the

6

information revolution in our contemporary world. This makes it a newly developed crime that has appeared after significant advances in communication technologies and digital programs.[7]

- **Cyberterrorism is a Transnational Crime :**

  Cyberterrorism is one of the most transnational crimes, crossing borders and continents due to the nature of the weapons used in attacks by hackers in the digital space. This allows terrorist organizations to carry out attacks across different geographical locations without being constrained by borders or security agencies, and without the risk of arrest. This contrasts with traditional terrorism, which requires physical presence at targeted sites for bombings, shootings, or kidnappings.[8]

- **Cyberterrorism is Difficult to Prove:**

  Cyberterrorism is one of the most challenging types of terrorism to trace back to its source or perpetrators, similar to bioterrorism, due to the difficulty of obtaining tangible evidence and the ease of hiding in the digital space. Especially when the cyberterrorist is highly skilled, it becomes difficult to identify them. Terrorists can easily change their IP addresses, which security agencies typically use to track criminals

[7] Khaled Mamdouh Ibrahim, *Cybercrimes*, Arab Thought House, Alexandria, 2009, p. 68.

[8] Abdul Rahman Abdulaziz Al-Shunaifi, Information Warfare, Gharib Office, Saudi Arabia, 1991, p. 113.

online. They also often use pseudonyms to log into various websites with anonymous identities to recruit others.[9]

Additionally, the digital space is not bound by national borders (such as checkpoints or customs), and the varying laws applied in different countries, along with the lack of a unified definition of cyberterrorism, have made it easier for terrorists to operate in cyberspace.

-Ease of Committing Cyberterrorism and Its Low Costs:

Cyberterrorism attracts many amateurs and professionals in the digital space due to its ease of execution. A terrorist only needs a computer and a high-speed internet connection to attack and hack any site in this vast world. This makes it very cost-effective compared to traditional terrorism, which requires significant financial resources to purchase weapons, mines, and explosives, pay terrorists, and cover travel expenses, military training programs, and the considerable losses in personnel and equipment that traditional terrorist organizations face. Cyberterrorism, on the other hand, incurs no such losses.[10]

-Diversity of Cyberterrorism Targets: Cyberterrorism has multiple targets depending on the intended objectives, whether these are military, public facilities, banks, healthcare institutions, transportation systems, energy supplies, or emergency services.

[9] Khaled Younes Arab, *Computer Crimes*, Master's thesis, Jordan University, 1994, p. 81.

[10] - Mahmoud Ahmed Ababneh and Mohd Omar Al-Rizaki, Computer Crimes and Their International Dimensions, Dar Al-Thaqafa, Amman, 2009, p. 30.

-Speed of Cyberterrorism Attacks: Cyberterrorism is one of the fastest forms of terrorism in terms of launching attacks. This is facilitated by the types of weapons used, such as viruses, worms, and electronic bombs, which can be easily deployed to target a specific site within seconds, especially if internet speed is very high. This enhances the spread and effectiveness of these harmful programs.[11]

II. Motivations and Dangers of Cyberterrorism : The scientific advancements in digital fields have contributed to the spread and variety of cyberterrorism due to the wealth of digital technologies. This has led to an increase in cybercrime rates, especially among marginalized youth who are excluded from social and political participation, creating a significant gap in society due to unemployment and exclusion. Some are driven to seek quick profits and join terrorist groups to earn substantial sums by blackmailing victims and destroying their files.[12]

On the other hand, the difficulty of monitoring the digital space is a major reason terrorists resort to this new form of terrorism to spread their extremist ideas and attack any entity opposed to their political, national, or religious ideologies. This makes the information network easily susceptible to breaches by terrorist organizations due to the absence of security barriers and borders, allowing access to any site

[11] - Raghda Al-Bahy, Op. Cit., p. 8

[12] - Hanin Bouadi, *Experiences in Countering Terrorism*, University Thought House, Alexandria, 1st ed., 2004, p. 16.

without permission or authorization. Additionally, the digital space offers an opportunity to showcase talents and expertise in accessing and hacking sites for profit, political, or terroristic purposes.[13]

Cyberterrorism poses an imminent and real threat to international peace and security and a severe risk to information systems anywhere in the world. The losses it can cause are far greater than those from conventional terrorist bombings. For example, 2017 was one of the worst years in human history in terms of cyberattacks, with approximately 2 billion digital records stolen. Ransom payments amounted to around 2 billion dollars as a result of the largest cyberattack globally, which affected 99 countries, including the United States, the United Kingdom, Ukraine, India, and Russia. The attack exploited a security flaw in Microsoft's software, targeting healthcare institutions in the UK, forcing the cancellation of all scheduled surgeries. The Russian Ministry of Defense also suffered significant damage.[14]

Thus, cyberterrorism primarily targets military sites, destroys infrastructure, breaches air, sea, and land navigation systems, alters or destroys military data and paths, controls missile or energy stations and

[13] - Abdullah Al-Aseeri, *Terrorism and Maritime Piracy*, Naif Arab University for Security Sciences, Riyadh, 1st ed., p. 236.

[14] Ahmed Khalifa Al-Maltt, *Cybercrimes*, University Thought House, Alexandria, 1st ed., 2018.

dams, spreads false information, and tarnishes the reputation of national symbols by disseminating misleading information via social media during election campaigns. It can also wage psychological warfare on victims by sending threatening emails or phone messages, leading to various consequences.

- **Damage or Corruption of Information on Websites:**This involves causing harm to or corrupting information stored on websites.
- **Physical Damage to Targeted Computers:**This includes disabling and paralyzing the functionality of targeted computers, such as with the "Friday Virus" that spread in the UK banking sector.

III. Methods of Cyberterrorism: Cyberterrorism employs various methods, including the following:

- **Email**

Email is one of the most commonly used communication tools due to its ease of sending and reading messages. This makes it an attractive option for terrorist groups to communicate between recruits and cells located anywhere in the world, exchange information among terrorists, and plan cyber operations. Emails can also be targeted for espionage purposes, especially against important figures in governments, to assist in cyberattacks.[15]

[15] Abdul Rahman bin Abdullah Al-Sind, Means of Cyberterrorism and Their Rulings in Islam and Methods of Combating Them, World Conference on Islam's Position, Imam Muhammad bin Saud Islamic University, 2004, p. 35

- **Creation or Destruction of Websites:** Terrorists may destroy websites by hacking and destroying data from any point in the world through the use of viruses or pressure programs that target stored information, preventing site browsing. On the other hand, terrorists also create hidden websites to spread their extremist ideas or promote vice in society through easily accessible programs.[16]
- **Hacking Security Systems of Websites:** Terrorist groups often hack security systems to obtain classified information or destroy government or private institution websites. They achieve this by using viruses with codes capable of easily penetrating security systems and damaging government or private information held by companies or organizations, such as the terrorist hacking of the U.S. Department of Defense and targeting military documents.[17]
- **Planning and Media Promotion for Cyberterrorist Groups:** Terrorist groups that use digital space as an attack platform seek to avoid physical meetings between their members by utilizing social media platforms for communication, planning, and disseminating statements and extremist terrorist ideas. They also spread false and misleading information to the security agencies of targeted countries, propagate a

[16] - Moza Al-Mazrouei, *Electronic Inventions: A Dangerous Challenge*, *Economic Horizons* magazine, United Arab Emirates, Issue 09, 2012, p. 45.

[17] - Zain Al-Abidin Awad Kazem Al-Kurdi, *Terrorism Crimes*, Al-Halabi Legal Publications, Beirut, 2018, p. 111.

culture of violence among youth, and intimidate societies. For example, the spread of Daesh videos containing shocking scenes, like the beheading of Coptic hostages in Egypt, promotes extremist ideologies, secures financial and logistical support, and facilitates illegal financial transactions for purchasing computers, malicious software, or engaging in money laundering related to human trafficking, drug dealing, and white slavery.[18]

-The second section : International mechanisms to combat cyberterrorism.

Cyberterrorism emerged and its risks increased with the development of the new digital space, necessitating the creation of legal and institutional cooperation frameworks to combat this new form of terrorism, particularly given its spread across all segments of society, especially among the youth. This spread was further facilitated by the use of electronic platforms for expressing citizens' opinions.The use of social media services such as Facebook and Twitter has made it easier to promote youth activities, as well as demonstrations and protests. However, this significant advancement in the digital space has not been matched by clear legal and institutional frameworks. This gap has raised several concerns, especially with the increase in cyberattacks on various countries and associated internet crimes. This has intensified the focus

[18] - Walid Mohamed Awriya, *Understanding Cyberterrorism*, Naif Arab University for Security Sciences Publications, Riyadh, 2012, p. 53.

of countries on the issue, leading to numerous initiatives by various international organizations, including

On the legal front, the European Convention on Cybercrime, signed in Budapest in 2001, is noteworthy. This convention aims to combat internet crimes, which are a collection of illegal or unauthorized activities related to the use of the internet, and is considered one of the most significant agreements addressing this issue.

Firstly - Institutional Framework for Combating Cyberterrorism:

International organizations are working diligently to combat cyberterrorism due to its significant threat to both national and international collective security. They have issued numerous recommendations for member states. The key international bodies involved include:

A - International Organizations :

-United Nations General Assembly Resolutions:

Since 1990, the United Nations General Assembly has issued several resolutions to address cyberterrorism. It also published a guide on preventing and combating computer-related crime in 1994. Key resolutions include:Resolution 45/121 of 1990-Resolution 53/70 of December 4, 1998-Resolution 54/49 of December 1, 1999-Resolution 55/28 of November 20, 2000-Resolution 56/19 of November 29, 2001-Resolution 57/53 of November 22, 2002-Resolution 58/32of December 18, 2003, on "Developments in the Field of Information and

Telecommunications in the Context of International Security"-Resolution 55/63 of December 4, 2000-Resolution 56/121 of December 19, 2001 on "Combating the Use of Information Technology for Criminal Justice Purposes"-Resolution 57/239 of December 20, 2002 on "Creating a Global Culture of Cybersecurity"-Resolution 57/239 of January 31, 2003-Resolution 58/199 of January 30, 2004 on "Creating a Global Culture of Cybersecurity"

These resolutions call on member states to cooperate and enhance a culture of cybersecurity. Additionally, the UN has issued several resolutions related to digital space security, including resolution CCPCJ 16/2/2007 from April 2007 on "Effective Crime Prevention and Criminal Justice Measures to Combat the Sexual Exploitation of Children" (paragraphs 7, 16).

Economic and Social Council Resolution E/2007/20 of July 26, 2007 : Titled "International Cooperation to Prevent, Investigate, and Prosecute Economic Fraud and Identity-Related Crimes" (E/2007/30 and E/2007/SR.45).

Economic and Social Council Resolution 2004/26 of July 21, 2004: Titled "International Cooperation to Prevent, Investigate, and Prosecute Fraud, Identity Misuse, Counterfeiting, and Related Crimes."

Paragraph 18 of the "Vienna Declaration on Crime and Justice: Meeting the Challenges of the 21st Century," adopted by the General Assembly in resolution 55/59 of December 4, 2000, and paragraph 36 attached to General Assembly resolution 56/261 of January 31, 2002,

concerning "Action Plans for Implementing the Vienna Declaration on Crime and Justice: Meeting the Challenges of the 21st Century."

Paragraphs 15 and 16 of the Bangkok Declaration on "Synergies and Cooperation: Strategic Alliances in Crime Prevention and Criminal Justice," adopted by General Assembly resolution 60/177 of December 16, 2005.

Recommendations from the Workshop Conference on "Measures to Combat Computer-Related Crime," held in Bangkok on April 22, 2005, as part of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice. Paragraph 2 of General Assembly resolution 60/177, which called on governments to implement all recommendations adopted by the Eleventh Congress.

Resolution 48/5 of the Commission on Narcotic Drugs: Regarding "Enhancing International Cooperation to Prevent the Use of the Internet for Narcotic-Related Crimes."

Paragraph 17 of General Assembly resolution 60/178 of December 16, 2005: Concerning "International Cooperation to Combat the Global Drug Problem."

- **Resolution 43/8 of the Commission on Narcotic Drugs, March 15, 2000:** On the topic of "Internet Drug Trafficking."
- **Economic and Social Council Resolution 2004/42:** Concerning "Legal Drugs Subject to International Control Sold to Individuals via the Internet."

- **Various Recommendations from Subcommittees of the Commission on Narcotic Drugs:** Addressing issues related to drug trafficking and matters concerning the Middle East and North Africa.

B. Specialized International Agencies:

Specialized agencies are dedicated to combating cyber terrorism and addressing its risks. The most notable of these include:[19]

- **International Telecommunication Union (ITU):** The ITU includes 192 countries and 700 private sector and academic institutions. As a specialized agency of the United Nations, it helps countries agree on common principles for information technology and communication infrastructure. The ITU has developed a plan to enhance global cybersecurity, based on seven goals:
  1. Develop clear strategies for international and national legislation to protect cybersecurity.
  2. Formulate national and regional strategies to create institutional mechanisms to combat internet crimes.
  3. Establish a global monitoring and early warning system for cyber crimes.
  4. Create a global digital identity.
  5. Build human and institutional capacities in the information technology field.

[19] - Ahmed Amin Al-Shawabkeh, Computer and Internet Crimes: Information Crime, Dar Al-Thaqafa, Amman, Jordan, 2004, p. 74.

6. Enhance international cooperation in cybersecurity.
7. Develop security standards and protocols for software applications and information systems.[20]

-Group of Eight (G8):

The G8 justice and interior ministers, in their various meetings, adopted several measures to combat cybercrime. These measures include:

- **Preventing Safe Havens:** Ensuring that cybercriminals do not find safe havens and are pursued and prosecuted regardless of where the harm occurs.
- **Criminalizing Violations:** Criminalizing all human rights violations on the internet with deterrent criminal penalties.
- **Ongoing Training:** Continuously training law enforcement personnel and equipping them with modern technical tools to handle contemporary cybercrimes.
- **Institutional Efforts:** Establishing 24/7 contact centers to protect electronic data, enhancing collaboration with the private sector to ensure the security of computer networks and communication systems, and developing effective mechanisms to counter cyber attacks. This includes continuous development of cyber resources and technologies, training for law enforcement, combating online child sexual

[20] George Labaki, International Internet Treaties: Facts and Challenges, Lebanese National Defense magazine, Issue 83, 2013, p. 04.

exploitation, and enacting laws to protect intellectual property rights against counterfeiting and piracy.[21]

- **Coordination:** Ensuring ongoing internal and international coordination among all stakeholders in the private sector, academic circles, and government institutions.

Additionally, the G8 group encouraged member states to raise public awareness regarding cybercrime. To achieve these goals, several action plans and principles were established[22]

-International Law Enforcement Agencies:

-Interpol: Interpol is one of the most significant international policing mechanisms for combating transnational cyber terrorism and cybercrime. It facilitates cooperation among member countries' police forces by standardizing extradition procedures, data collection, information exchange, investigation processes, and the pursuit and extradition of criminals. Interpol achieves these goals through various means, including disseminating warnings and alerts containing intelligence on cyber terrorism, maintaining an international notice system, providing expertise and training in combating cybercrime, and

[21] - For more details, refer to the Ministry of Europe and Foreign Affairs website at: https://www.diplomatie.gouv.fr/ar/politique-etrangere-de-la-france/%

[22] **-1997:** Action Plan on High-Tech Crime and Computer Crimes.-**1999:** Principles regarding the access to information stored on computers beyond national borders.-**2002:** Recommendations for tracking communications across borders in terrorism and criminal investigations.-**2002:** Principles for ensuring the availability of essential data for public safety.

storing and distributing criminal data to member countries in the form of guidance manuals and training resources on internet crimes and their prevention.[23]

-International Web Police: Founded in the United States in 1986, this organization is dedicated to tracking cybercriminals and their activities in the digital space. It handles user complaints and provides evidence to law enforcement agencies. The organization consists of 61 countries, comprising law enforcement bodies and police officers.[24]

-Internet Crime Complaint Center (IC3): Established in the United States on May 18, 2000, this center collaborates with the FBI and the National White Collar Crime Center to receive and track cybercrime reports.

Second - International Legal Framework for Combating Cyber Terrorism: Recommendations and international agreements are crucial tools in international cooperation to combat cybercrime. These include:

-European Council Recommendations: Due to the rapid advancements in information technology and the accompanying covert cyber crimes across several European countries, the European Council

[23] - Fahd Abdullah Al-Obaid Al-Azmi, Cybercrime Procedures, Dar Al-Jamia Al-Jadida, Egypt, 2016, p. 651.

[24] Sheikha Hussein Al-Zahrani, International Cooperation in Facing Cyber Attacks, University of Sharjah Journal of Legal Sciences, Volume 17, Issue 01, 2019, p. 746.

issued Recommendation No. 13/95 on September 11, 1995. This recommendation urged member states to review and update their national criminal procedural laws to keep pace with technological developments. It emphasized allowing laws to permit searches of computer systems, monitoring information, inspecting software, and detailing seized information, with the possibility of extending searches to other devices. Surveillance and recording procedures in criminal investigations should be applied when necessary.[25]

. With adherence to confidentiality, these recommendations require government employees to cooperate with investigative authorities in conducting surveillance and recording. The recommendations also urge European countries to standardize the handling of electronic evidence, establish specialized units for combating computer crimes, and retrain personnel in the judiciary[26]

B – Budapest Convention on Cybercrime : The European Parliament adopted the Budapest Convention on Cybercrime on November 23, 2001, in the Hungarian capital. This convention has been ratified by 30 European countries, as well as Canada, Japan, South Africa, and the United States. It is the first treaty aimed at combating computer crimes by coordinating national laws among its member states. The convention

[25] *Op. Cit.*, p. 747

[26] - Medhat Ramadan, Crimes of Assault on Persons and the Internet, Dar Al-Nahda Al-Arabia, 1st ed., 2000, p. 80.

uses several terms to describe criminal activities, including:Cyberterrorism-Cyberwarfare-Cybermoney laundering-Phishing-Although it is a European convention, it is open to countries outside the continent. The convention consists of 48 articles divided into 4 chapters:

Chapter 1: Definitions of terms related to the convention

Chapter 2: Measures taken at the local level, divided into two sections:

-Section 1: Substantive criminal law, which includes:

-Crimes against privacy and the integrity of computer data, such as unauthorized access (hacking), data espionage, illegal interception, and interference with data and computer systems.

-Crimes related to copyright and trademarks, which include:

-Sharing songs, files, and software protected by copyright through file-sharing programs-Circumventing digital rights management systems-Using trademarks in criminal activities to deceive-Crimes related to domain names-Computer-related fraud and deceit-Identity theft-Crimes related to content, which include:

A. Content of a sexual or pornographic nature.

B. Pornographic material related to children.

C. Data inciting racism, hatred, and glorifying violence.

D. Exposure to religions.

E. Illegal gambling and online games.

F. Defamation and false information.

G. Spam.

H. Other materials.

Section 2: Focuses on procedural law, particularly related to the preservation of stored information, evidence collection orders, search warrants, and the seizure of data stored on computer systems.

Chapter 3: International cooperation regarding the extradition of criminals, mutual assistance, and collaboration in investigations and data collection.

Chapter 4: Concerns joining and withdrawing from the treaty and resolving legal disputes.

Objectives of the Convention :

-Unify national laws in dealing with cybercrime.

-Enhance international cooperation among member states in investigation and prosecution of cybercriminals.

-Promote international collaboration in training personnel to combat cyberterrorism through comprehensive training for law enforcement officers and the development of training operations.

-Provide the required information from any party in an automated manner.[27]

[27] Munir Mohamed Al-Juhaini, Mamdouh Mohamed Al-Juhaini, *Internet and Computer Crimes and Methods of Combating Them*, Arab Thought House, Alexandria, 2004, p. 96

-Establish jurisdiction over any crime.

-Create an effective system for extraditing cybercrime suspects, facilitating the enforcement of law by the affected state, apprehending the cybercriminal, and returning them to their home country for trial. This includes obligating the state where the suspect is located to search for, investigate their identity and location, and apprehend and convict them according to its national law if their home state refuses to extradite them or denies their transfer to another state. Extradition is a crucial measure to reduce cyberterrorism, achievable through the enactment of specific extradition laws and regional and international agreements.Despite the positive outcomes achieved by the Convention as the first international treaty addressing this issue, human rights organizations have often criticized its provisions for potentially restricting individual freedoms and infringing on the confidentiality of data. Concerns include limiting the freedom of digital space users and violating their privacy under the guise of combating cyberterrorism.

Conclusion :

Cyberterrorism is a modern transnational crime that emerged and evolved with advancements in communication technologies and information technology. Its spread has been further exacerbated by the significant increase in internet users and the proliferation of devices

connected to the internet. This expansion has led to a rise in victims of cyberterrorism, as terrorists exploit the dark web, which serves as a fertile ground for their illegal activities due to the ease of encrypting user identities and using special software to hide locations. This complicates the detection of where these silent crimes are committed, making it more challenging to identify cyberterrorists, trace their locations, and prove their involvement, as evidence in the digital space can be erased with a single click on a computer. This situation amplifies the risks for countries with inadequate digital capabilities and a shortage of specialized digital skills, coupled with a decline in reporting cybercrimes, especially in the banking sector, due to fears of losing customer trust in the absence of a global legal framework to combat cyberterrorism. Additionally, new challenges such as digital currencies, artificial intelligence, and cloud computing exacerbate the issue, with the Budapest Convention of 2001 and the Arab Convention on Combating Cybercrime being notable exceptions. Some countries' adherence to sovereignty principles and respect for their citizens' digital privacy further limits efforts to combat cyberterrorism. The differences in legal and procedural systems from one country to another regarding criminalization of acts, as what may be considered a crime in one country might not be in another, impede the extradition of cybercriminals and complicate investigation and prosecution procedures.

The following are the key recommendations:

- ✓ Establish an international treaty to combat cyberterrorism supported by national legislation that is periodically updated to keep pace with developments in the digital space.
- ✓ Balance the respect for sovereignty and the protection of individual rights in the digital space with the need to combat cyberterrorism.
- ✓ Enhance international cooperation in training personnel and law enforcement authorities in the cyber domain.
- ✓ Accelerate judicial assistance procedures and exchange of cyber information.
- ✓ Provide financial resources and necessary technologies to developing countries to combat cyberterrorism.
- ✓ Adopt unified international standards for combating cyberterrorism through enhanced cooperation in the digital and judicial fields.
- ✓ Promote digital culture highlighting the importance of cybersecurity and the dangers of cybercrime to national security and international peace.
- ✓ Develop common provisions in international treaties regarding the extradition of suspects by defining criminalized acts and allowing the extradition of any cyberterrorist who has committed these acts.
- ✓ Establish mechanisms for monitoring and predicting cyber threats at national, regional, and international levels.

References

Books :

– Ahmed Khalifa Al-Malt, *Information Crimes*, University Thought Publishing, Alexandria, 1st Edition, 2018.

– Ahmed Amin Al-Shawabkeh, *Computer and Internet Crimes: Information Crime*, Dar Al-Thaqafa, Amman, Jordan, 2004.

– Bandar Aqab Darwish, *Evidence in Cyberterrorism Crimes*, Master's Thesis, Islamic Sciences University, Amman, Jordan, 2018.

– Bin Abdullah Al-Asiri, *Terrorism and Maritime Piracy*, Naif Arab University for Security Sciences, Riyadh, 1st Edition, 2014.

– Khalid Younes Arab, *Computer Crimes*, Master's Thesis, University of Jordan, 1994.

– Haneen Buwadi, *Experience in Combating Terrorism*, University Thought Publishing, Alexandria, 1st Edition, 2004.

– Khalid Mamdouh Ibrahim, *Information Crimes*, University Arab Thought Publishing, Alexandria, 2009.

– Raghda El-Behi, *Cyber Terrorism: Concept, Characteristics, and Patterns*, Egyptian Center for Thought and Strategic Studies, 2019.

- Mahmoud Ahmed Ababneh and Mohammad Omar Al-Razaki, *Computer Crimes and Their International Dimensions*, Dar Al-Thaqafa, Amman, 2009.
- Medhat Ramadan, *Crimes Against Persons and the Internet*, Dar Al-Nahda Al-Arabia, 1st Edition, 2000.
- Muneer Mohamed Al-Jahini and Mamdouh Mohamed Al-Jahini, *Internet and Computer Crimes and Their Means of Combating*, Arab Thought Publishing, Alexandria, 1st Edition, 2004.

- Fahd Abdullah Al-Azmi, *Information Criminal Procedures*, New University Publishing, Egypt, 2016.
- Abdulrahman Abdulaziz Al-Shinaifi, *Information Warfare*, Ghareeb Office, Saudi Arabia, 1991.
- Zain Al-Abideen Awad Kazem Al-Kurdi, *Terrorism Crimes*, Al-Halabi Legal Publications, Beirut, 2018.
- Waleed Mohammed Orya, *Understanding Cyber Terrorism*, Naif Arab University for Security Sciences Publications, Riyadh, 2012.

Scientific Articles:

- Georges Lebki, *International Internet Treaties: Facts and Challenges*, Lebanese National Defense Magazine, Issue 83, 2013.
- Sheikha Hussein Al-Zahrani, *International Cooperation in Combating Cyber Attacks*, University of Sharjah Journal of Legal Sciences, Volume 17, Issue 01, 2019.
- Moza Al-Mazrouei, *Electronic Inventions : A Danger and How to Face It*, Afaq Al-Iqtisadiya Magazine, United Arab Emirates, Issue 09, 2012.

Scientific Conferences:

- Abdulrahman bin Abdullah Al-Sanad, *Means of Cyberterrorism and Its Rulings in Islam and Ways to Combat It*, Global Conference organized by Imam Muhammad bin Saud Islamic University, 2004.
- Mamdouh Abdulhamid Abdulmutallab, *Crimes of Using the Global Information Network (Internet Crimes) from a Security Perspective*, Research presented at the Law, Computer, and Internet Conference

organized by the Faculty of Sharia and Law in cooperation with the Emirates Center for Strategic Studies and Research and the Information Technology Center at the United Arab Emirates University, May 1-3, 2000.

– Abdulrahman bin Abdullah Al-Sanad, *Means of Cyberterrorism and Its Rulings in Islam and Ways to Combat It*, Global Conference on the Position of Islam, Imam Muhammad bin Saud Islamic University, 2004.

Websites:

-Ministry of Europe and Foreign Affairs website: Link.
https://www.diplomatie.gouv.fr/ar/politique-etrangere-de-la-france

-Computer Viruses . Wayland university On the following website
https://www.wbu.edu/wbu-online/current-students/computer-viruses.htm