LEGAL CONFRONTATION OF CYBER TERRORISM

DR. BENMOUSSA WARDA[1]

[1]Law and Real Estate Laboratory, Faculty of Law and Political Science, Blida 2 University – Lounici Ali (Algeria).

The E-mail Author: ward73.b@gmail.com

Received: 16/09/2024 **Published: 20/04/2025**

Abstract: *Cyber-crime has emerged due to the development in the use of modern technological means, as it is committed through cyberspace, affecting individuals and groups, as well as one country and may extend to several countries. States, as well as threatening to use violence against individuals and groups and sowing fear and terror among individuals, or working to encourage them to join terrorist organizations by spreading misguided ideas and spreading false rumors in order to recruit them to carry out terrorist operations.*

Keywords: *Cyber Terrorism; Information War; Hack; Network War.*

INTRODUCTION

New kinds of crimes have appeared, perpetrated by smart people different from regular criminals. Rapid technological media and communication tool development has caused these crimes, known as cybercrimes, to spread widely.

The misuse of technology causes issues and hazards such the exploitation of the internet by terrorist groups to further their objectives. Propaganda bearing ideological teachings, funding terrorist activities, training, planning, and executing operations, or using computer networks to launch attacks, instill fear and terror, or promote violence all help to bring this about.[1]

After the events of September 2011, terrorist activity moved from the battlefield to cyberspace, where computers and modern communication technologies now link terrorist networks and coordinate terrorist operations.[2] Consequently, terrorism has come in many shapes, using modern technology and communication tools to spread messages of hatred and violence, therefore circumventing all electronic barriers.[3]

Through this introduction, we address this topic by presenting the following issue:

What is cyberterrorism, and how can it be prevented and combated?

By examining materials addressing the subject, we use the analytical approach to address this question. The following two-part outline will guide our examination of the problem:

- Chapter One: The Concept of Cyberterrorism and Its Characteristics
- Chapter Two: Legal Mechanisms for Preventing and Combating Cyberterrorism

[1]- United Nations Office on Drugs and Crime, Vienna, in collaboration with the United Nations Task Force on the Implementation of Counter-Terrorism Measures, Use of the Internet for Terrorist Purposes, New York, 2013, p. 12.

[2]- Lalu Sofriadi bin Mujib, "New Media in Confronting the Challenges of Cyber Terrorism," Al-Zahra Journal, Faculty of Islamic and Arabic Studies, Jakarta, 17th year, 1st issue, 2020, p. 239.

[3]- Ayyashi Fatima, Boudaf Ali, "The Impact of Cyber Terrorism on Children and Methods of Prevention," Journal of Rights and Freedoms, vol. 9, no. 1, 2021, p. 129.

1. THE CONCEPT OF CYBERTERRORISM AND ITS CHARACTERISTICS

Though he didn't define it, Barry Collin first used the phrase "cyberterrorism" in 1986, claiming it was hard to come at a precise idea for this word.[4]

Thousands of emails from Mexicans in 1997 wiped off a website. Sending roughly 800 emails in 1998 wrecked Sri Lankan embassy websites. Protesters against the Kosovo War sent "email bombs" which struck NATO's computer systems in 1999. That same year, a criminal killed his rival by getting into his hospital file and changing his treatment recommendations. Cyberterrorism became widespread globally following 2011.[5]

We first cover the concept of cyberterrorism in this part; then we discuss the particularities of cyberterrorism.

1.1 The Concept of Cyberterrorism

Unique qualities that separate cybercrime from conventional crime define it since it uses computers and depends on the internet and other modern communication tools.[6] So, cyberterrorism is regarded as one of the types of this crime. Its goals are several and differ greatly, thus a single definition has not yet been created. We investigate the meaning of cyberterrorism in the first section in this regard; the second part is devoted to its goals.

1.1.1 Definition of Cyberterrorism

The diversity of its forms, the variation in its manifestations, and the differences in international viewpoints, shaped by different ideologies and beliefs,[7] have prevented the world community from arriving at a consistent definition of terrorism. One definition that includes the fundamental components of terrorism is as follows: "Aggression against someone's faith, life, mind, property, or honor that is done by people, organizations, or governments in violation of human rights is known as terrorism. It includes all forms of intimidation, harm, threats, and illegal killing as well as activities related to brigandage, highway robbery, and any act of violence or threat carried out in support of an individual or group criminal agenda. Its goal is to terrorize or instill fear in people by causing harm or putting their lives, freedom, or security in danger."[8]

The Algerian legislator defined the act of terrorism in Article 87 bis of the Penal Code: " Any activity that aims to protect territorial integrity, national unity, state security, and the stability and regular operation of institutions..." This article then lists the objectives of such actions, including (spreading fear, obstructing traffic, attacking national symbols, attacking means of transportation, harming the environment, hindering the work of public authorities, and others).[9]

There is no unified concept of cyber terrorism, as it is a relatively new concept.[10] As such, there are various definitions, one of which states that "Cyberterrorism is the term used to describe attacks on information systems motivated by political, ethnic, or religious reasons, or the use of digital technologies to threaten and oppress others."[11]

---

[4]- Ayyashi Fatima, Boudaf Ali, Op. cit., p. 134.

[5]- Hassan bin Ahmad Al-Shahri, "Cyber Terrorism: The War of Networks," International Arab Journal of Informatics, vol. 4, no. 8, January 2015, Saudi Arabia, p. 5.

[6]- Abdel-Sadek Cheikh, "Prevention of Cybercrimes under Law No. 09-04, which Includes Special Provisions for Preventing and Combating Crimes Related to Information and Communication Technologies," Ma'alim Journal of Legal and Political Studies, vol. 4, no. 1, 2020, pp. 189-204, p. 193.

[7]- Lalu Sofriadi bin Mujib, Op. cit., p. 244.

[8]- Saykh al-Islam Muhammad Tahir al-Qadri, Fatwa on Terrorism and the Ban on Suicide, Jakarta, 2014, p. 222, cited in Lalu Sofriadi bin Mujib, Op. cit., p. 246.

[9]- See Article 87 bis of the Penal Code, as amended by Law No. 14-01.

[10]- Ayyashi Fatima, Boudaf Ali, Op. cit., pp. 131-133.

[11]- Wikipedia, "Cyber Terrorism," The Free Encyclopedia.

The U.S. Department of State defined it as: "Politically motivated intentional acts of violence against civilians or non-combatants carried out by nationalist or extremist organizations in an effort to sway, terrify, and terrorize the populace."[12]

Professor Hassan bin Ahmed Al-Shahri described it as "An electronic variant of traditional physical terrorism that emerged within the fields of internet, telecommunications, and information technology. Terrorists have unlawfully attacked targets and infrastructure constructed for the benefit of humanity using this technology. Both military and civilian locations, transportation and air transportation systems, water and energy networks, computer networks, information systems, and other infrastructures are included in these objectives. These attacks, whether religious, political, social, or economic, are carried out to overthrow governments, spread fear and terror, and forward terrorist objectives."[13]

In Articles 87 bis 11/ last paragraph, and 87 bis 12 of the Penal Code, the Algerian legislator has dealt with cyber terrorism specifying the use of information and communication technologies to carry out a sequence of acts:

- Committing terrorist acts, planning or preparing them, participating in them, training to commit them, or receiving training in relation to them.

- Recruiting people for the benefit of a terrorist, association, organization, group, or entity whose goals or operations are subject to crimes classified as terrorist or destructive acts, or overseeing, assisting, or directly or indirectly promoting its ideas.

1.1.2 Objectives of Cyberterrorism

The internet is used by terrorist groups to promote and enable their illegal activities.[14] Cyberterrorism is a kind of terrorism[15] in which these crimes are carried out for political, economic, and social reasons to undermine and destroy the infrastructure of countries, therefore endangering their security and stability and generating fear and terror.[16] Apart from spreading fear and terror, executing their terrorist agendas, and spreading extremist ideas, the cyber space is a rich ground for members of terrorist organizations who interact with one another, destroy and hack websites. This is done to find people to join their groups. They also create new generations of viruses to perform cyberattacks on the internet and steal corporate secrets.[17]

These terrorist groups and organizations build websites to enable contact with their leaders, advance their ideas, look for funding sources for their activities, and spread techniques for creating explosives or any tools used in their terrorist operations.[18]

These groups use as many people and websites as they can to collect donations and money that support their criminal activities and initiatives, or to draw attention and sway public opinion. Cyberterrorism might seek to bomb important sites or penetrate the military systems of the state, or it could target notable people under death threat.[19]

[12]- Hassan bin Ahmad Al-Shahri, Op. cit., p. 3.
[13]- Ibid.
[14]- Fawziya Haj Sharif, Al-Saji Alam, "The Reality of Cyber Terrorism and Mechanisms for Combating It," The Academic Journal of Legal and Political Research, vol. 3, no. 1, Algeria, p. 159.
[15]- Diab Al-Badaina, "The Role of Security Agencies in Combating Information Terrorism," paper presented at the training seminar Combating Information Terrorist Crimes, Naif Arab University for Security Sciences, Quneitra, Morocco, 9-13 April 2006, p. 8.
[16]- Hassan bin Ahmad Al-Shahri, Op. cit., p. 21.
[17]- Emirates Center for Strategic Studies and Research, "The Growing Threat of Cyber Terrorism," Studies and Reports, 21 March 2004, p. 190.
[18]- Saleh bin Ali, Cybercrime: Its Risks and Penalties, Vision Realization Office and Communications and Information Technology Commission, Vision 2030, Saudi Arabia, p. 11.
[19]- Hassan bin Ahmad Al-Shahri, Op. cit., p. 15.

1.2 Characteristics of Cyberterrorism

From conventional to cyberterrorism, terrorism has evolved; the techniques of carrying out attacks have been honed at a lower cost and can be used anywhere and anytime. It aims at a great many people without physical mobility. The internet has thus enabled these groups to gather in various places to plan and agree on the activities they want to carry out.

Focusing on the tools employed in the first part, this section will cover the traits of cyberterrorism and handle this feature regarding the time and location of committing the crime in the second part.

1.2.1 In Terms of the Means Used

Often hiding behind aliases, cyberterrorists trade ideas and information via email. They build websites to promote their ideas. Moreover, they hack computers by using and implanting viruses. By means of these portals, they also provoke youth to challenge the government. Often, these actions include violence, the provocation of anarchy, and the disturbance of public order and information security.[20]

Terrorist groups take advantage of computer system specialists who send many messages to stop access to particular websites or conduct denial-of-service attacks, compromising other sites and stealing information kept inside them. Their activities can escalate to the distribution of viruses disrupting and stopping the internet and computer systems in many countries all around.[21]

By setting passwords or installing software, the offender intentionally blocks the inquiry from reaching digital evidence; he then leaves instructions to destroy files once unauthorized access occurs or uses particular encoding to block inspection. These policies make it more difficult for the investigator to obtain the necessary digital evidence to establish the involvement of the offender in the crime. Thus, it is crucial to create investigative tactics depending on specialists who can negotiate the intricate manipulation techniques employed in carrying out these offenses and that can handle computer technologies.[22]

Though crucial in this kind of crime, digital evidence is challenging to trust without following legal standards of proof. Moreover, these kinds of evidence can be complicated and call for help from a specialist knowledgeable about modern technologies connected to computers and the internet in this sector. The expert has to be qualified and should use court-approved techniques.[23]

1.2.2 Regarding the Time and Place of the Crime

Operating in a digital environment, cyber terrorism activities can happen anywhere—at home, in an office, or any other site. They include threats and social consequences. Though the losses are incalculable, the cost of these activities is low.[24]

Cyber terrorism creates questions of jurisdiction, especially when the offender is in one nation, in touch with a second criminal in another country, and the agreed-upon operation is conducted in a third country. This scenario causes a jurisdictional conflict and begs the issue of which court system qualified to decide such a crime.

This kind of crime uses communication tools and information networks to threaten and harm others, therefore depending on scientific and technological capacity. Whether inside a single country or across several countries, it can happen anywhere, making it simple to commit such crimes as there are no barriers or geographical limits.

Another feature of cyber terrorism is that it targets data and information, thus physical violence is absent. Rather, it consists of orders, numbers, and changing indicators that can be deleted. The offender or offenders

[20]- Fawziya Haj Sharif, Al-Saji Alam, Op. cit., p. 165.
[21]- Hassan bin Ahmad Al-Shahri, Op. cit., p. 13.
[22]- Saleh bin Ali bin Abdul Rahman Al-Rabiah, Op. cit., p. 10.
[23]- United Nations Office on Drugs and Crime, Op. cit., p. 108.
[24]- Diab Al-Badaina, Op. cit., p. 7.

could also be found in different and far locations, either inside the same nation or across many others, which would make identification very challenging.[25]

Identifying cyber terrorists' actual identities is challenging since they often change their aliases. They hack several sites without law enforcement being able to catch them or reveal their offenses. The absence of security systems tracking these internet intrusions accounts for this.

2. LEGAL MECHANISMS FOR PREVENTING AND COMBATING CYBERTERRORISM

Cyberterrorism is classified as a crime under the Penal Code punishable by imprisonment and a monetary fine. The punishment is a fine between 100,000 and 500,000 and temporary incarceration from five to ten years:

- Anyone who plans, prepares, participates in, trains to commit, or receives training in relation to terrorist acts using information and communication technologies, or who uses such technologies to carry out such acts.

- Anyone who manages its affairs, supports its activities, or promotes its ideas directly or indirectly using information and communication technologies to recruit people for the benefit of a terrorist, association, organization, group, or entity whose purpose or activities fall under crimes described as terrorist or destructive acts.

Based on the Penal Code and the Code of Criminal Procedure, the Algerian legislator has proposed integrated legal systems comprising prevention and combating strategies for cybercrime. This covers the publication of Law 09-04, which details particular clauses for the prevention and combating of crimes connected to information and communication technologies. Later, Presidential Decree 15-261 was published on the composition, organization, and procedures of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies. Presidential Decree 20-183 later cancelled this decree; Decree 21-439 was then issued to also cancel the latter.[26]

These companies destroy all physical evidence,[27] so erasing everything they publish and send via the internet, making it hard to get proof and show crimes committed in the virtual world. Their activities call for fast execution; they leave no physical trace to assist in locating them and bringing them to justice.[28] This calls for contemporary methods in investigation and inquiry.

This part will cover the procedural guidelines for prosecuting cyberterrorism; the second half will focus on ways to support judicial authorities.

2.1 Procedural Rules

Article 3 of Law 09-04, as mentioned before, by the Algerian legislator, described these guidelines considering the legal clauses guaranteeing the confidentiality of correspondence and communications. These rules are described in the Criminal Procedure Code and this law according to the criteria for safeguarding public order or the needs of continuous investigations or judicial inquiries. It also provides technical methods for monitoring electronic communications and collecting and recording their contents in real-time, as well as conducting searches and seizures inside information systems. This section will set aside a portion for each of the processes described in this paper.

---

[25]- Saleh bin Ali bin Abdul Rahman Al-Rabiah, Op. cit., p. 9.

[26]- Abdel-Sadek Cheikh, Op. cit., p. 191.

Law No. 09-04 dated 5 August 2009, which includes the special provisions for the prevention and combating of crimes related to information and communication technologies, Official Gazette No. 47/2009.

Presidential Decree No. 15-261, dated 24 Dhu al-Hijjah 1436 (8 October 2015), which specifies the formation and organization of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, Official Gazette No. 86/2021, later repealed by Presidential Decree No. 20-183, which was subsequently repealed by Presidential Decree No. 21-493, Official Gazette No. 86/2021.

[27]- Ayyashi Fatima, Boudaf Ali, Op. cit., p. 131.

[28]- Hassan bin Ahmad Al-Shahri, Op. cit., p. 1.

2.1.1 Monitoring Electronic Communications

Electronic surveillance operations may be carried out in the following cases[29]:

- To stop actions called terrorism, sabotage, or crimes endangering state security.
- When information suggests a possible attack on an information system in a manner that endangers public order, national defense, state institutions, or the national economy.
- Judicial inquiries may be affected by electronic surveillance if it is impossible to meet the goals of continuous research without it.
- Executing requests for international judicial assistance.

Such surveillance operations may only be conducted with written authorization from the competent judicial authority.

The Public Prosecutor at the Court of Algeria is responsible for granting judicial police officers, as described in Article 13 of this law,[30] permission for a period of six months, which is renewable, when it relates to the first case mentioned above (related to terrorist and sabotage crimes and those affecting state security). This is founded on a study describing the kind of technical arrangements employed and their intended uses. Under the penalties specified in the Penal Code regarding privacy violations, these technical arrangements are solely meant to gather and record data about preventing terrorist activities, attacks on state security, and combating these threats.

While adding techniques meant to find the offenders so they can be caught and pursued, the inquiry has to depend on conventional investigative techniques. Using digital evidence calls for particular knowledge in criminal investigations; professionals can then use this knowledge in the virtual system to help.[31]

2.1.2 Search and Seizure

Given the electronic devices and papers involved in perpetrating the crime, search is among the most important processes in cybercrime. Legally authorized officials may access data processing systems to search them and seize information that will help reveal the truth.

A. Search

Judicial police officers and the appropriate court authorities may, under the Criminal Procedure Law and in the situations listed in Article 4 of Law 09-04, access systems for the purpose of searching, including remotely:

- Access an information system or any part of it, as well as the information data stored within it.
- Access an information storage system.

The search may be extended quickly to this other system or part of it, after prior notification to the competent judicial authority, if there are reasons to believe that the sought-after data is stored in another information system and that this data can be accessed from the first system.

It has been earlier shown that the information system outside the national territory holds the data being sought, which can be accessed from the first system. Thus, under the applicable international agreements and the principle of reciprocity, acquiring this data would need the help of the relevant foreign authorities.

[29]- See Article 4 of Law No. 09-04, Op. cit.

[30]- This pertains to the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies (see Article 13 of Law No. 09-04).

[31]- United Nations Office on Drugs and Crime, Op. cit., p. 54, and Article 9 of Law No. 09-04 states: "Under the penalties provided for in the applicable legislation, the use of information obtained through surveillance operations, as outlined in this law, is prohibited except to the extent necessary for investigations or judicial inquiries."

The authorities conducting the search may call on any person familiar with the operation of the information system under investigation or the steps taken to safeguard the data it holds in order to help them and offer all the required information to finish their work.[32]

B. Seizure

The whole system does not have to be seized if the authority running the search inside an information system finds stored data that could help reveal crimes or identify their perpetrators. Data pertinent to the inquiry should be copied instead, together with the required information to grasp it, onto an electronic storage device that can be seized and protected per the terms specified in the Criminal Procedure Code.

The authority carrying out the search and seizure has to guarantee the safety of the data inside the information system under examination in all situations.

Provided this does not compromise the data's content, it may, using the required technical tools, reconstruct or reformat this information to make it usable for investigative purposes.

The authority carrying out the search has to employ suitable methods to stop access to the data in the information system or to the copies made accessible to people authorized to use this system if the seizure process is technically impossible.[33]

2.2 Methods for Assisting Judicial Authorities

Cybercrimes in general and cyberterrorism in particular are committed in the virtual world, which allows people to remain in continuous communication and act quickly, so complicating their detection and proof. Virtual movement between different groups is made possible in this virtual environment by means of communication services combining voice, image, and text.[34]

Service providers[35] are obligated to help the authorities in charge of judicial inquiries by collecting and recording data about the substance of communications in real-time and guaranteeing this data is kept for the pertinent authorities. Under penalty of sanctions for revealing investigation and inquiry secrets, they must keep the confidentiality of the operations they conduct at the request of investigators as well as the information connected to them.[36]

This section will cover the National Authority for the Prevention and Combat of Crimes Related to Information and Communication Technologies in the first part; the second part will be devoted to mutual international judicial assistance.

2.2.1 The National Authority for the Prevention and Combat of Crimes Related to Information and Communication Technologies

The National Authority for the Prevention and Combat of Crimes Related to Information and Communication Technologies was established as an independent administrative body with legal personality and financial autonomy. It is placed under the authority of the President of the Republic, with its headquarters in Algiers, although it can be relocated by presidential decree. The authority operates under the oversight of the judiciary.[37]

[32]- See Article 5 of Law No. 09-04, Op. cit.

[33]- See Article 6 of Law No. 09-04, Ibid.

[34]- Kawthar Mazouni, The Digital Network and Its Relationship with Intellectual Property, Dar Houma, Algeria, 2008, pp. 13-56 (cited in Jamil Khafif, Cybercrimes Related to Financial Assets, PhD Thesis in Law, Faculty of Law, University of Algiers 1, 2016-2017), p. 195.

[35]- Article 02/D defines service providers as: "Any public or private entity that provides its users with the ability to connect via an information system and/or a communication network, or any other entity that processes or stores data for the benefit of the mentioned communication service or its users."

[36]- See Article 10 of Law No. 09-04, Op. cit.

[37]- See Article 13 of Law No. 09-04, Ibid. and Articles 2, 3, and 4 of Presidential Decree No. 21-439, Op. cit.

A. Composition of the Authority[38]

The President of the Republic exercises authority over both the General Directorate and the Steering Council, which together form the authority. Chaired by the Secretary General of the Presidency of the Republic, the Steering Council comprises the following members: the Secretaries General of the Ministry of Foreign Affairs and the National Community Abroad, the Ministry of Interior, Local Authorities, and Urban Planning, the Ministry of Justice, the Ministry of Post and Telecommunications, the National Gendarmerie Commander, the Director General of Internal Security, the Central Director of Army Security for the People's National Army, the Director General of National Security, the Head of Cyber Defense and System Security Monitoring for the People's National Army, and a representative appointed by the President of the Republic. The Authority's Director General is the Steering Council's Secretary.

Presidential decree appoints the Director General, who runs the General Directorate; his responsibilities end in the same way. The General Directorate comprises the following divisions: the Directorate of Preventive Monitoring and Electronic Vigilance, the Directorate of Administration and Resources, the Studies and Summary Division, the Cooperation and Electronic Vigilance Division, and Regional Attachments.[39]

Judges, officers, judicial police agents qualified by military security services, the National Gendarmerie, the National Security, technical and administrative support staff from the pertinent military security services, the Gendarmerie, and the National Security are all connected to the authority thus guaranteeing its operation.[40]

B. The Role of the Authority

The agency is in charge of encouraging and coordinating initiatives to combat crimes connected to information and communication technologies as well as those linked to them. It helps judicial police services and court authorities investigate information and communication technology-related crimes by means of information gathering, forensic expertise, and international information sharing to gather all pertinent data to locate the offenders of such crimes.

Article 4 of the decree assigns the authority a number of duties including several Steering Council and General Directorate activities focused on identifying and fighting crimes connected to information and communication technologies.

2.2.2 Mutual International Judicial Assistance

Some situations might call for cross-border inquiries; thus, nations have to concur on the same techniques to get the proof utilized in the inquiry. Judicial prosecution calls for specialized tactics that guarantee the evidence is accepted while honoring all rights set for the accused.[41]

Within the framework of ongoing investigations or inquiries to examine these crimes and identify the perpetrators, the competent authorities may exchange international judicial assistance to gather evidence in electronic form. Requests for judicial assistance may be accepted in urgent situations and in line with international agreements and the principle of reciprocity if they are made via rapid communication channels, including fax machines or email, provided that these means satisfy adequate security criteria to confirm their authenticity.[42]

Requests for help concerning the exchange of information or the implementation of any precautionary measures are handled in line with applicable international agreements, bilateral international treaties, and the principle of reciprocity. Requests for help could be denied if their fulfillment would compromise public

[38]- See Article 5 and subsequent articles of Presidential Decree No. 21-439, Op. cit.
[39]- See Article 14 of Law No. 09-04, Op. cit.
[40]- See Article 4 and subsequent articles of Presidential Decree No. 21-439, Op. cit.
[41]- United Nations Office on Drugs and Crime, Op. cit., pp. 101-102.
[42]- See Article 16 of Law No. 09-04, Op. cit.

order or national sovereignty. Moreover, answering requests for help could be conditional on things like keeping the transmitted data private or making sure it is not used for reasons other than those stated in the request.[43]

When the offender is a foreign national, Algerian criminal courts' jurisdiction goes beyond the national territory to include consideration of crimes connected to information and communication technologies in addition to the jurisdictional rules described in the Criminal Procedure Code. These offenses have to be aimed at strategic interests connected to the national economy, national defense, or Algerian state institutions.[44]

CONCLUSION

Regarded as one of the most lethal kinds of cybercrime, cyberterrorism has been growing with the growing use of information technology. Cyberterrorism knows no borders; its threats affect people, organizations, and whole countries. While encouraging member recruitment into terrorist groups by disseminating extremist ideas, terrorist groups use threats, intimidation, and fear to provoke the application of force and violence.

There is no worldwide convention particularly on cyberterrorism, nor is there a consistent definition for it. Though, nations believe it has certain qualities that set it apart from other offenses, which has required the creation of particular systems and processes for judicial follow-up. The Criminal Procedure Code and Law 09-04 describe these techniques, the latter of which contains particular guidelines for the prevention and fight of crimes connected to information and communication technologies. But, measures have to be taken to guarantee that these techniques complement the values of a fair trial.

Though the legislator works hard and laws are set up to stop and fight this kind of crime, cyberterrorism cannot be eradicated since computer systems are always open to hacking and cyberattacks. Protecting computers, vital websites, and sensitive data calls for the creation of specialized methods and the participation of professionals in this field. Moreover, the legislator has to draft particular laws covering both material and procedural guidelines as well as state-to-state cyberterrorism international cooperation.

REFERENCES LIST

A – Books

[1] *Saykh al-Islam Muhammad Tahir al-Qadri, Fatwa on Terrorism and the Ban on Suicide, Jakarta; 2014.*

[2] *Saleh bin Ali, Cybercrime: Its Risks and Penalties, Vision Realization Office and Communications and Information Technology Commission, Vision 2030, Saudi Arabia; n.d.*

[3] *Kawthar Mazouni, The Digital Network and Its Relationship with Intellectual Property, Dar Houma, Algeria; 2008.*

B – Theses

[1] *Jamil Khafif, Cybercrimes Related to Financial Assets, PhD Thesis in Law, Faculty of Law, University of Algiers 1; 2017.*

C – Newspaper Articles (Journals)

[1] *Hassan bin Ahmad Al-Shahri, "Cyber Terrorism: The War of Networks," International Arab Journal of Informatics, vol. 4, no. 8, Saudi Arabia; January 2015.*

[2] *Abdel-Sadek Cheikh, "Prevention of Cybercrimes under Law No. 09-04, which Includes Special Provisions for Preventing and Combating Crimes Related to Information and Communication Technologies," Ma'alim Journal of Legal and Political Studies, vol. 4, no. 1; 2020.*

[3] *Ayyashi Fatima, Boudaf Ali, "The Impact of Cyber Terrorism on Children and Methods of Prevention," Journal of Rights and Freedoms, vol. 9, no. 1; 2021.*

[43]- See Articles 17 and 18 of Law No. 09-04, Ibid.
[44]- See Article 15 of Law No. 09-04, Ibid. and Articles 582 to 589 of the Penal Procedure Code, Op. cit.

[4] *Fawziya Haj Sharif, Al-Saji Alam, "The Reality of Cyber Terrorism and Mechanisms for Combating It," The Academic Journal of Legal and Political Research, vol. 3, no. 1, Algeria; 2019.*

[5] *Lalu Sofriadi bin Mujib, "New Media in Confronting the Challenges of Cyber Terrorism," Al-Zahra Journal, Faculty of Islamic and Arabic Studies, Jakarta, 17th year, 1st issue; 2020.*

D – Seminar Papers

[1] *Diab Al-Badaina, "The Role of Security Agencies in Combating Information Terrorism," paper presented at the seminar Combating Information Terrorist Crimes, Naif Arab University for Security Sciences, Quneitra, Morocco, 9-13 April; 2006.*

E – Legal Texts

[1] *United Nations Office on Drugs and Crime, Use of the Internet for Terrorist Purposes, United Nations Task Force on the Implementation of Counter-Terrorism Measures, Vienna and New York; 2013.*

[2] *Law No. 09-04 dated 5 August 2009, including special provisions for the prevention and combating of crimes related to information and communication technologies, Official Gazette No. 47/2009.*

[3] *Presidential Decree No. 21-439 dated 7 November 2021, reorganizing the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, Official Gazette No. 86/2021. Repeals Presidential Decree No. 20-183.*

[4] *Wikipedia, "Cyber Terrorism," The Free Encyclopedia: https://en.wikipedia.org/wiki/Cyber_terrorism (consulted on 21/04/2024).*