The Mechanisms Encountering Cyber Terrorism in the Algerian Legislation

آليات مواجهة الإرهاب السيبراني في التشريع الجزائري

DR. SAYEH BOUSSAHIA (*)
Larbi Tebessi University, Tebessa
sayeh.boussahia@univ-tebessa.dz

DR. DOUNIAZED THABET
Larbi Tebessi University, Tebessa
douniazedtabet@univ-tebessa.dz

The date of Submission: September 5 , 2019 | The date of revision: December 9th, 2019 | The date of acceptance: December 17th, 2019

Abstract:

The e- terrorism crime is one of the most important features in the modern scientific development in the means of communication and information technology, where terrorist groups and organizations found their way in these modern means used to facilitate communication between terrorist groups and coordinate their operations and preparation and even their implementation.

This study seeks to try to demystify this new criminal phenomenon, define its concept, explain its characteristics, and identify its causes and ways of committing. It also aims at exposing the Algerian legislator's policy in combating this crime in the light of the existing legal texts and in light of the legislator's enactment after the amendment of the Penal Code under Law 16-02 of 19 June 2016 by adding articles 87 bis 11 and 87 bis 12 and thus access to the forms of protection which Legislator guaranteed against this new type of criminality.

Keywords: e-terrorism, development, terrorists, Algerian legislation, mechanisms, combat.

ملخص:

تعد جريمة الإرهاب الالكتروني من بين أهم ما أفرزه التطور العلمي الحديث في وسائل الاتصال وتقنية المعلومات، حيث وجدت الجماعات والتنظيمات الإرهابية ضالتها في هذه الوسائل الحديثة والتي باتت تستخدمها في تسهيل الاتصال بين الجماعات الإرهابية وتنسيق عملياتها و الإعداد لها وحتى تنفيذها.

تسعى هذه الدراسة إلى محاولة إزالة الغموض حول هذه الظاهرة الجرمية المستحدثة وتحديد مفهومها، بيان خصائصها والوقوف على أسبابها وأساليب ارتكابها. كما تهدف أيضا إلى التعرض إلى سياسة المشرع الجزائري في مكافحة هذه الجريمة على ضوء النصوص القانونية الموجودة وعلى ضوء ما استحدثه المشرع بعد تعديل قانون العقوبات بموجب القانون 16-02 المؤرخ في 19 جوان 2016 وذلك بإضافة المادتين 87مكرر11 و87مكرر12 ومن ثم الوصول إلى صور الحماية التي كفلها المشرع ضد هذا النوع المستحدث من الإجرام.

الكلمات المفتاحية: الإرهاب الالكتروني، التطور التكنولوجي، المنظمات الإرهابية، التشريع الجزائري، الآليات، المكافحة.

(*) **Corresponding Author.**

Introduction:

Modern technological revolution, the scientific development in the field of information technology and the advent of computers mechanism brought a significant change in the form of life in the world, so that relying on these means is increasing day after day in various fields.

Electronic means as provided by facilities and thanks to that seen in the continuous evolution of one the most important elements of public or private institutions, whether educational institutions, financial, security, health and even public facilities such as courts, tribunals. In addition to what was said the means of modern technology are witnessing prevalent and widespread social level where members of communities depend on these technologies in various areas of their daily lives through a range of applications offered by information technology direct such as online networking and the exchange of information and contracting at distance via the Internet.

Despite the great and multiple benefits for the use of modern electronic means , they are blamed for their misuse use, badness and harmfulness, which affected the security of individuals and nations negatively, through the emergence of the illegal use of technical information, this kind of modern crime, which has become a grave danger to the multiplicity of descriptions of criminal offenses steal stored information, illegal transfer of funds, sexual exploitation of children... etc.

The matter did not stop there but went to the development of some of the traditional crimes where the modern technology and the Internet have being used in terrorist attacks and sabotage [(1)], which are exacerbated by the day and threatening the entire world as a result of the serious damage caused to individuals, communities and countries, this calls for the need to confront this induced type of terrorism and named «CYBER TERRORISM » by taking appropriate measures and actions, at the international or national level, the same matter sought by The Algerian legislature by amending the penal code under law no.16-02 dated 19 June 2016 with the addition of articles 87 bis 11 and 87 bis 12.

The problematic in this regard will be **the nature of the actions taken by the Algerian legislature to confront the dangers of cyber terrorism?**

To answer this problematic, we should determine at the beginning the legal essence of cyber terrorism and then stand on the anti-legal mechanisms induced this type of crime in the Algerian legislation, through exposure to the following sections:

- First chapter: the notion of cyber terrorism,
- Second chapter: the legal mechanisms to fight the crime in the Algerian legislation.

Chapter One: The notion of cyber terrorism

Through this chapter, we'll expose the concept of cyber terrorism, and identify its means and forms as follows:

Section One: The concept of cyber terrorism

Section Two: Cyber terrorism forms and means

Section One: The concept of cyber terrorism

A- Definition of cyber terrorism:

(1)- United Nations Office ON Drugs And Crime, the use of internet for terrorist purposes, United nations, new York, 2012, pp.02 and beyond.

The definition of electronic terrorism requires the need to define, firstly, the traditional terrorism and then stand on the distinctions between them through the following:

1- Definition of traditional terrorism:

Till now, Scholars didn't agree about a specific definition to terror crime, and points of views still differ in dealing with the phenomenon of terrorism, thus the failure to agree on a inclusive definition of the concept of terrorism is due to the problems related to the development of the phenomenon of terrorism itself, to the complexity of its forms, to the multiplicity of its commission and its overlap with other phenomena and crimes. We will try to exposure of attempts to put a specific definition of the crime of terrorism, both at the linguistic, jurisprudential or legal level, as following:

- Linguistic definition to the crime of terrorism:

In describing the ambit of the concept, it is unavoidable to touch upon and trespass the obstacles at stake in rigorously defining a crime of terrorism and deliberating on the precise linguistic meaning of the words used in the disputed definition itself becomes almost inevitable.**(1)**

"Terrorism" comes from the French word terrorisme, and originally referred specifically to state terrorism as practiced by the French government during the 1793–1794 Reign of Terror. The French word terrorisme in turn derives from the Latin verb terrere (e, terreo) meaning "to frighten".The Jacobins, coming to power in France in 1792, are said to have initiated the Reign of Terror (French: La Terreur). After the Jacobins lost power, the word "terrorist" became a term of abuse**(2)**, so accordingly, the Arab lexicon mediator dictionary defined terrorism as "the terrorist is the description given to those taking the path of violence to achieve political goals"**(3)**.

- Jurisprudential definition to the crime of terrorism:

Despite the great difficulties encountered the jurisprudence to put a specific definition of terrorism, as already mentioned, scholars have made great efforts to come up with an agreed definition of terrorism according to their different views.

Terrorism is defined as: "that criminal act, coupled with horror or violence in order to achieve a specific goal," and in the same direction was defined as "criminal acts with the primary aim to spread fear and terror as a Mens rea using means that will create a state of public danger as Actus reus".

It's also known as the "illegal use of force or violence or threat of violence in order to achieve political objectives," In this regard, a part of jurisprudence went to say that creating a state of terror and fear in order to achieve the goal, whatever political, religious, ideological or racist**(4)**.

---

(1)- I.L. Braber, Defining the crime of terrorism in international law – a legal minefield, University of Amsterdam, Graduate School of Law, July 2013, p.10.

(2)- See https://en.wikipedia.org/wiki/Terrorism, last entry 13 March 2017, at 12:54.

(3)- This definition was stated in: Faleh Haitham Shehab, the crime of terrorism and ways to combat it in the comparative criminal legislation, Culture House for Publishing and Distribution, Amman, Jordan, first edition 2010, p.28.

(4)- Terrorism is, in its broadest sense, the use of intentionally indiscriminate violence as a means to create terror or fear, in order to achieve a political, religious, or ideological aim., see Fortna, Virginia Page (20 May 2015). "Do Terrorists Win? Rebels' Use of Terrorism and Civil War Outcomes". International Organization. 69 (3): 519–556.See also Abbas Chafaa, terrorist phenomenon between international law and religious perspective, Ph.D. thesis, University of Batna, 2011, p.28.

Among legal definitions of terrorism that resonated with jurisprudence, the definition of Pr.M.Cherif Bassiouni who identified terrorism as "a violent strategy criminalized internationally[1], stimulated by doctrinal concerns (ideological), envisages creating terrifying violence inside a special part of a particular society to gain access to authority or to do heretical to the demand or dark regardless of whether the perpetrators of violence are working for themselves and on behalf of them or on behalf of the State"[2].

- The international definition to the crime of terrorism:

Definition of terrorism and identifying terrorist acts in accordance with the provisions of the international and regional conventions and treaties are of paramount importance because they reflect a unified world view toward the phenomenon which has become a threat to the entire international system, not to a particular state; this requires agreements on international combat ways; thus among the international conventions that defined terrorism is Geneva Convention which was held in November 16, 1937, this convention was devoted to define and to identify terrorism manifestations of physical acts; the second paragraph of its first article stipulates the definition of terrorism as "representing criminal offenses against the state, which whose object or nature is spreading panic or fear in the hearts of all people"[3].

Among the regional conventions that defined the crime of terrorism «Arab Convention on the Suppression of Terrorism» issued by the Council of Arab Ministers of Interior and Justice, in Cairo in April 1998, wherein terrorist crime was known in its first article as: «Any act or threat of violence, whatever its motives or purposes, that occurs for the advancement of an individual or collective criminal agenda, causing terror among people, causing fear by harming them, or placing their lives, liberty or security in danger, or aiming to cause damage to the environment or to public or private installations or property or to occupy or to seize them, or aiming to jeopardize a national resource».

- The Algerian legislature's position to the definition of the crime of terrorism:

The Algerian legislature firstly included the criminalization of terrorism within the provisions of the legislative decree no.92-03 dated September 30, 1992 on combating sabotage and terrorism, this decree, which was abolished under order no.95-11 of 25 February 1995 amending the Penal Code, containing articles from 87bis to the text of article 87 bis 9 under the title (the offenses described as terrorist or subversive acts), where Article 87bis of the Penal Code states: "considers a terrorist or sabotage in the concept of this order, any act targeting the state security, territorial unity, safety and territorial integrity, stability of the institutions and their normal functioning through any act whose purpose as follows: ... . "[4]. It is noticeable that this definition of terrorism knew no precise definition, but only census terrorist acts criminalized as referred to by the legal text.

---

(1)- United Nations of the Next Decade, Implementation of the UN Global Counterterrorism Strategy, 42nd Conference on the United Nations of the Next Decade, June 8-13, 2007.

(2)- This definition is stated in, Faleh Haitham Shehab op.Cit., p.36.

(3)- The Sixth Conference in Copenhagen in 1935 adopted a text that defined terrorism in Article 1 as: International acts directed against the life, physical integrity, health or freedom of a head of state or his spouse, or any person holding the prerogatives of a head of state, as well as crown princes, members of governments, people enjoying diplomatic immunity, and members of the constitutional, legislative or judicial bodies [if the perpetrator creates] a common danger, or a state of terror that might incite a change or raise an obstacle to the functioning of public bodies or a disturbance to international relations.

(4)- See Article 87 bis of the Algerian Penal Code.

2- Definition of cyber terrorism:

The term cyber terrorism of two terms: «Cyber » which is the cyberspace and « Terrorism », so accordingly Cyber Terrorism is a use of modern technology and exploits it in the completion of criminal terrorist acts and to achieve the purposes of illegal terrorist groups.

And accordingly to that, jurisprudence defines cyber terrorism as "a situation where in the terrorist groups used modern communication technologies, including the Internet, to buy weapons or to make connections or relationships with third parties in order to plan future terrorist operations"**(1)**, it is also known as "aggression, intimidation or physical or mental threat using electronic means issued by states, groups or individuals on a human himself, on his religion, kind or his mind or his money unlawfully by various forms and types"**(2)**.

Terrorism is also known as: "Horror by any State, group or personnel spread covert or overt through electronic means by sabotage or murder or corruption at any of its forms or the threat of any of these against the legitimate authority"**(3)**.

Some jurisprudence goes on to say that cyber terrorism is no different in its definition of normal terrorism, but in the quality of the tool used to achieve terrorist purpose, for that it's accordingly known as: "The use of digital technologies and attacking information systems to intimidate and subdue others for political, racial or religious motives**(4)**. In this connection, it's also known as "that kind of modern terrorism, which depends entirely on the use of all scientific and technical means of potential of Internet networks and networks of thematic for the sake of intimidation, horror and damage to individuals, civil groups or governmental institutions"**(5)**. Terrorism was also known as: "The use of information resources of media computer and the Internet and satellite channels and devices for intimidation or coercion for political purposes or for intellectual persuasion, for passive and aggressive education", and so this kind of terrorism became linked to a large extent to the advanced level, which the IT and the media provide in all areas of life.

The United Nations, in October 2012, defined cyber terrorism as "the use of the Internet to spread terrorist acts"**(6)**.

---

(1)- Dardour Nassim, computer crime in the light of the Algerian and Comparative Law, Master Thesis, University of Constantine, 2013, p.155.

(2)- Aycer Mohammed Attia, the role of modern mechanisms in curbing novel Electronic crime: terrorism and ways to confront it, working paper submitted to the scientific forum on novel crime under the light of the current regional and international transformations, held at the Faculty of Strategic Sciences from 2 to September 4, 2014, Amman, p.8, available on the website:
http//:www.assakina.com/wp-content/uploads/2015/6/28,the date of entry February 2017.

(3)- Mohammed bin Abdul Aziz bin Mohammed Al-Aqeel, Electronic incitement to terrorism: idiosyncratic adaptation and judgment - Twitter model -a working paper submitted to the International Conference: The Arab media's role in dealing with the phenomenon of terrorism, Naif Arab University for Security Sciences, p.14, available on the website :
http://repository.nauss.edu.sa/handle/123456789/60016, date of entry: 28 February 2017.

(4)- Abdul Aziz Bin Humaidan Thumali, the impact of cyber terrorism and ways to combat it, research presented to the World Islamic Conference on combating terrorism, organized by the Muslim World League, Makkah, held on 22 to 25 February 2015, p.5, available on the website: Research-Conference www.themwl.org/peace/. Date of entry: March 1, 2017.

(5)- This definition is stated in, Amir Hassan Turki, Salam Jassim Abdullah, cyber terrorism and risks in the current era, Journal of Legal and Political Sciences, special issue, Faculty of Law and Political Science, University of Diyala, Iraq, p.327.

(6)- Abdulaziz Bin Humaidan Thumali, op.cit., p.06.

This trend was followed by the Algerian legislator through the text of article 87 bis 11 which was added to the provisions of the Penal Code under Law No. 16-02 of 19 June 2016[(1)], wherein he criminalized the offense of use of information and communication technologies in the enumerated acts of terrorism in the said article as following:

- Locomotion of an Algerian or a foreign resident in Algeria or attempt to travel to another state for the purpose of committing terrorist acts, planning, preparation or participating in training or to commit or to receive training on them.
- Providing or intentionally collecting by any means, directly or indirectly, or the intent to use them with knowledge to be used to finance the travel of people to another state for the purpose of committing acts mentioned in the paragraph above.
- Funding intentionally or regulating the travel of people to another state for the purpose of committing terrorist acts, planning, preparation or participating in training or to commit or to receive training on them or facilitate this travel.
- Recruit people for the benefit of a terrorist association or organization, group or organization whose purpose or activities fall under the sanctions on the crime of terrorism, or organize their affairs or supports acts or activities or publish her thoughts directly or indirectly.

Thus then we are in front of cyber terrorism crime, according to the view of the Algerian legislature when using information and communication technologies to commit one of the above-mentioned acts, also it's meant by technologies, information and communication the commission of the crime through the IT system[(2)], or a system of electronic communication[(3)].

It's evident from the above definitions of cyber terrorism that:

- The cyber terrorism essentially depends on the use of information technology and the exploitation of modern means of communication and information networks in order to achieve the planned objectives by terrorist groups.
- The cyber terrorism aims to achieve particular goals namely spreading fear and terror among people and destabilizing peace of mind and endangering their safety and security at risk, and also aims to harm the means of communication and information technology, funds and public or private facilities, departments and public utilities etc ...[(4)], the traditional terrorism seek to achieve most of these goals.

B- Cyber terrorism characteristics:

Cyber terrorism is characterized by a set of features is characterized different from the normal terrorism and from other crimes, but common in many of them with cyber crime, and are, in particular, as follows[(5)]:

---

(1)- Official Gazette number 37, dated 22 June 2016.

(2)- The system is intended informatics any separate system or group of systems connected to each other, or associated with, the one or more of them to address the mechanism for implementation of data for a particular program.

(3)- As electronic communications meant any messaging or sending or receiving signs, signals, writing, images, sounds, or different information by any means an electronic system.

(4)- For more detail on the objectives of cyber terrorism, see Abdullah bin Abdul Aziz bin Fahd Al-Ajlan, cyber cyber terrorism in the information age, working paper submitted to the International Conference on protection of information security and privacy in Internet Law, held in Cairo from 2 to 4 June 2008, p.2, available on the website:
http://www.shaimaaatalla.com/vb/showthread.php?t=3937, Date of entry March 2, 2017, at 11 and 16.

(5)- Aycer Mohammed Attia, op.cit., p.12-13, Abdullah bin Abdul Aziz bin Fahd Al-Ajlan, op.cit., p.09.

1- Cyber terrorism offense is transnational:

Information society does not recognize geographical borders, it is an open society through networks penetrating time and space, and by the emergence of information networks, there were no longer visible or tangible boundaries standing in front of the transfer of information across countries, this modern technology shortened distances, so that this property was reflected on the nature of the criminal acts committed by these techniques and for that crime became accordingly transnational. This property has created many problems such as the determining of jurisdiction, the applicable law, in addition to the problems associated with prosecution and other problems posed by crimes that cross national borders in general[(1)].

2- Easiness of commission of cyber terrorism:

The commission of this crime does not require violence or force as is the case for the crime of traditional terrorism, but requires only a computer connected to the network information provider and a special program so that the work of terrorist offender is located in his home or his office using modern technology.

3- Hallmark of the offender:

The perpetrator of this type of crime is often someone who is specialized in the field of information technology, or at least familiar to dealing with Computer and network information.

4- Speediness evidence erase and proving difficulty:

The crime is also characterized by difficult in proving because of the quick lack of digital evidence of and facility in being destroyed, so cyber terrorism often does not leave any physical evidence after committing the crime, which makes it difficult to be tracked for the sake of discovery of the crime. The difficulty of discovering these crimes is also attributed to lack of experience of security and judicial organs to handle with.

C- Reasons for the spread of cyber terrorism:

Reasons of public cyber terrorism interfere with the traditional reasons for terrorism[(2)], so that cyber terrorism is an updated image of the normal forms of terrorism, however, cyber terrorism is linked to a private reasons can be summarized as follows[(3)]:

1- Reasons related to informatics networks:

The reasons relating to the information network of the main reasons that led to the growing phenomenon of cyber terrorism, and linked these reasons, in particular, as follows:

- Ease of use of information networks:

---

(1)- John Rollins, Liana Sun Wyler, Terrorism and Transnational Crime: Foreign Policy Issues for Congress, Congressional Research Service, June 11, 2013.

(2)- There are many reasons leading to the spread of the phenomenon of terrorism, whether for personal reasons, ideological, economic, political, social, cultural. For more detail on these reasons, especially those related to the causes of its spread in Algeria, see Dich Musa, the legal system to compensate victims of terrorist crimes - a comparative study -, PhD thesis, University of Tlemcen 2016, pp.60-67.

(3)- For more detail on this see the reasons, Abdul-Qader al-Sheikhli, the nature of the cyber terrorism, a paper submitted to the global Islamic Conference on the fight against terrorism, organized by the Muslim World League, Makkah, held on 22 to 25 February 2015, S14-15, available on the website: Research-Conference www.themwl.org/peace/, the date of entry: March 1 2017, see also Abdullah bin Abdul Aziz bin Fahd Al-Ajlan, op.cit., pp.08-09.

Information networks are characterized by easy to use so that they do not take much effort or time or huge sources of funding, and accordingly, the cyber terrorist attack does not require more than the presence of any computer connected to the information network. This simple technique allows terrorist organizations to the implementation of strong, accurate and effective operations, increasing the area of terrorism and cause an increase in strength and dominance.

- Weakness of infrastructure relating to informatics networks and the easiness to penetration:

Information networks are designed openly without restrictions or by security barriers and so the structure to facilitate access without restrictions or barriers, and as a result, the electronic systems and information networks include informational gaps what was exploited by terrorist organizations by sneaking into the structures of informatics infrastructure, and the practice of sabotage and terrorist operations .

- Informatics networks are not subject to specific geographic boundaries:

As already mentioned that cyber terrorism is transnational as a result of the undergoing of information networks to certain geographical limits, the matter that led to the expansion of crime and the lack of effect in a specified range and even to the extent of the Universality of the crime.

- Absence of control over information networks:

The lack of a unified central point of control over what is displayed on the information network to be controlled is a significant cause in the spread of the phenomenon of cyber terrorism, where anyone can access and put what they want on the network and then log out without the slightest oversight. All what is owned by those who try to impose censorship is the denial of access to some sites after being blocked or closed or destroyed after the commission of the offender of what he wants.

2- Reasons related to the crime and offender:

- Difficulty in detecting and proving the offense of cyber terrorism:

Already said that cyber terrorism is characterized by difficulty to prove to the speed of the destruction of physical evidence of the crime, and therefore this reason became among the most important reasons that led to the proliferation of cyber terrorism.

- Easiness of stealth and the use of fake names:

The absence of spatial boundaries in the information network, as previously mentioned in addition to the lack of clarity of the digital identity of the user settler in the open environment is suitable opportunity for the terrorists, where a professional computer can provide the same identity and characteristics desired by or hide under a fictional character and then mount his cyber terrorist attack without a direct risk and out of sight.

- The spread of global terrorist networks:

In the world, many of global criminal networks are spread that are active in several areas, such as drugs, sex, murder, arms trafficking, money-laundering and terrorist attacks. These criminal networks often use all of their weapons, personnel and funds, and leaders in the implementation of criminal or terrorist plots against individuals and people [(1)].

(1)- To identify examples of these global criminal networks see, Abdel Fattah Ismail Abdul Kafi, terrorism and its Combating in the Modern World, 2006, without publishing house, pp.50-52.

3- Legal reasons:

Legal reasons for the spread of cyber terrorism, in particular, are related to regulatory and legal vacuum to the majority of countries of the world to address and confront this phenomenon by criminalizing the exploitation of information technology in carrying out terrorist acts. Even integrated incriminating texts are established, the offender can start from a country where strict laws do not exist and then launching his attack terrorist to another country with strict laws, here it can raise a problem of conflict of laws and the applicable law which are among the problems posed by cyber terrorism which states failed to address.

4- Globalization:

Globalization is considered of the most important reasons that led to the spread of contemporary terrorism through the appropriate climate for the growth of the phenomenon of terrorism in all its forms and effervescence, because globalization provides the means that would lead to the spread of terrorism in the entire world by exploiting the Internet as an information highway in the rumor terrorism around the world by the terrorist groups[(1)].

Section Two: Requirement means of cyber terrorism and its forms

Cyber terrorism is linked to the too advanced level, which the means of communication and information technology play in all spheres of life and in the whole world and through electronic systems and information networks, terrorism has taken new dimensions and its threat increased to the international communities, after the creation of new tools and techniques used in commission of cyber terrorism. Terrorist organizations and groups are based on various means in order to achieve their objectives related to luring individuals to engage in these groups and the implementation of their criminal schemes, these terrorist organizations and groups support on a variety of means, including:

A- Creation of websites terrorist on information network:

Terrorists take advantage of the global information network (the Internet) to create and design their own websites[(2)] through which they present their ideas and disseminate them, they also use online teaching others ways and means that will help accomplish terrorist operations such as how to make explosives, how to penetrate and destroy sites, how to access blocked sites, and then the sites become of the leading methods used in cyber terrorism[(3)].

It should be noted that the emergence of web-sites appear on the surface like a scientific organization which is really not well, for example, site Society in America carry a label the Muslim Student Association news, usually meant by the user to provide the addresses of universities or specialized institutes, but finding nothing and forwards to a site contains a detailed and comprehensive guide for all extremist organizations in the Arab world with the addresses and fax numbers that facilitate contacts[(4)].

B- The use of terrorist networks to the information network services:

---

(1)- For further expansion on the subject of globalization as a cause of contemporary terrorism see, Abdel Fattah Ismail Abdul Kafi: ibid., pp.57-75.

(2)- Website is an information stored in pages, and each page contains specific information formed by the page designer using a set of symbols called the language of the text is best (HTML), but in order to see these pages is a request for review Wide Information Network (www browser) and resolves symbols (HTML) and the issuance of instructions to show pages written.

(3)- Aycer Mohamed Attia, ibid. p.16.

(4)- For more examples of these sites, see Mostafa Mohammad Musa, a legal study of cyber terrorism, security, psychological, social, first edition, Egyptian National Library and Documentation, Egypt, 2009, pp.231-234.

Use of information network from the terrorist groups varies, in the following manners:

1- Exchange of information and the dissemination of ideas through the Internet:

It's really difficult to meet with the terrorist elements in one place and one time to learn the ways of terror and the exchange of ideas and information, but it has become easy through the Internet where a large group of people in distant places can simultaneously exchange talk and listen to each other via the Internet. Accordingly Internet has become a tool used by terrorist organizations and groups through discussion forums, and e-mail, as follows:[1]

- Chat Forums: Secret terrorist organizations realized the chat rooms dialogue as a space to the confluence of the terrorists and the exchange of news and information among themselves, as they are used at the same time to attract third parties and inciting violence and extremism, so as the Internet user has come out of curiosity or a desire to discussion and innocent dialogue, he'll find himself without knowledge in episodes of propaganda and incitement[2].

- E-mail: The e-mail is one of the means used by terrorist groups to share information among themselves and exploitation in the dissemination of ideas and promoting them via electronic mail.

2- The use of online services in achieving illegal goals of terrorist groups: Terrorist organizations use IT services and Internet technology in the accomplish of terrorist activity and spread their destructive ideas and achieve their illegal goals[3], through the following:

- Access to finance:

Terrorists are often assisted by personal information that users enter in the network through inquiries and surveys on websites to identify people with compassionate hearts, and then they are entreated for financial donations to juristic persons which represents the interface for these terrorists without doubt by the donor that he represent a terrorist group[4].

- Mobilization and recruitment of terrorists:

Terrorist groups and organizations use global information network to spread and promote the culture of terrorism and broadcast ideas that call for them, and strive to provide the greatest possible number of wishing to adopt the ideas and principles. Terrorist organizations through the information network try luring those who have tendencies and willing to engage in terrorist and sabotage acts which shall be accordingly an intellectual base gathering people who have the same ideas, tendencies and trends which makes recruitment easier later to carry out terrorist operations in the future process, that is the purpose for which terrorist groups seek to maintain their survival and continuity[5].

---

(1)- Al-Qaeda elements heavily relied on the Internet in planning for September 11, 2001 through regular e-mail messages via e-mail and rooms for the management of terrorist attacks and to coordinate actions and tasks assigned to each element of terrorism group.

(2)- Mustafa Mohamed Moussa, op.Cit., p.235.

(3)- For more details on the use of the Internet for terrorist purposes, see: Younis Mohamed Arab, the legal framework for cyber terrorism and the use the Internet for terrorist purposes, Studies and Research Center, Naif University for Security Sciences, Riyadh, Saudi Arabia, .2012, pp.165-168, Mustafa Mohamed Moussa, ibid., pp.229-262.

(4)- Abdullah bin Abdul Aziz bin Fahd Al-Ajlan, ibid. p.12.

(5)- Ibid. p.13.

- Terrorist data release:

The terrorist organizations use information networks in the deployment of various terrorist data through various means of information network, making it easier for TV channels broadcast which fasten its dissemination through various media which led to the speed of access to the various segments of society. Statements issued by terrorist organizations take a variety of directions where they draw the goals of general plans of the terrorist organization, and sometimes to threats and intimidation to launch a specific terrorist attacks, as issued, announcing the adoption of implementing specific terrorist attacks, they also comment on the news or statements issued by others.

C- The electronic eavesdropping:

The terrorist groups exploit information resources and electronic systems brought about by the scientific development in the field of information technology to spy on people, countries, organizations, international bodies and national institutions, both in the field of military espionage, political or economic, so with the presence of the means of modern espionage such as satellites espionage and satellite broadcasting, the traditional media espionage turned to electronic ways.

Spyware is as cyber terrorism if the purpose of penetrating the sites is the access to secrets and information affecting the security of the state and given to a hostile, or for the exploitation of secrets to the detriment of national unity and public interests[(1)].

Chapter Two: Legal mechanisms to fight crime in the Algerian legislation:

Section One: The preventive mechanisms

Cyber terrorism in the Algerian legislation is one of the crimes related to information and communication technologies as long as they are committed through the information system or a system of electronic communication, as referred to above. The Algerian legislature has provided for the procedures for the prevention of crimes related technologies, information and communication, in particular, in texts on the special rules for the prevention and suppression of this type of crime, as well as the establishment of the National Authority for the Prevention of it too, which we'll expose the following:

A- Rules on the control and surveillance of electronic communications systems informatics:

The Algerian legislature provided for special rules for the prevention and suppression of crimes related to information and communication technologies through the law No.09-04 dated August 5 (2009)[(2)], these rules relate to monitor electronic communications and surveillance systems informatics. Through the following, we'll address both procedures and their conditions as preventive measures of crimes related to information and communication technologies in general and the crime of cyber terrorism in particular.

1- Definition of an electronic communication surveillance and surveillance systems informatics:

- Definition of an electronic communications control:

The electronic communications control is a preventive measure stipulated by the Algerian legislature for the detection of crimes related technologies, information and

(1)- Chaanbi Sabra, op.Cit., p.446.
(2)- Official Gazette number 47, dated August 16, 2009.

communication, and is intended to measure the collection and recording of communications made through Computer or in the form of e-mail or the form of instant conversation made by computer then revealing their content in order to prevent from this type of crime[(1)]. By reference to the provisions of Law no.09-04 referred to above, the legislature has provided for objective conditions and other formalities to perform this procedure.

- Informatics systems control:

By this procedure, it is intended to inspect which is located on the information system, informatics system known as any system or a separate set of regulations related to each other where one or more of them makes an Automatic Processing of data to implement a specific program.

2- Conditions of validity of an electronic communication surveillance and informatics systems control:

These conditions are the objective conditions and other pro forma as follows:

- Objective conditions:

The objective conditions are related to the controls linked to the emergence of the right to resort to this action and in particular of the following:

- **Situations allowing** recourse to electronic surveillance and procedure informatics systems control:

Article 04 of aforementioned law no.09-04 stipulates the cases that allow resorting to surveillance and control, the cases were limited to be:

Prevention of the commission of acts described terrorist or vandalism crimes or offenses against state security: This legal description applies on the offense of cyber terrorism and considered by Algerian legislature under Article 87 bis 11 of the Penal Code as a terrorist and subversive crimes, and these procedures in this case are precautionary should be taken before committing the offense.

The case of providing information on the possible existence of an attack on the IT system of the threat to public order or national defense or state institutions or the national economy and is well known that the crime of cyber terrorism is among the most serious crimes, which represents an attack on the IT system and therefore requires the use of electronic communications surveillance, as well as informatics systems control.

The requirements of the judicial inquiries and investigations when it is difficult to access to a result in the interest of ongoing research without resorting to electronic surveillance, and in this case, the use of electronic surveillance and control will be after the commission of the crime and when it's difficult to know the perpetrators with traditional procedures.

In the framework of the implementation of international mutual legal assistance requests.

It is noticeable that all of these cases are linked to the crime of cyber terrorism and therefore we could resort to electronic monitoring and control procedure as measures to prevent the occurrence of this crime, or after the crime commission to know the perpetrators or as part of international mutual Assistant.

(1)- For more detail, see: Thabet Douniazed, Monitoring electronic communications and the right to privacy in the Algerian law, Journal of Social Sciences and Humanities, University of Larbi Tebessi, No. 6, December 2012, p.207.

- **The competent judicial authority** to resort to electronic monitoring and control procedure:

The judiciary is authorized for the issuance of the electronic monitoring and control, which was not explicitly defined in law no.09-04, but by reference to Code of Criminal Procedure, the matter is associated to the agent of the Republic or the investigating judge at the opening of the judicial investigation.

- The subject of monitoring and control:

As mentioned above, the action focuses on surveillance of electronic communications while the control is located on the IT system. We have already defined all of them above.

- **Status of the person subject to the control and surveillance:**

- Formal requirements:

The Algerian legislature through law no. 09-04 did not clarify formalities associated with this procedure, but when extrapolating the legal provisions included by the Act or in the Code of Criminal Procedure, it is necessary for the resort to electronic surveillance and control, the availability of the following formal requirements[(1)]:

-The need for the issuance of an order from the competent judicial authority to resort to electronic communications monitoring or information system control.

-The permission should be available in formality as to be released in writing and otherwise, against a known person with the necessity to clarify the nature of the required monitored electronic communications with the need to edit a record including technical operations that have been carried out.

-Causation of the authorization to resort to electronic monitoring, which should be linked to the status of the previous cases.

-The permission to be a fixed term, the legislator has identified this period in the case of terrorist crimes and sabotage and applied on the cyber terrorism by 6 months, subject to renewal, without specifying the number of times of renewal.

3- Effects of resorting to an electronic communication surveillance and systems informatics control:

Through the text on the electronic communications surveillance and systems informatics control procedures, the Algerian legislator aims to access to evidence for the purpose of the prevention of serious crimes such as cyber or to identify the perpetrators. The electronic monitor entails the compilation and the record of the content of these electronic communications, this registration should emptied in a prepared record in writing in order to maintain their integrity and not to be tampered with, the record must be placed in the case file with the sealed exhibits that should remain in the hands of the judiciary.

While the consequences of a systems informatics control are data reservation which are useful for detecting crime and the fact by copying it on the pillar of electronic storage subject to booking and putting in scores, according to the rules in force in the Code of Criminal Procedure.

B- Establishment of the National Commission for the prevention of crimes related to information and communication technologies:

(1)- For more detail about these conditions, see Thabet Douniazed, ibid. pp.215-222.

By applying the provisions of Article 13 of aforesaid Law no.09-04[(1)], it the National Commission for the prevention of crimes related technologies, information and communication was established, under the presidential decree no.15-261 dated October 8, 2015 setting for the lineup, organization and modes of functioning of Commission[(2)]. The body is considered an independent authority enjoys legal status and financial independence placed in front of the minister in charge of justice, headquartered in Algiers.

1- The Commission squad and organization:

The Commission includes[(3)]:

The Commission Director: This Committee is chaired by the Minister of Justice, and is composed of members: the Minister of the Interior, the minister in charge of mail and information and communications technologies, the commander of the national gendarmerie, General Director of National Security, a representative of the Presidency of the Republic, a representative of the Ministry of National Defense, two judges from the Supreme Court appointed by the Supreme Judicial Council[(4)].

General Directorate: headed by a General Director appointed by presidential decree[(5)].

Directorate for preventive surveillance and electronic alert[(6)].

Directorate for Technical Coordination.

Technical Operations Center.

Regional extensions.

2- Powers of the Commission:

The Commission exercises its powers enshrined in Article 14 of Law no.09-04, represented in:

- Activate and coordinate prevention operations of crimes related to information and communication technologies and their suppression.
- Help the judicial authorities and the judicial police in investigations being conducted on the relevant technologies, information and communication; include information collection and the completion of judicial experiments of crimes.
- Exchange information with their counterparts abroad in order to collect all the data useful in identifying the perpetrators of crimes related to information and communication technologies and determine their whereabouts.

Thus, Article 4, paragraph 2 of Presidential Decree 15-261 added other powers of the Commission as follows:

- Suggests a national strategy for the prevention of crimes.

---

(1)- See Article 13 of Law no.09-04 on the prevention of crimes related to information and communication technologies and their suppression.

(2)- Official Gazette number 53, dated October 8, 2015.

(3)- See Article 6 of Presidential Decree no.15-261 dated October 8, 2015, set for the lineup, organization and modes of functioning of the National Commission for the prevention and suppression of offenses against information and communication technologies.

(4)- For more details on the powers of the Committee, see Article 8 of Presidential Decree no.15-261, dated October 8, 2015, set for the lineup, organization and modes of functioning of the National Commission for the prevention and suppression of offenses against the information and communication technologies.

See also Counter-Terrorism Committee Executive Directorate (CTED), The Role of the Prosecutor in Terrorist Cases, seminar, Algiers, 5-7 June 2012, pp;1 and beyond.

(5)- To view the powers of the general director, see Article 10 of Presidential Decree no.15-261.

(6)- To see the powers of the general director, see Article 11 of Presidential Decree no.15-261.

- Ensures preventive monitoring of electronic communication inadvertent disclosure of crimes related to terrorist acts and sabotage and those which undermine state security, under the authority of a competent judge and excluding any other national bodies.
- Collects, records and preserves digital data and determine their source and routing for use in judicial proceedings.
- Develops cooperation with institutions and national bodies involved in crimes related to information and communication technologies.
- Contributes to the training of investigators specialized in the field of technical investigations related to information and communication technologies.
- Contributes to the modernization of legal standards in the field of its competence.

Following the competence of the above-mentioned body, it is clear that the tasks and powers entrusted to the National Commission for the prevention of crimes including the offense of cyber terrorism, aim to develop judicial and technical research areas to confront this type of crime.

Section Two: The deterrent mechanisms

Deterrent procedures are associated with the element of criminality and punishment, and therefore will, through the following, expose the elements of the cyber terrorism crime and the penalty in the Algerian legislature through the following sub:

A- Elements of the crime of cyber terrorism:

Cyber terrorism is a criminalized act by the legislator after the amendment to the Penal Code in accordance with the aforementioned 16-02 under articles and 87 bis 11, Article 87 bis 12, and in the light of this legal text, we determine the elements of the crime as following:

1- Actus reus:

The material element of the offense of cyber terrorism as stipulated in articles 87 bis 11 and 87 bis 12 requires elements related to criminal behavior, the result, the causal relationship between them, represented as follows:

- Criminal Behavior:

To accomplish the crime cyber terrorism, it's enough that the criminal offender commits one of the following:

- Travels (Algerian or foreign resident in Algeria) or attempts to travel to another country.
- Provides or collects by any means, directly or indirectly, money or the intent to use them with knowledge that they will be used to finance the travel of people to another country.
- Financing or organizing people travel to another country.
- Recruit people for the benefit of a terrorist association or organization, group or organization whose purpose or activities fall under the sanctions on the crime of terrorism, or organize their affairs or supports acts or activities or publish their thoughts directly or indirectly.

- Rea result:

Criminal behaviors must be associated with the above mentioned outcome of the crime i.e. to commit terrorist acts or planning, preparation or participating in training or to commit or to receive training which is the same goal that the culprit wanted to achieve.

- Causal relationship:

It must be linked to the result of criminal conduct committed by the offender.

2- Means used:

The crime or the criminal features referred to above must be committed through the use of information and communication technologies as referred to above. It is intended by technologies information and communication, the commission of the crime through the IT system or a system of electronic communication.

3- Mens rea:

Mental element is defined as a relationship between the crime materialism sides and personal offender, and accordingly takes one of two images: Criminal Intent and an unintentional error.

According to the text of the legislature, cyber terrorism is an intentional crime requires for its availability the criminal intent, whether special or general.

- General Criminal Intent:

The Algerian legislature did not define criminal intent, and by reference to the Fiqh, it's the interference of the offender voluntarily in order to commit an unlawful act with the enjoyment of all his mental faculties**(1)**. It's also known as the resort of the will of the offender towards acting with knowledge that the law forbids it**(2)**. The legislator stipulated explicitly the element in articles 87 bis 11 and 87 bis 12.

- Dolus specialis:

It consists in the end destination of the perpetrator of the offense as well as his will to conscious violation of Penal Code**(3)**. It is noticeable that the Algerian legislature, according to the crime of terrorism in general, and the crime of cyber terrorism in particular, requires special criminal intent which is to end by the culprit behind his act set by Article 87 bis 11 on the occasion of the use of information and communication technologies in the commission of terrorist acts, planning, preparation or participation in training or to commit or to receive training or travel to train.

B- Punishment prescribed by law:

By reference to the provisions of Articles 87 bis 11 and Article 87 bis 12 the legally due punishment for the crime of terrorism committed through information and communication technologies is the temporary imprisonment from 5 to 10 years and a fine of 100,000 to 500,000 DZD.

Conclusion:

This study dealt with one of the most important issues emerging on the legal arena and on a one of the manners of modern crime, the cyber terrorism, and therefore this study aimed at revealing the confusion about this manner of induced criminalization, where it focused on its definition, the statement of its properties, its objectives, its causes and means, then study was concluded to reflect the position of The Algerian legislator on the cyber crime through exposing the elements of the crime and the prescribed punishment, as well as preventive mechanisms to combat it.

Findings:

- The Algerian legislation is one of the Arab leaders in the fight against terrorism, legislations

(1)- Hussein bin Sheikh, Lessons in Penal Code, Houma Publishing, Algeria, 2014, p.149.
(2)- Bouskiaa Ahcene, brief in common criminal law, Houma Publishing, Algeria, 2012/2013, p.147.
(3)- Ibid., p.147.

through enacting a large arsenal of legal texts to cope with the phenomenon, as well as one of the first laws that criminalized the use of information technology in the crimes of terrorism. It is really a law that deserves study and analysis[(1)].

- The cyber terrorism is the next threat to the international community due to its multiplicity of forms and methods diversity as well as its breadth of goals, which is accessible through means of telecommunications and information technology and threatening security and stability.
- The lack of legal safeguards surrounding the provisions of electronic communications surveillance and systems informatics control procedures.
- Lack of national legislation encountering all the updated manners of terrorism through modern technology.
- Deficiency of training among investigators in the field of technology-related information.

Recommendations:

- The need to unify the international efforts to find a common definition of terrorism in general and cyber terrorism in particular.
- The need to keep up with incriminating texts against the developed manners of cyber terrorism constantly, as well as the enactment of laws and legislation that fill all the gaps surrounding the offense of cyber terrorism or methods of investigation, methods of electronic discovery and preservation of evidence.
- The need to develop a national strategy for the prevention and suppression of crimes related to information and communication technologies.
- The imposition of adequate oversight by the state through the developed body on all what is offered through the information network technology to block access to sites that broadcast terrorist ideology and tighten it and be blocked if necessary by special informational programs.
- The involvement of civil society in the need for cooperation on reporting on sites related to terrorists and terrorism, as well as to disseminate of culture of prevention and response of community, awareness about the danger of terrorism.
- Unify efforts, national and international in the fight against cyber terrorism, and is part of the expansion, development and improvement of international cooperation in the criminal level traditional mechanisms as well as the coordination and exchange of information and experiences between all the devices involved in combating cyber terrorism in all countries of the world.
- To convene more research, studies, seminars and conferences to study the seriousness of cyber terrorism and its development.

References:

Official texts:

- ✓ Ordinance No. 66-156 of 8 June 1966 on the Penal Code, as amended and supplemented.
- ✓ Law no.09-04 on the prevention of crimes related to information and communication technologies and their suppression.

(1)- UN-ESCWA, The ESCWA Cyber Legislation Digest, Development Account Project, Regional Harmonization of Cyber Legislation to Promote Knowledge Society in the Arab Region, United Nations, New York, 2013.

- ✓ Presidential Decree no.15-261 dated October 8, 2015, set for the lineup, organization and modes of functioning of the National Commission for the prevention and suppression of offenses against information and communication technologies.

Books:

- ✓ Abdel Fattah Ismail Abdul Kafi, terrorism and its Combating in the Modern World, 2006, without publishing house.
- ✓ Bouskiaa Ahcene, brief in common criminal law, Houma Publishing, Algeria, 2012/2013.
- ✓ Faleh Haitham Shehab, the crime of terrorism and ways to combat it in the comparative criminal legislation, Culture House for Publishing and Distribution, Amman, Jordan, first edition 2010.
- ✓ Fortna, Virginia Page (20 May 2015). "Do Terrorists Win? Rebels' Use of Terrorism and Civil War Outcomes". International Organization. 69 (3).
- ✓ Hussein bin Sheikh, Lessons in Penal Code, Houma Publishing, Algeria, 2014.
- ✓ I.L. Braber, Defining the crime of terrorism in international law – a legal minefield, University of Amsterdam, Graduate School of Law, July 2013.
- ✓ Mostafa Mohammad Musa, a legal study of cyber terrorism, security, psychological, social, first edition, Egyptian National Library and Documentation, Egypt, 2009.
- ✓ UN-ESCWA, The ESCWA Cyber Legislation Digest, Development Account Project, Regional Harmonization of Cyber Legislation to Promote Knowledge Society in the Arab Region, United Nations, New York, 2013.
- ✓ United Nations Office ON Drugs And Crime, the use of internet for terrorist purposes, United nations, new York, 2012.
- ✓ Younis Mohamed Arab, the legal framework for cyber terrorism and the use the Internet for terrorist purposes, Studies and Research Center, Naif University for Security Sciences, Riyadh, Saudi Arabia, 2012.

Theses and dissertations:

- ✓ Abbas Chafaa, terrorist phenomenon between international law and religious perspective, Ph.D. thesis, University of Batna, 2011.
- ✓ Dardour Nassim, computer crime in the light of the Algerian and Comparative Law, Master Thesis, University of Constantine, 2013.
- ✓ Dich Musa, the legal system to compensate victims of terrorist crimes - a comparative study -, PhD thesis, University of Tlemcen 2016.

Articles:

- ✓ Amir Hassan Turki, Salam Jassim Abdullah, cyber terrorism and risks in the current era, Journal of Legal and Political Sciences, special issue, Faculty of Law and Political Science, University of Diyala, Iraq.
- ✓ Thabet Douniazed, Monitoring electronic communications and the right to privacy in the Algerian law, Journal of Social Sciences and Humanities, University of Larbi Tebessi, No. 6, December 2012.

Symposiums:

- ✓ The Sixth Conference in Copenhagen in 1935.
- ✓ United Nations of the Next Decade, Implementation of the UN Global Counterterrorism Strategy, 42nd Conference on the United Nations of the Next Decade, June 8-13, 2007.
- ✓ Abdullah bin Abdul Aziz bin Fahd Al-Ajlan, cyber terrorism in the information age, working paper submitted to the International Conference on protection of information security and privacy in Internet Law, held in Cairo from 2 to 4 June 2008.
- ✓ Mohammed bin Abdul Aziz bin Mohammed Al-Aqeel, Electronic incitement to terrorism: idiosyncratic adaptation and judgment - Twitter model -a working paper submitted to the International Conference: The Arab media's role in dealing with the phenomenon of terrorism, Naif Arab University for Security Sciences.
- ✓ Counter-Terrorism Committee Executive Directorate (CTED), The Role of the Prosecutor in Terrorist Cases, seminar, Algiers, 5-7 June 2012.
- ✓ John Rollins, Liana Sun Wyler, Terrorism and Transnational Crime: Foreign Policy Issues for Congress, Congressional Research Service, June 11, 2013.
- ✓ Aycer Mohammed Attia, the role of modern mechanisms in curbing novel Electronic crime: terrorism and ways to confront it, working paper submitted to the scientific forum on novel crime under the light of the

current regional and international transformations, held at the Faculty of Strategic Sciences, Amman, 2 to September 4, 2014,.

- ✓ Abdul Aziz Bin Humaidan Thumali, the impact of cyber terrorism and ways to combat it, research presented to the World Islamic Conference on combating terrorism, organized by the Muslim World League, Makkah, held on 22 to 25 February 2015.
- ✓ Abdul-Qader al-Sheikhli, the nature of the cyber terrorism, a paper submitted to the global Islamic Conference on the fight against terrorism, organized by the Muslim World League, Makkah, held on 22 to 25 February 2015.

Websites:

https://en.wikipedia.org/wiki/Terrorism, last entry 13 March 2017, at 12:54.

- ✓ http//:www.assakina.com/wp-content/uploads/2015/6/28
- ✓ http://repository.nauss.edu.sa/handle/123456789/60016
- ✓ www.themwl.org/peace/
- ✓ http://www.shaimaaatalla.com/vb/showthread.php?t=3937
- ✓ www.themwl.org/peace/