Electronic Terrorism

الإرهاب الإلكتروني

Ladgheche Salima **(1)**
Ladgheche Rahima **(2)**
(1) *Faculty of Law and Political Sciences-University of Djelfa, (Algeria)*
ladgchesalima@yahoo.fr
(2) *Faculty of Law and Political Sciences-University of Djelfa, (Algeria)*
drrahimala@gmail.com

RECEIVED	ACCEPTED	PUBLISHED
25 – 04 - 2020	08 – 09 - 2020	30 – 09 - 2020

Abstract:

The electronic terrorism phenomenon is the electronic version of traditional terrorism. This research aims to identify the concept of information crime and electronic terrorism, and explain their characteristics as well as clarifying the growing role that the Internet plays in spreading ideas and principles of terrorist organizations. In this study, we have relied on the descriptive analytical approach through the study of electronic terrorism, where our main lines of work were analysis and interpretation. As for the conclusions reached from it, that one of the greatest means used in electronic terrorism is to use electronic mail to communicate among terrorists and exchange information between them. The security services also need a lot of work to develop their capabilities so they can deal with computer crimes and prevent them.

key words: *Threat; Communications ; Internet; Information Crime; Electronic Terrorism.*

الملخص :

تعتبر ظاهرة الإرهاب الإلكتروني النسخة الالكترونية من الإرهاب التقليدي ويهدف هذا البحث إلى الوقوف على مفهوم الجريمة المعلوماتية والإرهاب الالكتروني وبيان خصائصهما بالإضافة إلى توضيح تنامي الدور الذي يلعبه الانترنت في نشر أفكار ومبادئ التنظيمات الإرهابية. ولقد اعتمدنا في دراستنا هذه على المنهج الوصفي التحليلي من خلال دراسة الإرهاب الإلكتروني، والتعرض له بالتحليل والتفسير. أما عن الاستنتاجات المتوصل إليها فمنها؛ أن من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم. كذلك أن أجهزة الأمن تحتاج إلى كثير من العمل لتطوير قدراتها للتعامل مع جرائم الكمبيوتر والوقاية منها.

الكلمات المفتاحية: تهديد؛ اتصالات؛ انترنت ؛ جريمة معلوماتية ؛ إرهاب إلكتروني.

(1) *Corresponding author:* ***Dr ladgheche Salima*** *e-mail: ladgchesalima@yahoo.fr*

Introduction:

Information crime is the unlawful act committed by a perpetrator who is familiar with computer technology, with the intention of attacking programs and using them as leverage. In this era of technological development and widespread use of the Internet, the employment of digital technologies by terrorists has caused countries great harm by implementing their terrorist plans. Electronic terrorism is a stage in which terrorist organizations have developed their methods to achieve their goals broadly and at minimal costs.

The importance of the subject: Since ancient times, Mankind has suffered from a dangerous phenomenon represented in the appearance of many criminal acts against individuals and society, that aim to raise terror and spread fear. In the current era, and due to the development of information technology, new patterns of crimes have emerged, after the computer networks are linked to the global intranet , Which led to the emergence of the crime of electronic terrorism, which is characterized by being cross-border and by its speedy implementation, and this is where we can see the importance of studying this issue.

The problem of the study: In general, Terrorism is a complex phenomenon due to the multiplicity of its causes, so cyber terrorism became an obsession experienced by all countries and feared by individuals, that is why it is difficult to deal with it without defining the information crime and its characteristics, also explain the methods of electronic terrorism and methods to fight it. There is no doubt that this phenomenon requires the necessity of researching in its different aspects.

From the precedent we present the following main problematic: What are the meanings of electronic terrorism and what are the effective ways or methods to combat and fight it?

And from this main problematic we propose, ask and focus to the following sub-questions:

What is the definition, meaning, concept or term of information crime? What is electronic terrorism? How can we define the characteristics of electronic terrorism?

Methodology used: In this article, We relied on the descriptive analytical method, by highlighting the phenomenon of electronic terrorism, and explaining its features and its identification, as well as analyzing this new terrorist crime.

To answer the questions of the problem of the study, this article was established through two main topics:

- The Concept of Information Crime and Electronic Terrorism
- The Means of Electronic Terrorism and Methods of Combating it

Section I: The Concepts of Information Crime and Electronic Terrorism

We demonstrate the concepts of information crime and electronic terrorism, by providing a definition for each, and by highlighting their characteristics as follows:

A) The Concept of Information Crime:

Many professors and researchers have provided several definitions of information crime, depending on: its object, the aggressor's interest, its dimensions, its targeted field and its extent. Information crime has several characteristics, which we present in the following two sub-categories:

1-**The Definition of Information Crime :**

Information crime can be defined as the crime that is committed if a person uses his knowledge of the computer and the working systems of information network illegally, and there are those who define it as any illegal work in which the computer and its systems are used as a tool or subject of the crime[1].

Some jurists see it as every act or willful omission that results from the unlawful use of information technology and aims to attack material or moral funds[2].

Another definition, an information crime is every criminal activity in which the computer system performs an instrument that is not completely criminal or has been replaced by it[3].

Informatics crimes are also known as: "that type of crime that requires special knowledge of computer technologies and information systems, to commit or investigate and prosecute the perpetrator," and it can also be defined as" the crime that is committed if someone uses his knowledge of the computer with an illegal act, " also there are those who define it as: "Any illegal act in which the computer is used as a tool or subject for crime", and in all these cases, the crime of informatics does not care about the borders between countries, not even between continents, as it is a crime that often occurs across many international borders[4].

The Algerian legislator has called the term "information crimes" the term "crimes related to information and communication technologies," and according to the provisions of Article N°2 of the Law 04/09 dated 05/08/2009 that contains the special rules for the prevention and control of crimes related to information

and communication technologies, in the Official Journal N°. 47 of 2009, he defined them as: "Crimes of prejudice to the systems for the automatic processing of data specified in the Penal Code and any crime committed or facilitated by an information system or electronic communication system"[5].

By setting the law 04/09 which includes the special rules to prevent and combat crimes related to information and communication technologies, whose texts were mostly in conformity with the provisions of the Budapest Convention to combat information or virtual crime, especially procedural texts, the legislator aims to establish a legal framework appropriate to the privacy and seriousness of information crime, that's why the law came to combine the procedural rules that complement the Code of Criminal Procedure with the preventive rules that allow early monitoring of possible attacks and rapid intervention to identify the source of the attacks and identify the perpetrator in order to achieve protection for Criminal electronic data from the information crimes[6].

The national legal system did not know the so-called attacks on automated data processing systems, except after the amendment of the Penal Code according to the Law N°. 15/14 dated 10/11/2004, in which the legislator completed Chapter Three of Chapter Two of Book Three with a new section, Section Seven bis, which includes articles from 394 to 394 bis 7. The French legislator preceded the Algerian legislator by the issuance of Law No. 88/19 of 01/05/1988 related to information fraud[7].

2-**Information Crime Characteristics**:

- It requires to have a computer and the technical knowledge to use it: the computer is considered as one of the main requirements for committing computer crimes until it is considered so, in addition to the above, these crimes require sufficient knowledge of technical skills and knowledge, such as technical knowledge of the computer and how to operate it and use it and this is confirmed by studies and statistics that dealt with the issue, as the perpetrators of these crimes are specialists in processing information automatically [8].

- The trans-boundary (international) nature of information crime: It can be said that one of the most important characteristics that distinguishes an information crime is its transcendence of geographical boundaries, and then its acquisition of an international nature, or as some people call it crimes of a cross-border nature, after the emergence of information networks, the borders are no longer visible or concrete stands in the way of the transmission of information across different countries. The ability of computers to transfer and exchange large amounts of information between systems separated by thousands of miles, have

led to a result that indicates that multiple places from different countries may be affected by a single information crime at the same time, and the tremendous speed through which the crime is executed Informatics, the amount of information and targeted funds, and the distance that may separate the perpetrator from this information and funds. The information crime has characterized the traditional crime significantly [9].

- The difficulty of proving cyber crime, the difficulty of proving cyber crime is due to many things[10].

1- It is a crime that does not leave any material effects after it is committed, it is a crime that occurs in an electronic environment in which information is transferred and circulated electronically, it is an invisible transfer and there is no paper documents.

2 - The difficulty of keeping a technician in the evidence of electronic crime, as the electronic criminal can, in less than a second, erase or distort data and change the information on the computer.

3- You need technical expertise and the traditional investigator is difficult to deal with. The computer crimes require special knowledge of computer technologies

4- It depends on intelligence to commit it, and it can be described as smart crime.

Attractive crimes for criminals: These are fast-tracked crimes that require neither effort nor movement to the crime scene and its difficult discovery, so it is easy to commit it to an employee of a company that depends on computers for its work in exchange for huge profits[11].

B) The Concept of Electronic Terrorism:

Cyber terrorism is a crime that is mainly associated with terrorism and extremism, as electronic terrorism represents the evolution of violence and terrorism, using technology, we show the concept of electronic terrorism as follows:

1-Definition of Electronic Terrorism :

The meaning of terrorism is the use of violence, or the threat of it and its various forms, such as assassination, mutilation, sabotage and torture, in order to achieve a specific political goal, such as breaking the spirit of resistance among individuals and demolishing morale in the public, which is the use of coercion to subjugate a party opposing the will of the terrorist side. It is violence directed against the public in order to achieve the appearance of fear.[12].

It is also the aggression practiced by individuals, groups, or states against a person in his religion, blood, mind, money, and width, and it includes the types of intimidation, harm, threat, unlawful killing, and related to images of sparring, intimidating the way, and blocking the way, and every act of violence or threat, It takes place in implementation of an individual or collective criminal project, and aims to throw terror among people, intimidate them by harming them, or endanger their lives, freedoms, security, or conditions of danger [13].

As for electronic terrorism, it is the activities carried out by individuals or groups using information technology and the Internet, with the intention of destroying the associated and managed infrastructure with such technology, such as water and electricity distribution networks, banking services systems, health records, military systems, and other infrastructure that their destruction would cause direct and indirect damage to citizens and states[14].

It is also aggression, intimidation, or threats, financially or morally, by using electronic means issued by states, groups, or individuals against a person's religion, self, honor, mind, or money, without the right, in all its forms, and forms of corruption on earth[15]. This type of terrorism is a manifestation of the fusion between violence for political purposes and the employment of modern technologies in the areas of communication and information, which is one of the most prominent mechanisms of globalization[16].

Electronic terrorism is the digital weapon that uses modern technological means for the purpose of aggression, intimidation, and material or moral threat emanating from states, groups, or individuals against a person in his or her religion or himself, or unlawfully displaying it, his mind, or his money, or on state institutions and with all kinds and forms of aggression [17].

The Criminal behavior in information terrorism consists in creating a website or publishing information on the Internet belonging to a terrorist group, under camouflage designations to facilitate communication with members of this terrorist group, or to promote its ideas and recruiting new terrorists, or to finance it or to highlight the strength of the terrorist organization, and to give instructions and e-training through Teaching ways and means to carry out terrorist attacks. Terrorist websites have been created on the Internet that show how to make bombs and explosives, and deadly chemical weapons, as well as ways to hack email, and how to penetrate and destroy websites. Electronic, and access blocked sites, and teaching methods of spreading viruses to other acts of sabotage. Information terrorism is distinguished from other types of terrorism in the modern way of using information resources and electronic means created by the

civilization of technology in the information age, so electronic systems and infrastructure are the target of terrorists[18].

Penetrating information systems and networks has become possible, as well as using them to destroy the information infrastructure that supports the governments, public institutions and major economic companies. Because of the interconnection of information networks, the possibility of a breakdown of information system infrastructure and information networks is not in the targeted countries or in major companies only but in the world all this is not excluded, and the danger of information terrorism lies in the ease of using this digital weapon, as the information terrorist from his home or office, and in complete secrecy out of the sight of the authorities and society, presses the keyboard and from Then destroying the information infrastructure by targeting and closing vital sites, or paralyzing command and control and communications systems, cutting off networks, disrupting air defense systems, derailing missiles from their path, controlling air, land and sea navigation lines, or paralyzing power and water supply stations, or the penetration of the banking system and damage to the business of banks and global financial markets, this causes great losses that exceed those caused by explosives and traditional terrorist acts.

E-mail is used to communicate among terrorists among them, ensuring the secrecy of communications and the exchange of information, as terrorist groups exploit the Internet to create sites to publish their data, promote these groups and create an intellectual base among the network users to bring in new elements and recruit them, thus ensuring the continuity of the terrorist action[19].

Terrorism in the digital age, or what is known as terrorism via Internet, is that of harnessing the international information network (the Internet) in practicing terrorist activities (planning, training and implementation) by taking advantage of the capabilities that this network facilitates for terrorists, as well as what this network itself is exposed to direct attacks in order to destroy and destroy the data and information stored in it or paralyze its work so that it is no longer able to perform its role efficiently for revenge, extortion, or the achievement of a destination (political or otherwise), as in broadcasting various viruses to destroy and destroy the databases or files of the target party with terrorism or by what is known as logical bombs, and electronic bombing[20].

Terrorist groups recruit - through the Internet - new terrorist elements to help them carry out their criminal acts, and in that they depend on the youth, especially the mentally and intellectually vulnerable, so terrorist groups announce through their websites about their need for suicide elements as if they advertise

job vacancies for young people, using the religious aspect to achieve that. It always describes the goals that their operations target as unbelievers, inviting young people to Jihad and urging them to martyred for the sake of God and win paradise. The websites of terrorist groups provide a great deal of control over the information and media messages that they want to direct, but also give them the flexibility to send messages to different groups of the target audience, and to draw a mental image of the group and its enemies as well[21].

2- Characteristics of Electronic Terrorism :

the characteristics of electronic terrorism : Electronic terrorism is characterized by a number of characteristics and features in which it differs from other crimes, and prevents it from being mixed with ordinary terrorism. The most important of these characteristics can be summarized in the following[22]:

1- Electronic terrorism does not require violence and force in its commission, but rather a computer connected to the information network and equipped with some necessary programs.

2- Electronic terrorism is characterized as a transnational terrorist crime, transnational and continental, and not subject to a limited regional scope.

3- The difficulty of detecting cyber terrorism crimes, and the lack of experience of some security and judicial agencies in dealing with this type of crime.

4- Difficulty of proof in electronic terrorism, given the rapid absence of digital evidence, and the ease of destroying it.

5- Electronic terrorism is characterized by the fact that it usually takes place with the cooperation of more than one person to commit it.

6- That the perpetrator of electronic terrorism is usually from those who specialize in the field of information technology, or at least someone who has a degree of knowledge and experience in dealing with computers and the information network.

7- Electronic terrorism leaves no physical evidence after committing its crimes, which makes it difficult to trace and discover the crime in the first place. Basically tracking and detecting crime.

8- Ease of destroying evidence if any evidence is found that can convict the perpetrator.

Electronic terrorism also has other characteristics [23]:

9- Ease of communication between terrorists from a distance without the need to meet them through E-mails, chat rooms, or the like through the means

provided by the World Wide Web, and this would make it difficult to determine their whereabouts.

10- Terrorist acts in general, which are carried out via or on the Internet, are characterized by belonging to the sect of organized crime, or at least they share some characteristics with it. Informatics makes it more eager to organize itself tightly and accurately in order to make the most of the privileges offered by this network.

11- Terrorist crimes via Internet are easily funded by using the information network to transfer money as quickly as possible, and under usually borrowed names.

12- Carrying out terrorist activities does not require moving from one place to another, or being in places that are a target for terrorists, but rather it may be done remotely by entering the private site and disrupting its system.

13- Terrorism via Internet is classified as a cross-border crime or continent, or what is known as transnational crime that transcends the regional borders of States, which gives it an international dimension, and this would create many legal challenges to confront and address it with regard to specific procedures for inference, investigation and trial. Due to the difficulty in determining the location of the crime and hence the applicable law, terrorist activity may take place in the east of the globe and the harmful result lies in the west, which raises conflicts of competence in relation to it, and requires the formulation of appropriate legal rules for this type of crime.

14- The losses caused by terrorism in the digital age are fatal, almost twice the losses caused by traditional terrorist acts, whether in terms of lives or property, especially in countries that rely heavily on information technology.

15- Terrorism via Internet is no longer limited to achieving political goals, as it is usually the case with traditional terrorism, but it rather has multiple other purposes, and may be foremost among them economic, retaliatory, or religious purposes.

Section II: The Means of Electronicterrorism and the Methods to Fight it

The means of cyber terrorism vary in order to achieve its goals, and accordingly several methods have been found to combat it, separating them as follows:

A) Means of Electronic Terrorism:

Electronic terrorism has many tools, which are E-mail, the creation of websites on the Internet, and the destruction of websites. We describe them as follows:

1-E-mail :

It is one of the important means used in electronic terrorism, by using the E-mail to communicate between terrorists and exchange information between them. Actually, many terrorist operations that happened; the E-mail were a tool of exchanging information and transferring it between the ones involved in terrorist operations and those who planned them. Terrorists exploit E-mail, the worst exploitation of it also, by spreading and promoting their ideas and seeking to increase the number of followers and sympathizers through electronic correspondence[24].

2- Creating Websites :

Terrorists create and design websites for them on the World Wide Web (the Internet) to spread their ideas and advocate for their principles, but rather to teach ways and means that help in carrying out terrorist operations, websites have been created to teach the manufacture of explosives, how to penetrate and destroy websites, ways to penetrate e-mail, and how to enter Blocked websites, method of spreading viruses and more. If obtaining media outlets, such as television and radio channels, is difficult, creating websites on the Internet and exploiting dialogue forums and others to serve the goals of terrorists is easy and possible, and some terrorist organizations find thousands of websites, in order to ensure a wider spread, and even if access to some of these websites is prevented Otherwise, other websites may be accessible[25].

Terrorists have found their goal in the digital means in the information revolution, so terrorist organizations have many websites on the World Wide Web the (Internet), so those websites have become one of the most prominent means used in electronic terrorism. What increases the severity of these websites, that terrorist or extremist groups depend in their terrorist plans and methods on simple methods that allow everyone direct access to blocked sites through regular browsing or through exchange programs, and there are websites that publish sensitive information about how to prepare explosives and toxic materials and manufacture lightning strikes in accurate details And components, many of which can be obtained from anywhere without raising suspicion, and the risk of providing this information is not limited to misguided groups, but it can pave the way for committing individual crimes[26].

3- The Destruction of Websites :

Destruction of sites means: unlawful access to a primary or secondary link point connected to the Internet through an automated system (PC-Server) or a networked interconnected systems group (Intranet) with the aim of sabotaging the point of contact or system[27].

This is done through a number of individuals who have advanced skills in computer programs and through which we can send a repressed number of files to the website to be destroyed at the same time, thus confusing the site for its inability to absorb these files, which in turn leads to the destruction of the website[28].

There is no technical or organizational means that can be applied and completely prevents the website from being destroyed or permanently hacked, as technical variables and the penetrator's knowledge of the gaps in the applications, which were built mostly on the basis of the open design of most parts of the open source)) whether in the connection point components or systems or the network or programming, has made the prevention of penetrations very difficult, in addition to that there are terrorist organizations that include within their work and responsibilities the desire to penetrate and destroy websites and it is known that the institutions have the capabilities and capabilities that the individuals do not have.

Computer hackers (Hackers) can access confidential and personal information and penetrate privacy and confidentiality of information easily, due to the amazing development in the computer world that is accompanied by greater progress in information crime and the ways to commit it, especially since the perpetrators are not ordinary users, but may be experts in the field computer[29].

The electronic penetration process is carried out by leaking the main data and codes for the Internet programs, and it is a process that takes place from anywhere in the world without the need for the presence of a penetrator in the country where the websites were penetrated because the geographical dimension has no importance in limiting electronic penetrations and is still a large percentage Of the breakthroughs not yet discovered due to the complexity of the computer operating system.

One of the methods used to destroy websites is to pump hundreds of thousands of E-mails from the destroyer's computer to the target website to affect the website's storage capacity, so this huge amount of E-mails constitutes pressure that ultimately leads to the explosion of the working website on the network and the dispersal of data The information stored on the website is transmitted to the

aggressor's device, or enables it to freely navigate the target website easily and easily, and obtain all the numbers, information and data that it needs for the attacked website[30].

B) Methods to Fight Electronic Terrorism :

The methods of combating electronic terrorism vary between prevention and treatment methods, as follows:

1- Methods to Prevent Electronic Terrorism :

Given the risks posed by terrorist activities via Internet, the countries of the world are beginning to feel the imminent danger, and they are seriously thinking about countering this type of terrorism by developing technologies that enable them to protect themselves from terrorist attacks via Internet, as well as reviewing their national legislation to counter this pattern of Terrorism, also by strengthening cooperation between them through collective and bilateral agreements and raising the efficiency of the security and judicial agencies in order to be able to track terrorists and reveal their plans. Among the efforts made in this regard, many countries have tended to pass legislation to combat information criminality, including terrorist activities over the Internet, by issuing special legislation for this purpose or by introducing amendments to their penal laws[31].

The media is considered one of the most powerful modern communication tools that helps the receiving audience to experience the era and interact with it, and it has also an important role in explaining issues and putting them before the public opinion in order to prepare it, especially towards issues related to national security, as well as to what is going on the World stage. From this angle, the twenty-first century is considered the era of international media and propaganda with all its political, military, economic and social components in light of the communication and information revolution, which will not stop with the continuation of the process of innovation and change that led to a huge development in communication and information technology, and it should be noted that the media has an active role in shaping the context of political reform in different societies, as it reflects the nature of the relationship between the state and society. The contribution and role of the media in the process of political and democratic reform depends on the form and function of those means in society and the size of freedom, the multiplicity of opinions and trends within these institutions. From this angle, the Arabic and international media have focused on the phenomenon of terrorism and extremism and its implications for the Arabic region and the world[32].

- To impose adequate control by the government on everything that is created through the network to prevent access to some sites that transmit terrorist thought, by proposing the creation or design of a computer program called "Internet Police" whose tasks are to purify the Internet aimed at blocking terrorist sites. It prevents users from obtaining incorrect and harmful information, and deletes and stops any messages from sources that are hostile to the values and traditions of our society[33].

- Internet access filtering [34]: No country in this era that can live isolated from the rapid technological developments and the economic, social, and security implications arising from it. In light of the close interconnection between parts of the world through information and communication technologies and applications which allowed the flow of money, goods, services, ideas and information between the users of those techniques, it became necessary for every country to protect its individuals, institutions, capabilities and civilization from the effects of this openness, and with everyone now recognizing the great benefits of information technology, the dangers inherent in the penetration of this technology in our homes and institutions require society and the state as a whole to prevent these risks of all kinds from occurring. One of the most important things that must be provided in this regard is the prevention of harmful websites that call for corruption and evil, including websites that call and teach terrorism, aggression and assaulting others, as this method is one of the useful and beneficial methods, for a person does not expose himself to temptation and evil. The Muslim asks Allah to protect him from being tempted, and Almighty God - says about Joseph, *peace be upon him*: {**He said, "My Lord, prison is more to my liking than that to which they invite me. And if You do not avert from me their plan, I might incline toward them and [thus] be of the ignorant."**} [Holy Quran][35].

It has been stated in some studies that countries that impose strict laws to prevent harmful and destructive websites have a low crime rate, and that's why the city of King Abdulaziz for Science and Technology has sought to block pornographic websites from Internet users in the Kingdom of Saudi Arabia in order to preserve morals and maintain the nation from the tampering of the tampered and the criminals corruption. In the year 1417 AH, Cabinet's Resolution N°. (163) was issued, entrusting the King Abdulaziz City for Science and Technology with the task of introducing the global Internet service to the Kingdom, and undertaking all necessary measures, including filtering the content.

Some countries have sought to block harmful websites. In Turkey, the Turkish telecommunications company that provides all parts of the country with

Internet services has decided to block some harmful websites on the Internet, and therefore it has installed devices and tools that purify the sites and block harmful websites and prevent their occurrence, and there are Several Islamic and non-Islamic countries filter the Internet and block websites that seem to be morally or intellectually harmful.

- Evidence service: Evidence services software are private databases, usually of a high level of security, designed to collect and manage information related to networks users. The goal of this kind of software is not only to collect passwords and usernames, but it has evolved today to include the biological features of the users. This information is used to renew the rights of users on the network with all its components, such as applications, servers, and folders, and even the screen format used by the user. It is centrally managed from the network administrator's office without any need to visit the device or the user. The company of Novell is the leader in this field with its wide collection of applications dedicated to this purpose [36].

2- Methods of Curing the Electronic Terrorism :

The methods of curing the electronic terrorism are divided to: the methods of the stage before the crime, contemporary methods of the occurrence of the crime, and methods after the occurrence of the crime, as follows:

First: The Stage Before the Crime Occurred

It can be said that this stage depends and is based on several axes that can be summarized as follows [37]:

1- Axis I: Monitoring and following up on suspicious websites through sections and teams specialized in electronic terrorism only.

2- Axis II: strengthening regional and international cooperation between the different countries of the world in following up and monitoring such suspicious websites.

3- Axis III: focusing on conducting in-depth studies and research on electronic terrorism, its images and effects, and submitting the necessary recommendations to the competent authorities in the state to put in place the necessary legislation to confront such crimes and reduce and control them as soon as they are discovered. Here, the importance of a tight legislative system and penalties deterred by the organization highlights the work of places and shops, the role of amusement, youth gatherings, and internet shops, among others.

4- Axis IV: Educating the public and individuals about the dangers of electronic terrorism crimes, clarifying and clarifying the ways and means of extremist or terrorist groups to solicit individuals and pushing them to engage in the clutches

of this crime, as well as publishing the names of suspicious websites and warning individuals against dealing with them or entering such sites.

5- Axis V: Find, equip, and prepare specialized teams to investigate this type of crime, qualify them and train them on modern means to investigate cyber terrorism.

It is necessary to emphasize the need to enhance cooperation and coordination with institutions concerned with crime (such as Interpol) in order to counter all forms of terrorism via the Internet, and to develop mechanisms of cooperation at the criminal level in a way that is compatible with the expansion of the information network instead of the traditional slow and complicated procedures. It also calls for countries to be urged to join international conventions on combating terrorism crimes via the Internet, and to encourage the creation of Arabic federations to tackle this range of crimes, and to work to strengthen preventive security by activating the role of Arabic organizations, departments and governments in confronting terrorist crimes via the Internet, and advocacy To establish a specialized Arabic police to fight terrorism via Internet [38].

Second: The Contemporary Stage of the Crime

This stage begins from the moment the implementation of the material pillar of the crime of cyber terrorism begins or from the moment of seizure of any of its elements or from the moment information is available to the security services that there is planning to commit this type of crime, whether it is in the country in which this group operates on its territory and the target Among these activities is another country or otherwise[39].

This stage is considered an attempt to commit a crime, which the Algerian legislator calls an attempt. Article 30 of the Algerian Penal Code stipulates that: “Every attempt to commit a crime that begins with the commencement of execution or with unambiguous actions that lead directly to its commission is considered the same as the crime itself if it did not stop or fail Its effect is only as a result of circumstances independent of the will of its perpetrator, even if the intended target cannot be reached due to a material circumstance that the perpetrator is ignorant of.

Article 394 bis 7 states that: "The attempt to commit misdemeanors stipulated in this section shall be punished with the penalties prescribed for the misdemeanor itself.".

According to the text of Article 16 bis contained in Law N°. 06-22 dated December 20, 2006 amending and supplementing the code of criminal procedure, the judicial police officer has the power to monitor people against whom there is

one or more justifications for their perpetration of a terrorist crime, and to monitor the destination or transfer of things or funds and proceeds from the commission of this crime, and this jurisdiction remains restricted to the necessity of informing the relevant representative of the republic and not objecting to it. In order for the observation to be correct, there must be sufficient evidence of the observer's carrying out of terrorist acts, and this matter is estimated by the prosecutor, as it must be Its purpose and primary goal Is to uncover terrorist activity.

Article 65 bis 5 states: "If the necessities of investigation are required in the crime in which it was committed, or a preliminary investigation in drug crimes, transnational organized crime, crimes against automated data processing systems, money-laundering or terrorism crimes, or crimes related to the legislation on exchange, as well as corruption crimes, The competent representative of the Republic may authorize the following

-Interception of correspondence made using wire and wireless communication devices.

-Making technical arrangements, without the consent of the concerned parties, to capture, confirm, transmit and record speech uttered in private or secret by one or several persons in private or public places, or to take pictures of one or several persons present in a private place ... ".

So, through this article, the Algerian legislator took the possibility to eavesdrop [40].

Through the Law 04/09 dated 08/08/2009 containing the special rules for the prevention and control of crimes related to information and communication technologies, Official Gazette N°. 47 of 2009, in its second chapter, the law stated provisions for the control of electronic communications, and the seriousness of potential threats and the importance of protected interests were taken into account while developing these rules, where the law stipulated four cases in which the security authorities are allowed to use control over correspondence and electronic communications, including the prevention of acts described as terrorist crimes, sabotage and crimes affecting the security of the state, also in case there was any available information on the possibility of an attack on an information system in a way that threatens the state institutions, the national defense or the public order, and the requirements of investigations and judicial investigations, when it is difficult to reach the result of the interests of ongoing research without resorting to electronic surveillance, and within the framework of implementing mutual international judicial assistance requests[41].

Third: The Post-Crime Stage

This stage begins after the perpetrator or the perpetrators are trialed, and the punishment imposed on them is carried out, because the activity of the extremist terrorist groups does not end with the punishment of the elements affiliated with them, as is the case in ordinary crimes, but these perpetrators may take advantage of their presence in prisons to promote their extremist or terrorist ideas, which leads to invite some prisoners to join these groups, after the time for carrying out the punishment has ended. In addition, the security services must take into consideration a set of measures at this stage, including[42]:

-Imposing strict censorship on perpetrators convicted of cyber terrorism crimes while they are in prisons.

-Monitor, follow-up and control the visitors of those convicted of electronic terrorism crimes.

-Exchange the cooperation with neighboring countries, by sharing with them the necessary information about these groups.

Conclusion:

Because of the technological development that the world is witnessing, no country can be immune from the economic, social, cultural and security effects, therefore it is necessary to spread the information culture among our new generations, and prepare them to be aware of the dangers that the terrorist entities seek to achieve via Internet, we can do that by utilizing the media to clarify the risks of electronic terrorism. It is also necessary to cooperate with other countries and exchange information, especially the bodies concerned with combating electronic terrorism, to counter all threats used by terrorist organizations to strike the stability and interests of states, in addition to the need for states to join the International Treaty against Cyber and Internet Crime.

The Results:

1/Despite the numerous attempts to make a definition of electronic terrorism, these efforts were unsuccessful due to the differences in international interests.

2/There have been many terrorist methods dedicated to threaten and destroy information networks and electronic systems.

3/There are many reasons to confirm electronic terrorism crimes, including the fact that they need high technical expertise.

4 / Many countries are seeking to counter cyber terrorism, but these efforts need more development and international coordination.

Suggestions and propositions: Based on what was presented in this article, we present and propose the following suggestions:

1 /Focusing on developing awareness of information culture, information security, and familiarity with the dangers of the digital revolution.
2 /Working to develop and raise the level public awareness that the phenomenon of electronic terrorism is not a problem of the state or the country alone, but rather the problem is for all ,that means for everyone or any individual in society.
3 /Improving and developing the abilities and capabilities of the security agencies to communicate, exchange information and pass it through the joint committees between the security services.
4/ Preparing databases and information about the phenomenon of electronic terrorism and its perpetrators to planning how we are confronting and fighting this dangerous phenomenon.
5/ Developing legal frameworks which are related with electronic terrorism cases to prosecute the perpetrators of these dangerous crimes.
6 / Coordination ,insertion and exchange the informations and experiences between agencies that are concerned to combating terrorism via the Internet in all countries in the world.
7 /Signing international accords, treaties and agreements which are related to electronic terrorism for facilitate the process of extradition, follow-up, and prosecution of criminals.

Bibliography:

[1]- *Rashid Muhammad Al-Marri,* ***Cybercrime in the Shadow of Contemporary Criminal Thought: A Comparative, Analytical, Comparative Study****, PhD thesis, Faculty of Law, Cairo University, Egypt, 2013, P14.*

[2] - *Khaldoun Aisha,* ***"The Special Nature and Forms of Cybercrime"****, Journal of Studies and Research, Ninth Issue, Ziyan Ashour University of Djelfa, Algeria; 2012, P 114.*

[3] - *Aimour Radia,* ***"Cybercrime"****, Law and Political Science, Sixth Issue, Ammar Thaligi University of Laghouat ,Algeria; 2011, P 96.*

[4] - *Ali Jabbar Al-Hussainawi,****Computer and internet crimes****, Al-Yazouri Scientific Publishing and Distribution House, Amman; 2009, P 33.*

[5] - *Sawyer Sufyan,* ***Information crimes****,Master Thesis, Faculty of Law and Political Science, Abu Bakr Belkaid University of Tlemcen, Algeria, 2011, P16.*

[6] - *Maatouq Abdel-Latif,* ***The legal framework for combating information crimes in Algerian and comparative legislation****, Master Thesis, Faculty of Law and Political Science, Hajj Lakhdar University of Batna, Algeria,2012, P128*

[7] - *Rabeh Wahiba****, "Information Crime in Algerian Procedural Legislation"****, Researcher Journal for Academic Studies. The fourth issue, Hajj Lakhdar Batna University, Algeria; 2012, P 322.*

[8] - *Mahmoud Ahmed Ababneh,* ***Computer crimes and their international dimensions****, The House of Culture for Publishing and Distribution, Amman; 2004, P36.*

[9] - *Sawyer Sufyan, op Cit,P20.*

[10] - *Aimur Radhia, op Cit, p97.*

[11] - Khaldoun Aisha, op Cit, P114.

[12] - Siham Muhammad al-Hajj Ali al-Sarabi, **"Causes of Terrorism Violence and Extremism"**, Journal of Studies and Research, Fourth Issue, Ziyan Ashour University of Djelfa, Algeria; 2009, P 10.

[13] - Mustafa Muhammad Musa, **Electronic Terrorism**, The Egyptian National Book and Documentation House Cairo; 2009, P93.

[14] - Raed Al-Adwan, **"International Treatment of cyber Terrorism"**, Intervention within the scientific forum employing social networks in combating terrorism, Naif Arab University for Security Sciences, Riyadh, 16-17 February 2013, P8.

[15] - Acer Mohamed Attia, **"The role of Modern Mechanisms to reduce emerging Crimes - Cyber Terrorism and Ways to Combat it"** Intervention within the scientific forum, new crimes in light of regional and international changes and changes. College of Strategic Sciences, Amman, Jordan, 2-4 September 2014,P9.

[16] - Wagih El-Desouky El-Morsy, **"Modern Electronic Methods used by Terrorist organizations in Terrorist Crimes"** Intervention within the scientific symposium the role of civil society institutions in countering terrorism, Studies and Research Center, Naif Arab University for Security Sciences, Riyadh, 26-28 August 2014.

[17] - Hassan Turki Omair, and Salam Jassem Abdullah, **"Electronic Terrorism and its dangers in the Current Era"**, Journal of Legal and Political Sciences, special issue, Diyala University, Iraq; 2014, P328.

[18] - Matouq Abd al-Latif, op Cit, P79.

[19] - Baker, David Mc. A, The Effects of Terrorism on the Travel and Tourism Industry, en ligne: https://arrow. Tudublin.ie/ijrtp/Vol 2/Iss1/9.(Date of review:01/02/2020).

[20] - Musa Masoud Arhum, **"Terrorism and the Internet"**, Journal of Studies and Research, Fourth Issue, Ziyan Ashour University of Djelfa, Algeria; 2011, P168.

[21] - Saghir Youssef, **Internet Crime**, Master of International Business Law, Faculty of Law and Political Science, Tizi-Ouzou University, Algeria, 2013, P55.

[22] - Wajih El-Desouky El-Morsy, op Cit, P145.

[23] - Musa Masoud Arhum, op Cit, PP169-170.

[24] - Acer Mohamed Attia, op Cit, P15.

[25] - Gabriel Weimann,Terror on the Internet: The New Arena, the New Challenges, by washington, dc: united states institute of peace press, 2006, P12.

[26] - Ibid. P13.

[27] - Abdul Rahman Bin Abdullah Al-Sanad, **The means of electronic terrorism - its rule in Islam and ways to combat it**, en ligne: www.hamelte elssakina.com. Date of publication: 04/05/2012. Date of review: 01/02/2020.

[28] - Hassan Turki Omair and Salam Jassim Abdullah, op Cit, P331.

[29] - Gabriel Weimann, op Cit, P15.

[30] - Abdul Rahman Bin Abdullah Al-Sanad, op Cit, PP10-11.

[31] - Musa Masoud Arhum, , op Cit, P176.

[32] - Tahseen Muhammad Anis Sharadqa, **"The role of the media in combating terrorism and extremism"**,Intervention within the international conference the role of Sharia, law and information in combating terrorism. Zarqa University, Jordan; 30 and 31 March 2016, P3.

[33] - *Mohamed Mohamed Al-Alfy,* ***"Electronic and virtual terrorism legislation"*** *Intervention within the first judicial forum, crimes of terrorism and state security, College of training. Naif University for Security Sciences, Riyadh; June 28-30, 2010, P23.*

[34] - *Abdul Rahman Bin Abdullah Al-Sanad, op Cit, P14.*

[35] - *Surah Yusuf, verse 33.*

[36] - *Saad Atwa Al-Zant,* ***"Cyber terrorism and paraphrasing national security strategies"****, Intervention in the emerging crime conference - how to prove and confront it. National Center for Social and Criminal Research, Cairo; December 15 and 16, 2010, P 8.*

[37] - *Acer Mohamed Attia, p Cit, PP28-29.*

[38] - *Musa Masoud Arhum, op Cit,P181.*

[39] - *Acer Mohamed Attia, op Cit, P30.*

[40] - *Sagheer Yusef, op Cit, P81.*

[41] - *Ibid , P113.*

[42] - *Baker, David Mc. A, op Cit.*