Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.79, 2018

The Legal Structure of the Electronic Terrorism Crime in the Jordanian Penal Legislation

Dr. Ibtisam Saleh
Assistant Professor Amman Arab University, Jordan

Abstract
This study investigates the Jordanian legislator's prevention of the electronic terrorism crime which is considered most dangerous amongst terrorism types at present. This is due to the wide usage of modern technology around the world and to the huge loss that might be caused by a successful operation that takes place under its concept.In order to meet the study objectives, it is quite crucial to look first into the general concepts and the electronic terrorism ones. Second , we have explained the several sorts of electronic terrorism represented in spreading and exchanging data throughout the Internet, creating electronic websites, destroying websites and damaging data and information systems. Third, we have moved to the Jordanian legislator's processing manner in preventing electronic terrorism crimes in which we have clarified the limits of applying the legal texts that spoke about general terrorism in the Penal Code if it is done electronically. After that, we have made it clear that the cybercrime law did not mention terrorism because there is a text in The Terrorism Prevention Act that accuses these texts, as it was considered the same as the terrorism acts in the strict terrorism prevention act. This is the reason why it has criminalized using the information system, internet or any other publishing means to publish, inform or create electronic websites to facilitate terrorism acts or to support a terrorism community, organization or association in promoting its ideas or financing them.
Keywords: Electronic Terrorism, Electronic Websites, Information Systems, financing terrorism.

1. Introduction

After the huge uprise which has been brought by the technological civilization in the information age, the concept of electronic terrorism has appeared. The criminal use of modern information technology has increased and threatened the safety of countries and governments. Accordingly, threatening, horrifying , spreading terrorism notions, and exchanging extremism and terrorism data has prospered throughout modern technology means. This has widened with the development of calculators, internet and social media. Terrorists create and design their own websites on the world wide web in order to spread out their ideas and principles, implant their notions, recruit new terrorists, give instructions, electronic instructing and electronic training on helpful methods in terrorist attacks. Using the Internet has made it really simple for terrorists and criminals to meet and exchange opinions and ideas.

After 11 September attacks, the connection between the Internet and terrorism has come clearly into sight. Facing terrorism has become more electronic than concrete, real wars also turned to be digital, and the Internet is now one of the most dangerous weapons that is used to achieve offensive terrorist objectives. This has called 30 countries to sign the first international Convection on Cybercrime in the Hungarian capital, Budapest, in 2001. The cybercrime has become an unpleasant situation that frightens the world by threatening it with terrorist attacks and poisoned notions throughout modern technology. Moreover, technological development does not stop, which complicates fighting these warlike operations which use development as a means to get to its goals. Terrorism and the Internet are connected in two ways. First, the Internet has become a platform for communities and individuals to spread out their hatred and a connection amongst them and with their adherents. Second, terrorism is applying sabotage acts in internet and computer networks.

In spite of the Jordanian legislator's standing against electronic terrorism in The Terrorism Prevention Act, the legal text has ignored many criminal behaviors the connected to terrorism. Thus, widening the conviction related to electronic terrorism is now a must to involve all illegal terrorist behaviors.

2. Electronic Terrorism Definition

Defining electronic terrorism stems from defining terrorism in general , and it is no different but in the tool used to achieve the terrorist goal, as electronic terrorism uses information, social media and internet to frighten, hurt and threaten people.

In retrospect to the Jordanian legislator's plan in dealing with cybercrime, we find that it has defined terrorism in Article 2 in The Terrorism Prevention Act and its justification, number 55 for Year 2006 as: "every intentional act meant to threaten, whatever its motivations, means, or objectives were, which is committed to some criminal aim , either individual or collective, that might threaten the society's safety or start a disorder. This might also ruin public order, frighten people, put their lives in danger, destroy environment, damage public, private and international facilities, ruin diplomatic delegations, illegally occupy these facilities, put national and economic resources in danger, force any national or regional organization to do any work or not to do it, and

block the application of the Constitution, laws and legislations". This definition is similar to public terrorism in Article 147/1 in the Penal Code, and it is not that much different.

Considering electronic terrorism, even though the cancelled information system code of 2010 prohibited it in Article 10, The Cybercrime Law has mentioned nothing about electronic terrorism. This is due to Article 3 in The Terrorism Prevention Act, which has said: "Considering the rules of The Penal Code or any other law, the following acts are considered prohibited terrorism: using the information system, the Internet, any publishing means or designing electronic websites to facilitate terrorism or support or finance some community, organization or association that adopts terrorism or spread out its notions". Thus, the legislator has incriminated electronic terrorism and considered it a similar crime, yet it has not defined it clearly.

Because electronic terrorism has newly appeared, its definitions are many. Some have defined it as: "the concrete or abstract aggression, frightening or threatening to use electronic means by countries, communities or individuals against man in his religion, race, mind or money with no right in different sorts and images of corruption"[1]. Others have defined it as: "illegal attacks or threats to attack electronic calculators, networks or data done to revenge, blackmail, force or affect governments, peoples or international communities in order to achieve political, religious or social goals"[2]. Therefore, electronic terrorism is the electronic attack at information systems, modern computer techniques justified by several reasons in order to damage the infrastructure to frighten, horrify and conquer other humans.

Terrorism springs from different motives. It aims at achieving specific goals, but electronic terrorism is remarkable because of modern methods represented in using information resources and technical means in the information age, so electronic systems and infrastructures are the objective of such terrorists.

Electronic terrorism refers to two elements, which are cyber space and terrorism, in addition to the virtual world which is the place where computers, programs and internet work and data move. Because countries have organized information technology through satellites and international networks, the criminal risk for communities and individuals has increased. They have used the information technology in destroying the informational infrastructure that the governments and huge economic companies are depending on. Based on that, electronic terrorism is dangerous in that the networks are easily used by anonymous users, at their houses, offices or cafes, safe and away from authorities, especially in developed countries whose infrastructure is managed by technology and networks.[3]

3. Electronic Terrorism

It is not easy to specify electronic terrorism sorts as their nature needs unlimited categorization due to the usage of progressive developing technology.

3.1 .Spreading out and Exchanging Terrorist Data through the Internet

The Internet has facilitated the terrorists' meeting and notion exchanging, considering the possibility of several people from different places meeting at a specific time to talk and listen to each other on the internet. They actually can also spread their notions and principles on electronic websites and chat rooms. Hence, they are more likely to attract new members, a matter not easy to achieve without a data network. The email is considered the most important service that the Internet provides since the user can send electronic messages to an Internet user or even users. This allows the exchanging of messages and data with others of Internet users. The email is remarkable for being quick in delivering messages and easy to use wherever the receiver is. That is exactly why it is the main electronic terrorism method. Recently, many terrorist operations have depended on the email as a successful means to exchange data between planners and supervisors.[4]

The Internet is helpful for the terrorism communities in connecting and coordinating with each other because, first, it is not expensive compared to other methods. Second, it has a wide variety of sorts of exchanged data as it is an electronic encyclopedia enriched by data attracting terrorists to grasp such matters as nuclear construction locations, generating power resources, international flight schedules, data related to procedures of terrorism preventing, command and control locations and a lot of other detailed data supported by scanned copies. All of the above combined have helped to perfectly coordinate and plan terrorist operations.[5]

For instance, Google Earth made it easy for the Pakistani Lashkar-e-Taiba terrorist community to plan for Mumbai attacks in 2008. In 2007, some American soldiers took photos at an Iraqi military base, where in the background appeared some helicopters, which they then uploaded to the Internet. The photos were no help to give the plane types or any sort of data to the terrorists, but some of them were able to use the Geotags from the

[1] "*The Bishop*" Ali Adnan (2011). Cyber crime. Beirut, Lebanon: Zain Legal publications, p. 59.
[2] Ahmad, Tariq Afifi Sadeq (2015). The Cybercrimes, Cairo, Egypt: The National Center for Legal Pu blications, p. 185.
[3] "*The Little*", Jameel Abdul Baqi (2008, 15-19 November). How much the Penal code and criminal procedure are enough to face the cybercrime. Internet and Terrorism Conference, Cairo, Egypt, p. 6.
[4] Ibrahim, Khaled Mamdouh (2008), *Email as a Great Proof*, Cairo, Egypt, Dar Alfikr Alarabi, p. 19.
[5] "*The Bishop*", previous reference, pp. 81-82.

photos in order to locate the military base, and they finally succeeded in damaging four of them with mortar shells.[1]

Furthermore, the Internet with its services is also used in electronic terrorism training away from the police sight as terrorist camps can be easily discovered and raided. Some terrorist communities have produced guides for terrorist operations including the means to train, plan, implement and hide. These guides can be sent easily over the Internet to the terrorists all over the world , not to mention that several websites have instructions to build bombs, explosives, incendiary and destructive weapons.

Moreover, terrorist communities use the Internet in spreading out the data on websites, emails or chat rooms. TV channels that race to get these terrorist data have also helped with publishing them over media, which have doubled the access to the different society layers.[2] Another thing which terrorists use the Internet for is getting funds; they use the statistical population private information of Internet users which they upload as answers to the surveys and questionnaires. After that, they get to know those of merciful hearts and try to convince them to donate for some people who are actually a fake interface for terrorists. This is all done in a cunning way so that the donor does not doubt that he is financing one of the terrorist communities.[3]

3.2 Structuring the Electronic Websites

Since the Internet is an accelerating developing world, opinions about the electronic terrorism have changed. After being limited in a concrete damaging procedure, it now involves more dangerous activities represented, as one researcher noted, in the terrorist communities' daily usage of the Internet for planning and coordinating their operations around the world. The terrorist existence is widespread all around the world. A terrorist website that appears today will quickly change its electronic type and disappear to appear again in a new mood and new electronic address after a short while. The websites for these communities do not only address their agents and sponsors; they also address the media and the audience of the communities that they frighten and horrify. Their aim is to attack enemy states by broadcasting horrifying films for hostages during their execution. At the same time, the terrorists claim that they hold a noble case and complain from the bad treatment which they receive.[4] Thus, terrorists construct their websites on the web to spread out their notions and principles and call for finding new terrorists, and to practice electronic training on helpful methods and ways in terrorist attacks as some websites have been constructed to teach making bombs, explosives and chemical fatal weapons, or to teach email breakthrough, destroying electronic websites, logging into blocked websites and how to release viruses.[5]

The Website is defined as a central site that includes a number of web pages that can be reached easily from the homepage. While the web page is a file written in the programming language HTML, it may include texts, photos and links for other web pages and can be reached from a web browser by typing its address. The website is usually created by the online companies, governments or individuals. In 2015, the Jordanian Cybercrime Law Number 27 has defined the website as "an area that makes the data available on the web by using a specific address".

Amaq website is the official website for ISIS (Islamic State of Iraq and Syria), which was created in 2014. Dabiq is also a website which is the official weekly journal for ISIS. The first publication was released in July 2014.A report by Jeff Bearden, the security expert, has revealed that the terrorist ISIS has 90 thousand Arabic pages on Face book, and 40 thousand pages in other languages, and the website ISIS opened in 7 languages. This community blackmails the youth financially and emotionally to enroll them to it and especially targets the minor female Muslims. Jeff also noted that 3400 members are joining ISIS monthly due to the enrolment electronic campaigns.[6]

3.3 Destroying Websites, Data and Information Systems

These are campaigns that target the Internet and computer networks, whether they are military, economic or security. They threaten the national safety and the military and economic security of one or more countries. The campaigns aim is to destroy electronic data , websites, and information systems and to damage the infrastructure. For instance, it is possible to breakthrough a hospital website and threaten the patients' lives by manipulating cure systems, threatening the international economy by a breakthrough in the connections of national airports and disruption of flight schedules and thus cause a mess between passengers and navigators and more importantly to break through the security system of a country and paralyze it for the good of the terrorist

[1] http://political-encyclopedia.org/
[2] "*Al-Ajeelan*" Abdullah Bin Abdul Aziz Bin Fahed (2008). Electronic Terrorism in Information Age. Events of Information Security and Privacy conference in the cyber law, Cairo, Egypt, p. 15.
[3] "*The Little*" , previous reference, p. 6.
[4] Dadra Houimel (2013). *Terrorism in the Electronic Space*: Comparative Study. Unpublished PhD thesis, Amman Arab University , Amman, Jordan, p. 100.
[5] Jafar Ali (2013) *The Modern Information Technology Crimes on People and Governments*, Beirut, Lebanon. Zain Legal and Literary Library, p. 610.
[6] https://ar.wikipedia.org/wi/

community.[1]

The main reasons that lead to website damaging are:[2]

- Using numbers and words by Internet users that are easy to memorize, which facilitates the breakthrough operation.
- Not updating the operating system continuously which might have some security bugs that should be fixed using some files which the producing company releases.
- Not using enough security programs to prevent the breakthrough or destruction, or not updating these programs even after the warning of a breakthrough case.

There is no applicable technical or organizational method to stop website damaging or breakthrough permanently. This is due to technical variables and the breaker's knowledge of the application gaps which were all designed on the basis of open-source design on the level of the connection point-components, systems, network or programming. In addition, there are some terrorist communities that are responsible for website damaging. The breakthrough happens by leaking out main data and Internet related special symbols, which is a process that may take place at any location around the world with no need for the breaker to be in the same country.[3]

The terrorist communities aim towards the breakthrough of military targets related to the Internet. This kind is rare as it requires precise knowledge about the target and the data wanted; this knowledge is not available but to governments. Governments also restrict procedures to keep this data private and safe. They do not connect the devices with such data to the outside world unless it was exposed to inner corruption. It is imagined to destroy the economic data systems. Considering its interconnection and openness to the world, they make an attractive aim for terrorists and hackers. Undoubtedly, there are huge damages resulting from the breakthrough to the economic data systems, in addition to its effect on weakening the economic system. Thus, terrorist communities might electronically attack the banks through the Internet in order to transfer money to the terrorist community to finance their terrorist activities. They might also breakthrough the electrical power systems, especially in developed countries that depend on the network in managing electrical power systems. This electronic terrorist attack leads to dangerous consequences especially with the modern mankind dependence on electrical power.

4. The Jordanian's Legislator Attitude towards The Electronic Terrorism Crime

4.1. The Extent of Traditional Terrorism Actualization by Electronic Means according to the Jordanian Penal Code

The elements that electronic terrorism consists of are not that far from those of general terrorism; the difference is merely in methods. These elements are derived from Article 2 of The Terrorist Prevention Act, and they are represented in:

First: Using Violence or Threatening of Using It

Our Jordanian legislator has adopted violence and strength as a pillar to define terrorism in Article 1/147 of The Penal Code and the Article above. This explains why using violence or threatening of using it is the main clear image of terrorism as both strength and violence are the means that terrorist communities have widely used in their crimes since they are considered a supporting way of the physical criminal behavior and thus they are listed under terrorism.

Violence is every physical behavior that begins a physical event like hitting or wounding somebody; it also involves damaging and destroying acts. Violence or threatening of using it must be up to some level of danger which might be achieved either by a weapon or other means.[4] While threatening is raising fear with others from injury or evil, no matter it comes from saying, writing, drawing, movement or gestures; there is no condition for it to be in actions, threatening itself is enough to cause fear and panic since it is the clear image of terrorism even if it is not accompanied by strength or violence.[5]

Eventually, an innovative abstract definition of violence, meant in the above two traditional definitions, can be pictured. This means to look at violence as a result of an abstract behavior in which you can picture an obvious abstract violence in the doer's ability to use the systems of information technology in order to inflect the intended harm. While threatening of violence can be imagined in an electronic environment. [6]

Second: Using Violence or Threatening of Using it as Committed by Individuals or Communities

Terrorist acts need time to plan and deliberate before committing them. Terrorist acts are no coincidence; they

[1] https://www.ita.gov.oml/ITAPORTal_AR/Pages.aspx/

[2] "*The Prop*", Abdul Rahman Bin Abdullah (2004), Methods of Electronic Terrorism and How to Prevent It in Islam, events of Islam Attitude Towards Terrorism, The Kingdom Saudi Arabia, Rayed, p.7.

[3] "*The Bishop*", previous reference, p. 86.

[4] "*Al-Nawayseh*" Abdul Ilah Muhammad (2010). *The Crimes against State Security in the Jordanian Legislation.* Amman, Jordan, Wa'el Publishing House, p. 258.

[5] "*Ali*" Fadel Shayea' (2016) financing *of Terrorism by Money-Laundering*. Beirut, Lebanon, Al-Sanhouri Publishing House, p. 58.

[6] "*Al- Manae'sa*" Osama Ahmad Zoubie, Jalal Muhammad (2014). Crimes of Information Technology's Systems, Amman, Jordan. The Culture Publishing House, P. 232.

are crimes planned by either an individual or by a community, which means a number of individuals.[1]

Third: Violence or threatening of using it should be able to scare people, horrify them, endanger their lives and safety, harm the environment, damage public facilities, properties, diplomatic delegations, and national properties or occupy or capture any of them, endanger national resources or finally disabling the application of provisions or laws of the Constitution. This terrorist element might happen as a result of the culprit manipulation with the electrical and water pumping systems, their averages, quality, or distribution by using the information technology systems.[2]

Fourth: Using planned violence or threatening of using it should be aimed to corrupt public order or endanger the society's safety and security, which is exactly the aim of terrorism, and it is no condition of the harm to be accomplished , but it is enough to be possible such as the culprit's manipulating traffic lights management and operating systems, the culprit's breakthrough of gas pumping systems between the countries' lively institutions and threatening of changing the pressure degrees. [3]

As a result, any electronic operation or threatening of it that can endanger the society's safety and security or corrupt the public order, either it happened or threatened with, individually or collectively, is enlisted under traditional articles discussing terrorism in the Penal Code.

4.2. Electronic Terrorism in the Jordanian Terrorism Prevention Act

Article 3 in The Terrorism Prevention Act has stated that: "considering the Penal Code or any other law, the following actions are considered forbidden terrorism: using the information system, information networks or any other publishing means or creating websites in order to facilitate terrorism, supporting terrorist acts, supporting a terrorist community, association or organization, promoting their notions or financing such parties".

Reading the above lines, we find that the Jordanian legislator has incriminated using the information system, information networks or creating websites in order to facilitate terrorism support a terrorist community or promote or finance its notions.

About facilitating terrorist acts, it is achieved by any activity which the culprit does to pave the ground for some terrorist operation which needs a positive attitude from the culprit through the information system or the networks in order to facilitate terrorist acts such as spreading out how to manufacture terrorist's special devices of explosives, incendiaries and other tools. The crime might happen by creating a website of any nickname to help operating terrorist acts even if nothing happened after that. Yet, it is difficult to highlight this intention if creating the website did not result in any afterward activity. About supporting the organization, association or the community that does some terrorist activities using the information system, the information networks or creating a website can be achieved by all supporting means, whether materialistic or abstract. Promotion is actually spreading out positive notions about terrorist parties to encourage others to support or join them.[4]

The State Security Court, which is the juridical party concerned with looking into the crimes mentioned in The Terrorism Prevention Act, has been directed to emphasize the sentences in the cases related to ISIS and Al-Nusra Front up to a sentence of 10 years with hard labor for anyone who promotes or supports their notions. The court's increasing of the sentence has come in a legal systematic outline that aims at fighting terrorism and extremism as Jordan is working to get rid of them. In one sentence it has said: " the activities that the accused person has done are represented in his being a member of ISIS and being in several terrorist communities through the information network, social media and promoting them by publishing the combat operations in the Syrian and Iraqi fields and publishing pictures of victims. He also confessed of the nature of the operations which this party does, which, after applying all basic elements of the law, has been revealed to be a crime of using the information network to spread out terrorist notions contrary to Articles 3/5/7/c of The Terrorism Prevention Act.[5]

In a later decision it has said: "The culprit, one of the Islamic extremists, has joined several groups on the information network especially the Face book, and has promoted ISIS' notions in order to attract the highest number of addressees for joining this terrorist community that targets Jordan, its safety security, which after applying all basic elements of the law has been revealed to be a crime of using the information network to spread out terrorist notions contrary to Articles 3/hw 7/c of The Terrorism Prevention Act"[6]

The third image for electronic assistance to terrorist communities which Article 3/h has discussed is represented in using the information system, information network or creating a website for financing a terrorist community, association or organization. The incriminated act in this image is represented in financing any

[1] "*Al-Nawayseh*", previous reference, p. 259.
[2] "*Al- Manae'sa*", Zoubie, previous reference, p. 324.
[3] " *Kate 'a*" Ghassan Sabri (2011). The Arabic Efforts in Terrorism Prevention, Amman, Jordan. The Culture Publishing House, p. 87.
[4] "*Al*-Nawayseh" Abdul Ilah Muhammad (2017). Information Technology Crimes, Amman, Jordan, Wae'l Publishing House, p. 378.
[5] *Court of Cassation*, criminal number 377/2015. Justice publications, 23/7/2015.
[6] *Court of Cassation*, criminal number 15/2016. Justice publications, 10/2/2016.

terrorist community using information technology.

The Terrorist Prevention Act has not defined the concept of "financing terrorism" because Money Laundering and Financing of Terrorism Law in 2006 defined financing terrorism as: "doing any activity of those mentioned in Paragraph B of Article 3". Article 3 has defined financing terrorism as money providing, collecting, and direct or indirect transferring ,whether money was from known legal resources to a terrorist organization, association, agency, community to terrorist acts, either it was used fully, partially or was not used at all and either the terrorist activities were accomplished or not. The National Agreement for Preventing Financing Terrorism (1999) defined it as a crime accomplished whenever a person ,either directly or indirectly, illegally or intentionally, provides or collects money in order to use it fully or partially in a terrorist activity. Article 1 of the same agreement has clarified that money is anything with an abstract or material value, either transferred, estate, legal documents or tools in its several forms, in addition to electronic and digital support, bank credit operations, travel checks, bank checks, bills, shares, stocks, securities, and letters of credit.

Therefore, financing terrorism can be achieved by any financial support whatever its form is. This financing is given to individuals or organizations that support terrorism or plan for terrorist operations. It might be from legitimate sources such as charitable, social or cultural associations or from illegal sources like drug dealing, weapons trade or money laundering. The reasons behind terrorism are a many. However, the main reason causing the terrorist action, facilitating recruitment of terrorists, buying weapons and distributing them in terrorist operations and sheltering terrorists is the financing that terrorist communities get.[1]

Every user of the information system or information network or maker of a website for financing terrorist parties is responsible for his actions according to Article 3 of The Terrorism Prevention Act.

It must be noted that Article 3/a of The Terrorism Prevention Act considers financing terrorism as an independent crime, not only a participation in the crime. Thus, the crime happens no matter if the terrorist act happens or not as it is enlisted under the forbidden terrorist acts in Article 3/a: directly or indirectly, providing or collecting money in order to serve terrorist operations given that they are used fully or partially no matter if the terrorist act has been accomplished inside the Kingdom against the citizens or its exterior interests.

It must be mentioned that the Jordanian legislator in Article 147/2 has incriminated doing bank operations especially deposits and transfers, with the condition of being completed by a bank or a financial institution in Jordan and of being related to some terrorist act. That is why undertaking any internal or external electronic bank operation related to depositing money in some bank from financial institutions that run financial activities such as exchange operations is included in the incriminating text, in addition to undertaking any electronic transfer provided that that money is suspected to be related to terrorist acts. The Jordanian legislator has given the general prosecutor the power to provisional seizure of the suspected money thought to be related to some terrorist activity. He also gave the right to the accused person to challenge the results that are sentenced against him in the State Security Court, which must decide on this challenge within a week.

The Jordanian legislator in Article 3/e from The Terrorism Prevention Act has not put conditions on criminal results, which means that the moment the culprit uses the information system or the Internet or creates a website in order to help terror, the crime is committed even if the help fails, but it is a must to have the general criminal intention which includes knowledge and will. Knowledge is supposed to cover all helping crime elements and willing to do the action of the crime. It also includes the specific criminal intention, which is represented in the intention to facilitate the terrorist acts or finance and support the terrorist parties. The doer of these acts is sentenced with temporary hard labor from three years up to fifteen years, according to Article 7/b of The Terrorism Prevention Act.[2]

This was affirmed by the Court of Cassation in a recent decision: "Considering the actions of the suspect represented in following ISIS news and publications through the Internet until he agreed over their notions, and then he started posting these news and publications to his acquaintances and friends in the university on social media wishing to attract more supporters to this terrorist community, if the suspect was with his own conscious free will doing so, this is considered promoting a terrorist community"[3].

However, the legal text is criticized for ignoring other criminal behaviors connected with terrorist crimes which are no less dangerous than the criminal acts which it has incriminated like creating a website or using informational systems or informational network to train on terrorist acts and operations and explosives manufacture, or to achieve permanent connections between terrorist communities and organizations.

5. Conclusion

The technological revolution in the information age has released the widespread use of the term "cyber terrorism" and the increased the risk of terrorist crimes both in terms of facilitating the connection between terrorist communities and coordinating their operations and in helping to create advanced criminal methods.

[1] "*Ali*", previous reference, p. 160.
[2] "Al-Nawayseh" , previous reference, page 390.
[3] *Court of Cassation*, criminal number 201/350. Justice publications,1/2/2018.

Through this study, we have found out the following results:

1- Electronic terrorism depends on the use of scientific and technical capabilities and the exploitation of communicative means and information networks in order to frighten, horrify, harm, or threaten others.

2- The physical element types and forms in traditional terrorist crimes mentioned in Article 147 in The Penal Code may be achieved with the usage of information technology, and in each case the operation is connected to a reliable electronic domain, provided that sufficient threatening violence is used to implement an individual or collective operation, provided that this threatening violence can cause terror among people or endanger their lives.

3- The Jordanian legislator has incriminated the provision of electronic assistance means to terrorist communities in The Terrorism Prevention Act and defined them by electronic facilitating of terrorist actions, supporting terrorist communities or electronic promotion, and electronic financing for terrorist communities. These means are separate from terrorist acts. There is no requirement for a terrorist crime to occur as a result of assistance or for the sponsor to be a member in the group or terrorist organization.

6. Recommendations

- We hope that our Jordanian legislator would modify Article 3 / e of The Terrorism Prevention Act and add the following paragraphs: He is punished with (the punishment is left to the legislator):

1. Anyone who has created a website or published information on the Internet or an information technology device, provided that the data is related to a terrorist community even under or nickname and the purpose of construction is to be spreading data, assist and facilitate the communication of the leadership with other members or to spread out their notions.
2. Anyone who uses information technology or information network or create a website for training on terrorist acts and operations, teaching how to manufacture incendiary or explosive devices or any tools used in terrorist acts, or developing perceptions of how to plan or implement terrorist operations.
3. Anyone who uses information technology or information network or create a website to finance and collect funds for a terrorist organization, association, or community.
4. Anyone who creates a website used to serve a website.

7. References:

- "The Bishop" Ali Adnan (2011).Cybercrime. Beirut, Lebanon: Zain Legal publications.
- Ahmad, Tariq Afifi Sadeq (2015). The Cybercrimes, Cairo, Egypt: The National Center for Legal Publications.
- "Al- Kafi" Mustafa Yousef, Al-Shamayleh, Maher Odeh, Al-Lahham, Mahmoud Ezzat (2015) *Electronic Terrorism and Media,* Amman, Jordan, the Scientist Hurricane Publishing House.
- Ibrahim, Khaled Mamdouh (2008), *Email as a Great Proof*, Cairo, Egypt, Dar Alfikr Alarabi.
- "*Ali*" Fadel Shayea' (2016) financing of Terrorism by Money-Laundering.Beirut, Lebanon, Al-Sanhouri Publishing House.
- "Al- Manae'sa" Osama Ahmad Zoubie, Jalal Muhammad (2014).*Crimes of Information Technology's Systems, Amman, Jordan.* The Culture Publishing House
- Jafar Ali (2013) *The Modern Information Technology Crimes on People and Governments*, Beirut, Lebanon. Zain Legal and Literary Library
- "Al-Nawayseh" Abdul Ilah Muhammad (2010). *The Crimes Committed against State Security in the Jordanian Legislation*, Amman, Jordan, Wae'l Publishing House.
- "Al-Nawayseh" Abdul Ilah Muhammad (2017).*Information Technology Crimes,* Amman, Jordan, Wae'l Publishing House, p. 378.

-Kate'a" Ghassan Sabri (2011). *The Arabic Efforts in Terrorism Prevention,* Amman, Jordan.The Culture Publishing House.

- "The Little", Jameel Abdul Baqi (2008, 15-19 November). *How much the Penal Code and criminal procedure are enough to face the cybercrime*. Internet and Terrorism Conference, Cairo, Egypt.

"Al-Ajeelan" Abdullah Ibn Abdul Aziz Ibn Fahed (2008). *Electronic Terrorism in Information Age*. Events of Information Security and Privacy conference in the cyber law, Cairo, Egypt

"The Prop", Abdul Rahman Ibn Abdullah (2004), *Methods of Electronic Terrorism and How to Prevent It in Islam,* events of Islam Attitude Towards Terrorism, The Kingdom Saudi Arabia, Riyad.

"Al-Zebn" Dadra Houimel (2013). *Terrorism in the Electronic Space*: Comparative Study. Unpublished PhD thesis, Amman Arab University, Amman, Jordan,

http://political-encyclopedia
https://ar.wikipedia.org/wi
http://mawdoo3.com
https://www.ita.gov.oml/ITAPORTal_AR/Pages.aspx