International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 8, Issue 4, 2019

Innovative Ways to Tackle Cyber Terrorism and the Role of Public and Private Law in Attaining it: A Focus on Causes and Solutions

Ali Jabbar Salih[a], Farouq Ahmad Faleh Alazzam[b], Khaled Khalaf Abed Rabbo Aldrou[c], [a]Dean of the Faculty of Law at Jadara University – Jordan, [b,c]Faculty of Law – Jadara University. Jordan, Email: [a]dr_alijabbar@yahoo.com, [b]farouq.azzam@hotmail.com, [c]Aldrou1970@yahoo.com

This research aims at studying and defining the actual concept of cyber terrorism with explaining its reasons, objectives and the expected scenarios to design suitable means of prevention and to confront them, especially in light of the weakness of the criminal, constitutional, commercial, civil and other relevant laws and legislations. This is due to the rigidity of laws and the lack of keeping pace with developments on the international and domestic scene. This legal vacuum has led to the spread of a serious and contagious pandemic around the world which does not stop, and no single country has been able to stop and control its effects as it has no principle and does not distinguish between young, elderly, race, religion or gender. Cyber Terrorism knows no borders, destroys, kills and exploits anyone who is on its way to attain his ambitions and advantages. Cyber-terrorism is closely linked to the use of the Internet as a high-tech medium and is the direct cause of the increase in cybercrime as it assists it to spread criminal acts, including terrorist attacks against computers, networks, and information stored electronically for revenge, destruction, murder and blackmail to achieve their interests and the terrorist organizations which are spread around the world. And whether their interest is political, economic, religious or social. Cyber Terrorism depends on two major elements: terrorism and cyberspace, which has a great role in increasing this type of crimes making it a real threat to the stability of societies, states and individuals. This research also aims to clarify the reality and the adequacy of laws and legislations in combating cyber terrorism from criminal, civil, commercial and constitutional aspects and stating ways of developing them with reference to the Jordanian situation in this field.

Key words: *Cyber terrorism, cybercrime, cyber hacking, cyber security, cyber-terrorism prevention, cyber-terrorism mechanisms, Internet, Jordanian Laws and Legislations.*

Introduction

Cyber terrorism has a hazardous effect on all societies .It is a kind of crime that has developed along with the development of technology and the Internet, where the committers of these crimes conduct their crimes using the Internet either as a tool to facilitate commission of the crime or to conceal its effects. Criminals also use the internet to communicate between each other and set plans for conducting violent acts that result in threaten, loss of life or significant bodily harm in order to achieve political or ideological gains through threat or intimidation.

Additionally, it is committed against information network platform, social network or any means that depends on technological communication .Terrorist groups benefited from these means throughout spreading their ideas and values on the social networks to reach as many individuals as possible to recruit them and teach them how to penetrate websites illegal.
They also aimed to recruit specialists and to be able to illegally penetrate sensitive networks of countries and disrupting them or sending threatening messages to them to accept their demands.

In other words, cyber-terrorism is a hidden and persistent threat which affects negatively all societies and nations.

But the questions that arises in this research are: is there sufficient legal and legislative protection to handle this type of crime or are they just theories, proposals and conferences that does not have a real definition of the concept of cyber terrorism or explaining its real reasons or seek to develop preventive and therapeutic means to address it?

Are there any parties benefit from the spread of these crimes to achieve hidden interests ? Is it reasonable that there are no modern means in this era to control modern technology and the Internet, taking into account the existence of laws and legislation on cybercrime, which can track all users of the Internet?

For these reasons, researcher used the descriptive analytical methodology to determine the definition and the real causes and objectives of cybercrime and then explain the scope of cyber-terrorism using information via the Internet to obtain facts to suggest solutions to combat cyber-terrorism.

Cyberterrorism: concept, causes, and objectives

Defining the concept of cyberterrorism, its causes and objectives gives a clear picture on deciding the solution. Therefore, the researcher presents different definitions of the cyberterrorism.

The concept of cyberterrorism

terrorism is defined as a pattern of violence that includes the systematic use of murder, threat of use, physical harm, and measure to terrorize or intimidate a target group for the widest range of victims who have been terrorized to create an atmosphere of terror (Shaimi, 2015).
On the other hand, terrorism is defined as an attempt to spread panic and terror for political purposes (Kafi, 2007).In accord to the emergence of modern communication technology means and its use in conducting crimes and terror the concept of cyberterrorism has arisen but allocating a concrete definition to cyberterrorism can be hard, due to the difficulty of defining the term terrorism itself.

According to John Arquilla and David Ronfeldt (2001,) Collin Barry defined cyberterrorism as “The convergence of cyberspace and terrorism”. Mark Poliit (1997), who is a Special Agent for the FBI, defined cyberterrorism as “Intentional, politically motivated attack against information, computer systems, computer programs, and statements of the following targets against violence by anti-national groups or their secret agents” (Ushie Henry Ekpe, 2013, p 38).

Denning defined it as "Information warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary” (Sirohi, 2015, p10).

The Jordanian Prevention of Terrorism Act, Article (No. 3 / E of 2014) defined it as : “the use of the information system or the information network or any means of publication or media or website to facilitate the carrying out of terrorist acts or support for a group or organization that is engaged in terrorist acts or to promote their ideas or funding or to carry out any act that would expose the Jordanians or their property to the risk of acts of hostility or reprisal against them”.

Historically, cyberterrorism first appeared in 2000 CE when the computer virus “I love you “was spread and destroyed information valued at about $ 10 billion. In 2003, a virus called “Blaster” destroyed half a million computers. The United States also linked the attacks of September 11, 2011 with cybercrime attacks, consequently, thirty countries signed the first

international convention to combat information crime in the Hungarian capital Budapest of the same year. The Council of Europe in the International Convention on the fight against cybercrime estimated the cost of repairing the damage caused by computer viruses by about $ 12 billion a year.

In October 2012, the United Nations defined cyber terrorism as "the use of the Internet to spread terrorist acts".

Recently, an American military report accused the Chinese army of being behind pirate networks used in a war. This is evidence that cybercrime poses a major threat to the stability of countries and has risen to the concept of cyber terrorism, which poses a clear threat to national security. Modern societies are operated by computers and the internet which expose it to multiple attacks of "hackers" (Hussein, 2010).

Accordingly, there is no comprehensive and precise definition of cyber terrorism because it is difficult to accurately identify terrorist crimes because of the rapid technological development in all aspects of technology, the internet and the nature of state policies.
The researcher can define cyberterrorism as aggression whether material or moral, using electronic means emanating from States. It can also be defined as, the use of scientific and technical capabilities to exploit the means of communication and information networks in order to intimidate, coerce, harm or threaten others. Therefore, it is considered a cyber-attack on information systems and computers with modern technologies and for multiple reasons such as destroying the infrastructure, intimidation coercion governments and civilians (Saned, 2004).

Finally, Cyber terrorism or digital terrorism is considered another form of terrorism as a result of technological innovations and information revolution and exploitation of internet web to cause offence are damage.

This raises the question. How do terrorist organizations exploit modern means of communication?

This question can be answered as the internet is a two-edged sword.

Recently, many experts have considered the internet the most dangerous weapon of terrorist organizations, a threat to the security and stability of societies. They used it to incite hatred, extremism, violence and murder. Thus, it is the best means on which these organizations use to mobilize and recruit individuals, on the basis that they achieve the goal as quickly and at a lowest cost. This explains the increasing number of those joining them.This is confirmed by the report of the security expert in the issues of digital terrorism, Bardin Jeff that the terrorist

organization DAESH has thousands of Web sites of more than 50 thousand sites, and more than 90 thousand pages in Arabic on the social networking site Facebook and about 40 thousand pages in several foreign languages, and this helped in the recruitment of thousands of young people monthly via its electronic campaigns (Khalil, 2006).

The causes of Cyberterrorism

Cyber terrorism is a complex, comprehensive and multifaceted phenomenon. It uses a variety of mechanisms and elements. Generally, it has the same traditional reasons of any conventional terrorism, but it differs in term of being sophisticated, it can't be traced easily, the terrorist organization employs malicious computer technology rather than kinetic force.
The causes of cyber terrorism vary according to different political, economic, social, religious and ideological differences. It can be said that the causes are intertwined, and the motives are overlapping, so we will identify the general causes of cyber terrorism in the first part, then explain the specific causes of cyber terrorism in part .

General causes of cyber terrorism

The causes of cyber terrorism vary in degree of importance and extent of influence in different international societies depending on the different political trends, economic, social conditions, religious differences, etc. Therefore, what applies to a country or society may not be applied to another society or country. The most important causes are generally considered to be as follows:

a) Intellectual reasons: The intellectual motives leading to terrorism, such as the intellectual emptiness, which leads to intellectual radicalization and religious extremism.

What is meant here is the absence of the human mind and thoughts, which resulted from gaining information from different sources which he analysis and benefits from in acquiring intellectual and constants beliefs whether they are positive or negative. I think that there is still no complete intellectual immunity in a country in the world and this is an important and major cause of terrorism in general and cyber terrorism in particular.
States must be aware of this phenomenon which is extended in all societies and strive to combat it by all ways and means because it is inconceivable that there is a natural person who has intellectual safety and seeks to destroy, kill, harm and sabotage.

b) Political reasons: The motives and political reasons of cyber terrorism are many and varied, the most important of which are the unjust policies of states against citizens and the political pressure applied to them, which leads to the violation of their rights and the lack of social balance among citizens, in addition to political frustration and the marginalization of certain groups. These acts motivate the

establishment of secret organizations and the reactions of anger that leads to revenge through terrorism, which provides them with the appropriate environment to commit their crimes.

According to Ajlan (2008) The lack of social justice, inequality among members of the same society, the disparity in the distribution of services, the neglect of a large part of society in terms of living and humanity, and the lack of counselling, guidance and awareness programs are also an important cause of terrorism. It can be said that the most important reason is the weakness of the international system and local legislation in responding to this type of crime through sanctions and deterrent measures.

c) Personal reasons: There are many personal reasons leading to terrorism, most notably the love of fame, that appears in the appearance of a hero even if the means of fame is destruction and murder, of course this is the result of mental illness suffered by this person. I believe that the numbers of these people are increasingly noticeable. This phenomenon is widespread in society, where most of them speak of their imaginary heroics, which are false championships, but the danger lies in the fact that if they are adopted by terrorist organizations to achieve their personal desires, their psychological illness becomes a reality through murder and sabotage (Bawadi, 2004).

Other reasons which encourages joining the terrorist groups are failure to gain their worth in their families and society, attain fame, mental illness, losing the feeling of belonging to their homeland. All these reasons and justifications for joining the terrorist cells and organizations are considerable, especially if this coincided with failure in scientific and practical life or functional aspects or a failed emotional experience in all aspects of life. In these cases, an individual may resort directly to terrorism as a respond, and because it is the shortest way to make money and fame.

It can be said that all the divine laws call for a human being to be good and harmless to others. It also calls for good morals, tolerance and rejects hatred that leads to killing, vandalism and damage to society.

d) Economic causes: Poverty is a major cause and a strong motive for crime in general and terrorism. Economic problems in some developing countries and the exploitation of economic resources by the influential people and the suffering of individuals from housing, debt, poverty, high cost of living, inflation in prices of food and basic services, lack of individual income. All these factors negatively affect individuals and lead to resorting to terrorism. The widespread unemployment, the lack of job opportunities and the lack of justice in the distribution of employment are among the most important factors contributing to the crime, assault, theft and the spread of terrorism. Undoubtedly, people are driven by hunger, poverty and unemployment.

Additionally, the scientific and technical progress of international banking systems has facilitated the transfer of funds and transfers between countries through the World Wide Web. This has assisted terrorist organizations to exploit the opportunity to achieve their illegal purposes (Elfeel, 2011), especially in the absence of the role of the United Nations to establish clear international cooperation to resolve international economic problems.

e) Social causes: The most important causes of terrorism are the social reasons. Mahmoud (2013) I believed that broken family ties and social disintegration leads to the spread of mental illness, crime and terrorism as a result of the absence of cohesion among the family and community members as the close-knit family cannot be deviated.

It should also be noted that good upbringing is based on ethics and avoiding abuse to others. Moreover, spreading the culture of public interest has a positive role in avoiding persons who have a distorted thought and those who have distinction between religions, societies and countries, consequently, has a positive role in not engaging in terrorist organizations.
We conclude that, most members of terrorist organizations lack family cohesion and good education and love of good. Moreover, all terrorists lack correct religious beliefs and have no ethics, and this is what the world has seen on television and the internet for their actions that are devoid of religion and morality.

Special causes of cyber terrorism

There are many special reasons for cyber terrorism:

- The weakness and the penetrability of information network infrastructure.
  The information networks are originally designed without restrictions or security barriers to facilitate the entry of users. (Saqr, 2007, p120). The electronic systems and information networks contain information gaps that can be used by terrorist organizations to penetrate the infrastructure and conduct terrorist operations.
  Although countries are following up and making changes to attain information security for their agencies, terrorist organizations employ highly experienced and professional mercenaries to work with them to penetrate the information networks and perform other illegal things.
- The lack of clarity of the user digital identity.
  This makes the opportunity appropriate for terrorists, where a computer professional can hide under a fake character and thus launch his cyber-attack away from the control of public authorities. (saghier, 2001, p17).
- The ease of use of the information network and the low cost.

This aspect allowing the terrorists a great opportunity to reach their illicit goals without the need for sources of funding, a cyber terrorist attack requires no more than a computer connected to the network and the necessary software, the difficulty of proof is one of the strongest motives that facilitate committing a cyberterrorism attacks; it helps the perpetrator to escape punishment.

- The difficulty of detecting and proving terrorist crime.
  This occurs particularly in the field of penetration crimes, which helps the terrorist to move freely within the sites he targets before committing his crime (Batali, op. cit, p. 44). The difficulty of proof is one of the most important motives for committing cyber terrorism because it gives the terrorist an opportunity to escape punishment (Salama, 2006).
- legal vacuum and lack of information networks control.
  In some countries there is a legal and regulatory vacuum, and this is the reason for the spread of cyber terrorism, a terrorist may conduct his attacks from hostile countries to attack other countries. All these reasons encouraged the spread of the phenomenon of cyber terrorism, which has become the best means of criminal action of various terrorist organizations.

It is notable that countries have developed legal legislation to combat this crime, whether of legislation in the criminal, constitutional, commercial or civil law, but they are still unable to eliminate this kind of crime and this requires the legislators in all countries to update the legislation constantly to encounter this dangerous type of Terrorism.

The objectives of cyber terrorism

According to Nawayseh (2011) cyber terrorism aims at various illicit targets.

1) Propaganda and attract attention to stir public opinion.
2) Collect and grab money.
3) Revenge of opponents.
4) Threatening and blackmailing public authorities and international organizations.
5) Damage and destruct the infrastructure and means of communication of countries, whether public or private organizations
6) Endangering the members of society and threatening the economy and national security.
7) Violation of public order and information security. (Alfi, 2005)
8) Spreading terror and fear among individuals, nations and communities.

Terrorists and the Internet

To what extent can cyber-terrorists use information to serve their goals, and are there new prospects for cyber-terrorism?

This research focuses on the scope and limits of terrorist use of information and what areas are expected to be used.

(i) *The scope of Internet use by terrorists.*

According to Alfi (2013) a study conducted by Gabrielle Wimann, who is an expert on international terrorism Harvard-USA, on how terrorist groups use the internet to achieve their malicious purposes. The results revealed that uses are as follow:

- Information exploration: Internet itself is a huge electronic library that contains sensitive information that terrorists seek to obtain such as nuclear facilities, international airports and information on ways to combat terrorism, so that a large amount of their inventory depends on the electronic sites that are available to all, without violating any laws or network protocols.
- Communication: Internet assists sporadic terrorist organizations to communicate and coordinate with each other because of the low cost of Internet connection compared to other means. It also has variety of information that can be exchanged. The absence of an apparent leader of the terrorist group has become an essential feature of a modern terrorist organization compared to the old hierarchical pattern of terrorist groups, all because of the ease of communication and coordination across the World Wide Web (Badaina, 2002).

- The mobilization and recruitment of new terrorists: The recruitment of new elements within terrorist organizations maintains their survival and persistence. They take advantage of the sympathy of other users of the internet with their issues and attract people in terms of glamorous and enthusiastic through the chat rooms, and we know that the entertainment of young people and adolescents are sitting for long hours in internet cafes for chatter with all humans around the world.

- Giving instructions and electronic indoctrination: The Internet is filled with a huge number of sites containing manuals and instructions explaining the methods of making bombs and deadly chemical weapons, and when using the search engine “Google” to search for sites containing topics such as "terrorist" the results will be great.

- Planning and coordination: Internet is a very important means of communication for terrorist organizations, permitting them the freedom to coordinate precisely to conduct specific terrorist attacks. Gabriel Wiman adds that al-Qaeda members have relied heavily on the internet in planning the September 11 attacks. Email and chat rooms to manage terrorist attacks and coordinate the actions and tasks of each terrorist.

- Access to funding: Terrorists use selected demographic data from users' personal information on the web through online inquiries and surveys to identify people with compassionate hearts and then use them to pay financial contributions to legal persons representing the front of these terrorists. This is done by e-mail in a cunning manner that is not suspected by the donor as helping a terrorist organization.

The new expected scenarios of cyber terrorism

The expected cyber-attacks occupy an advanced position in the effort of specialized international institutions in terms of research and studies. These scenarios can be divided into targeting military and economic systems, targeting transportation systems, power generation, electricity, intimidation and espionage. The most prominent of these new Expected are:

a) Targeting military systems and economic infrastructure.

One of the most dangerous scenarios is the penetration of weapons information systems by terrorists. Through this infiltration, it can control all weapons systems, and this could result in a global catastrophe. In terms of economics, the world has become dependent on information networks in the world of finance and business. This scenario includes a major imbalance in the systems of networks that control the activity of banks and international financial markets, spread of chaos in international business transactions. In addition, A partial or total disruption of trade and business systems can be made to disrupt economic activities to stop working (Khalil, 2000).

b) Targeting transportation, power generation and water systems**.**

Transportation is targeted through the penetration of control systems of air, land and sea lines, resulting in technical malfunction in the movement of aircraft and trains and change their time schedule to create chaos or collision between them as well as ships, submarines and tankers. The same acts could occur to computers and computer networks that control power distribution resulting a disrupt of many life facilities in the State due to the lack of energy sources, the same may happen for water networks. Terrorists may attempt to disrupt medical information networks (Qadeh, 2018), which can be attacked and hacked and manipulated, resulting in casualties as a result of this penetration. This penetration has devastating social effects.

c) Intimidation and cyber espionage.

Terrorist groups and organizations use communications through the World Wide Web to intimidate and spread fear and terror for financial funding by sending threatening e-mails, threats through websites, forums, chat rooms. The types of threats differ, sometimes it takes the form of threatening the life of prominent political figures by killing them. The threat of bombing national facilities, furthermore, spreading viruses for damage, destruction of information networks and electronic systems (Ajalan, op, cit, p22).

Terrorists are expected to spy on individuals, countries, organizations, bodies or international or national institutions, where the process of sending electronic espionage systems performed in several ways, the most popular is the e-mail where the victim opens the attachments sent within the message of unknown sources. Another way is by downloading programs from untrusted sites, terrorists can use viruses in hacking and information espionage (Ajalan, op, cit, p23).

When they penetrate the e-mail of others, they access to information and data, realize their secrets, and spy on them to know their correspondence and communications to benefit from them in their terrorist operations or threat to get them to do certain planned actions.

Obviously, all sectors have been targeted by terrorists for their reliance on informatics (Badayneh,op,cit,p37) especially, the telecommunications and information sector, the public telecommunications network, the internet, personal computers, and all sectors which depends on cyber information such as academic organizations, government and commercial use, transport, railways, ports, water lines, airports, transport companies, shipping services and the energy sector, Oil and natural gas, the financial sector, banks, investment companies, security exchanges, emergency services and government services.

Thus, cybercrime is a behaviour involving a digital environment, a computer and the availability of a connection to the information network. The physical work is carried out through the computer or through the automated processing of data. It is necessary to initiate the technical activity leading to the crime. Such as the manipulation of data or the destruction of information systems (Ibrahim, 2009). Other activities such as spamming in the sense of sending emails to attack on the information network, where the terrorist organizations and groups destroy the infrastructure of the systems of various locations, for example, exposing Amazon to sell its books online and spamming the company CNN news with several mails, which led to slow flow of information.

Combating cyberterrorism crimes with preventive procedures and remedial methods

In spite of the difficulties faced by States in the fight against cyber terrorism, there are means and efforts taken around the world in combating these crimes that has widely spread because of the use of internet and the ease of concealment and destruction of the effects of crime. Consequently, several countries have cooperated with each other on local and international levels to enhance their cyber security and impose legislation to combat the increasing danger of those crimes.

We cannot deny that there are difficulties facing combating of cyber terrorism and hinder international cooperation such as the ease of concealment of crime and the difficulty of tracing the perpetrators of most of the terrorist crimes as a result of the inability to detect their identities and the absence of a joint international agreement on criminal acts because of the lack of a unified concept of this crime. Despite the existence of the Budapest Convention of 2001, which is the beginning of international cooperation, the efforts still limited in contrast with the cyberterrorism, which is still ascending continuously.

There are also legal obstacles and technical problems related to the investigation procedures, tracking and prosecuting the perpetrators of this type of crime, in addition to the difficulty of proof and of obtaining evidence(Adly,op,cit,p17). The problem of conflict between the right to privacy and inspection is a real problem because terrorist crimes are of an international nature. The perpetrator of the crime of cyber terrorism is extraterritorial.

Corresponding to the increasing threats and dangers of using modern technology, it is imperative for different countries to seek mechanisms through which to lessen the threats posed by cybercrime by relying on an effective security policy that places cybersecurity at the top of their priorities and strategies.

The aim of cybersecurity is the ability to resist deliberate and unintentional threats, response and recovery, and thus to be free from the threat or damage caused by the disruption or destruction of ICTs or by the misuse of ICTs (Bologna & Hammerli, 2013). This requires the protection of networks, computers, programs and data from attack, damage or unauthorized access (De Franco, 2014).

Finally, considering these challenges, State, that seeks to maintain its security, stability and sovereignty must pay close attention to the issue of achieving and developing its cybersecurity in order to avoid the dangers of cybercrime by adopting preventive and remedial policies.

International, regional and national efforts to combat cyber terrorism

Abdul Hamid (1999) stated that the world was trying with all its capabilities to deal with cyber terrorism, where security cooperation is necessary, and it is the only way to prevent these crimes. Khreisat (2006) mentioned that the Arab countries alerted to the dangers of terrorism and have signed agreements and treaties. The most important of these agreements is the Arab Convention against terrorism. The United Nations General Assembly stressed the importance of initiating operations and procedures in the areas of crime prevention and international criminal justice. The United Nations launched the Information Bank and e-mail under the name of the International Criminal Justice Information Network (uncidin) in order

to transfer studies and research from criminal institutes to governmental and non-governmental organizations and the experts in criminal justice (Shalala, 2003).

The Security Council issued several resolutions on combating terrorism, but it was not comprehensive or related to cyber terrorism in particular, the most important of which is resolution 1267/1999 on the situation in Afghanistan and resolution 1373/2001, which is the most important and comprehensive terrorism resolution, on which the international legal system is based on to prevent and eliminate terrorism(Khresat,op cit,p.54).

Regionally, many agreements have been concluded to encounter these crimes because of the difficulty of confronting this terrorist threat by a single country, thus, it became necessary to consolidate the policy of security integration.One of the most important forms of Arab cooperation is the Arab Convention for the Suppression of Terrorism of 1988, which was adopted by Arab Ministers of Interior and Justice, which discussed ways to confront terrorism in all its forms. The agreement was made up of 42 articles, based on preventive measures, combating terrorism and cooperation in the judicial field. An Arab agreement was also signed to combat the crimes of information technology in 2012 to enhance cooperation among Arab countries in the field of combating information technology crimes to maintain the security of States, their interests and the safety of their members.
Nationally, the Jordanian Legislative authority issued the cyber Crimes Act of 2018. The provisions of this law emphasis the deterrent penalties for the perpetrators of these crimes and defining the types of crimes.

It should be noted that Jordanian laws whether criminal, commercial or civil laws, have worked to their full potential to counter cyber terrorism because it affects electronic commerce and the property of the state and individuals. Jordan has issued criminal legislation criminalizing cyber terrorism and imposed deterrent penalties for being a full-fledged crime. But sometimes there is a difficulty in following up this crime from within Jordan, especially if the elements are fragmented, some of them inside Jordan and the other outside Jordan, here is the need for judicial cooperation agreements between countries. Therefore, laws must be developed to deal with this issue from all sides, so that it can be kept abreast of developments and serve as a constitution supervised by a supreme committee of various disciplines.

It should be noted that Jordanian laws, whether criminal, commercial or civil laws, have exerted their full potential to counter cyber terrorism because it affects electronic commerce and the property of the state and individuals. Jordan has issued criminal legislation criminalizing cyber terrorism and imposed deterrent penalties for being a full-fledged crime. But sometimes there is a difficulty in following up this crime inside Jordan, especially if their elements are spread, some of them inside Jordan and the other outside it.

Therefore, it is the necessary to conclude judicial cooperation agreements between countries and developing them to deal with this issue from all sides, so that it can kept abreast of developments and serve as a constitution supervised by a supreme committee of various disciplines.so, it can be said that all these efforts are insufficient to combat cybercrime and need much more effort because terrorism is expanding day after day, which calls for solutions to prevent and combat terrorism at all levels.

Preventive procedures to cyber terrorism

There are several methods, and procedures that can be followed to prevent cyber terrorism, the most important of which are:

1. Adopting a preventive policy to spread the culture of security and raise the awareness of the community of dangers and threats of cyber terrorism. Protect members of society against all destructive ideas published by various websites and social media by blocking and removing those publications which promoting the idea of terrorism through the Internet and the prosecution of supporters. In accordance to Khreisat (2006) Educating children by their parents from childhood has a great role in raising them to respect people and the principles of good morals to achieve intellectual stability, In addition, the security awareness plays a major role in achieving intellectual security and instilling security concepts in the emerging minds by dedicating the role of family and society and focusing on the role of individuals in resisting intellectual deviations that generate many social problems. It should be noted that the right religious education away from extremism and ignorance and the focus on the values and laws of society have an important role in the prevention of cyber terrorism.
2. Enhancing cooperation and coordination between countries and international institutions can be achieved by unifying different efforts to control what is provided through the network, protecting important sites and providing the necessary technologies to confront them through Internet service providers by reporting terrorist activities that involve acts that violate security and order (Nazmi, 2010).
3. Updating and protecting ICTs, identifying the strengths and weaknesses of the legal legislations related to combating cyber terrorism crimes, and working to overcome obstacles to their application.
4. Activating the role of the media in encountering the criminal ideology of terrorist organizations on the Internet, and warning from various sites that incite violence and calling for mobilization and recruitment of extremist thought.

5. Focusing on the role of the media in the dissemination and broadcast of television work on terrorism and its devastating consequences, and provide advice and guidance on the use of the Internet and what is published by terrorist organizations on various websites.
6. Urging countries to freeze the funds of terrorists and their associated individuals and institutions through the establishment of intellectual conferences.(Khreisat,op, cit,p.45)
7. Adding anti-terrorism material within the school and university curricula for the formation of generations who decline terrorism in all its forms, encourage conducting scientific research on the phenomenon of terrorism to refute the thought of the terrorism.
8. Disseminating the values of citizenship, tolerance and middle thinking and strengthening the status of security institutions in the hearts of citizens, through defamation of their achievements in the field of combating cyber terrorism.
9. Benefiting from the experiences of the leading countries in the field of achieving cybersecurity and identify the best global techniques used in the combating cybercrime and cyber terrorism.
10. Creating information technology system that allows the regulation of electronic transactions and protect customers from its risks by providing systems to regulate the behaviour of individuals and institutions in the field of dealing with information technology.(Badaina,op,cit ,p305)
11. Purchasing hardware and software that achieve the greatest security for information and provide the latest programs to detect viruses to protect the computer.
12. Establishing a specialized departments in the Ministry of Interior and security bodies to monitor electronic activities and prevent the crime of cyber terrorism (Juhaini, 2005).
13. Following-up scientific publishing in the security field and from interested organizations to benefit from their research findings (Badaina,op,ct , p 323).

Ways to Combat Cyber terrorism

A number of ways to combat cybercrime can be applied in accord to the ability of states to do so. For example, in 1996, USA President Bill Clinton formed a committee to protect the sensitive infrastructure of the United States (WWW.NIPC.GOVE), the electrical power, telecommunications and computer networks, which are considered a vital element in existence of the United States because it will be the first target of possible terrorist attacks. Special bodies and centres have been established to deal with the potential of cyber terrorism, such as the Central Intelligence agencies.

Europeans set up NATO forces took similar procedures as the United States. There are also joint projects such as the Echelon project, which was jointly set up with European countries to spy on Internet messages and phone calls in the world and the Carnivore project. The FBI also pursues the Hackers (Infiltrators) and the secret services are pursuing digital terrorism in the cases of electronic banking and fraud and eavesdropping.

In the Arab world, experts point out that there are a lot of cyber-infiltrations by terrorists, especially in the area of remittances. There is also an exchange of information between terrorists to incite terrorist operations and to recruit elements, but Arab intelligence has spent hundreds of millions of dollars tracking and analysing websites through which these operations are closed and they still combat these sites.

As for Jordan, the level of combating cyber terrorism is good despite all the difficulties facing Jordan in many respects. Despite this, it has issued the appropriate laws and legislations to address this global issue, but Jordan has not reached advanced stages.

The most reliable methods of countering cyber terrorism are:

- Providing a legislative environment to deal with this type of crime, if there isn't a legislative cover or a legal text criminalizing this type of action, we cannot talk about mechanisms to investigate the crimes of cyber terrorism. It is also necessary to stress on the penalties against all those who have been proven to have committed this crime(Atia, op,cit,p.27).
- Reviewing the tactics and trainings adopted to combat terrorism periodically and modify what is necessary to suit the requirements to combat future terrorist threats on the world stage.
- Monitoring strictly the perpetrators of cybercrime offenses during their time in prison.
- Applying the principle of isolation and separation, by isolating convicted persons in this type of crime from other sentenced to avoid the danger of the impact of other prisoners.
- Implanting sources within the prisons where convicted persons of cyber terrorism are, and surveillance the visitors of those convicted of the crimes of cyber terrorism.
- Applying reform and rehabilitation programs for convicted persons in this type of crime. These programs aim to rehabilitate the inmates and try to benefit from them and to recruit them for the benefit of the state. This is, therefore, an important source of information about terrorist or extremist groups.
- Enacting of special laws or legislations that fill all gaps in the crime of cyber terrorism and their means of investigating, such as laws on how cyber evidence is discovered, kept, and evidence that is legally accepted to prove it.

- Establishing a national body of experts and specialists working on developing a national strategy for cyber security, focusing on protecting the infrastructure of information networks and software systems, coordinating and unifying efforts between the different fronts in the country: security, legislative, judicial and technical. Controlled and legally proven.
- Convening agreements between states regarding the crimes of cyber terrorism, organizing all procedures related to the prevention and treatment of this crime and exchanging information and evidence thereon, including the activation of extradition agreements for crimes of electronic terrorism.
- Promoting international cooperation through the monitoring by each State of the electronic subversive acts on its territory against States or others outside these territories.
- Monitoring terrorist sites to be a source of great information for the security services, in terms of terrorist relations, terrorist ideology, terrorist plans, and the study of statements issued by terrorists, to know their plans and strategies so that the security services can confront terrorism at the same intellectual and logistical level if they do not excel by using their weapons and their locations.
- Implanting security elements in these sites in order to corrupt or destroy their plans, or to publish a correction of the information contained therein, so that anyone who enters these sites loses confidence in the context and the beliefs of these sites, and whether the founder of these sites is the people of thought or other areas, where these sites will lose credibility. And instead of penetrating the official sites, these sites themselves are infiltrated by some patriotic, intellectual and religious young people to enter, debate and disperse the efforts of people of distorted thought and terrorism.
- Coordinating with site administrations and search engines such as Google, Yahoo, YouTube, Windows Live, Facebook, etc. to prevent terrorists from accessing these websites, not to use their sites as a means to spread terrorist ideology, and to beware of these sites. International and regional cooperation and a real barrier of terrorist ideology, as this distorted thought is quick formed spread.
- Establishing, developing and activating international counterterrorism centres and institutions within the public and private sectors worldwide.

Conclusion

Combating cyber terrorism is one of the most important new challenges imposed by rapid technological developments, and therefore the States and communities should make every effort to succeed in combating the various risks generated by cyberspace, which topped by cyber terrorism and other threats.

Finally, many efforts have been made on the issue of combating and preventing cyber terrorism despite the difficulties facing the security authorities, different definitions of cyber terrorism were stemmed according to the states' political standards, several conventions were held. All these efforts show the seriousness of this crime globally.

Additionally, there are a link between terrorism and modern technology of communication and the internet.

Cyber terrorism has various reasons, methods and forms, it didn't come out of a vacuum, so all states should investigate these causes and find solutions.

Results

This research addressed the subject of electronic terrorism in our modern time, which extended rapidly due to several reasons such as: intellectual, religious, economic and social vacuum .More effort is required at the international level, national and regional to reach the guaranteed results .In addition to the need for more focus on the religious role Social and educational.

Competent authorities also should keep an eye on the channels of deviant thought owners who spread discourse of terrorism with a focus on accustoming society to obey laws and regulations ,respect and comply with its orders.

The Internet must remain a space for the dissemination and sharing of science and knowledge and an instrument of creativity, rapprochement and cooperation between individuals, peoples and nations, not a means of threatening, exploited by terrorist groups to achieve their criminal goals and to dissemination their ideas.

Recommendations

- Issuing legislation to deal with the crimes of cyber terrorism, and to review and update them constantly in line with the special nature of these crimes.
- Cooperating and coordinating with countries under the supervision of the United Nations through the establishment of special centres in the ministries of interior to follow up the latest developments of cyber terrorism crimes in the world and ways to combat them.
- Allocating special and independent departments at the level of the country to combat cybercrimes and appointed trained persons in the field of electronic in order to deal with these crimes.
- Modernization the security services and developing their professional capacity to deal with cyber terrorism through training and holding of external and internal courses.

- Training a specialized team to monitor websites, especially those used to disseminate ideas that serve terrorist notions and to block suspected sites that may belong to terrorist organizations or simply have terrorist tendencies, or which may serve the purposes of terrorist groups directly or indirectly.
- Raising awareness among members of society at all levels through school and university curricula, television programs and holding seminars to show the risks resulting from the unsafe use of the Internet.
- Paying more attention of the legal aspect of these crimes, studying them, as well as technical attention such as encouraging research and studies in this field.
- Unifying criminalization images related to cyber terrorism.
- Providing citizens with the opportunity to participate in combating cyber terrorism by finding a means of communication with the security authorities to report on these crimes.
-Continuously updating criminal, commercial and civil law in the field of electronic terrorism developments with
-Developing solutions by governments to the causes of terrorism, especially economic ones
-Developing programs to eradicate intellectual illiteracy under the supervision of the Ministry of Education focusing on intellectual awareness in schools, institutes and universities
- Seeking more cooperation between the Ministry of Interior and the Ministry of Communications to tracking terrorist organizations by monitoring the Internet and track their activities , preventing their penetration and combating them.

REFERENCES

Abdul Hamid, M.(1999). Arab security cooperation and security challenges, Riyadh, Saudi Arabia, Naif Academy for Security Sciences, p. 112.

Adly, M, S.(2009). Legislative Space in the Field of Combating Electronic Crimes, Research published on Shaima Atallah website, p. 16.

Afif, M, A.(2011). Terrorism Crimes in the Jordanian Penal Code, PhD Thesis, Faculty of Law, Amman Arab University, Jordan, p. 266 September, p.9.

Ajlan, A, A.(2008). Electronic Terrorism in the Information Age, Research presented to the First International Conference in Cairo on 2-4 July, p.11.

Alfi, M.(2013). Legislation Combating Electronic Terrorism Crimes: Substantive Provisions and Patterns, Working Paper presented at the Scientific Symposium on Arab and International Laws in Combating Terrorism, held in Riyadh, 15-17, pp.6-8.

Alfi, M.(2005). Cyber - Espionage and Cyber - Terrorism, Arab Lawyers' Forum, p. 88.

Attieh, A, M.(2014). "The Role of Modern Mechanisms to Reduce New Crimes: Electronic Terrorism and the Methods of Countering it", Paper presented at the Scientific Forum: Crimes Emerged in the Shadow of Regional and International Changes and Changes, Amman, 02-04.

Arquilla, J, & Ronfeldt, D.(2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. USA; Rand publication, p281.

Badaina, T, (2002). Security and Information War, Dar Al Shorouk for Publishing and Distribution, Jordan, p 134.

Bateli, Ghai.(2015). electronic crime, comparative study, publications of the Algerian House of Publishing and Distribution, Algeria,

Bawadi, H.(2004). The Experience of Electronic Terrorism, 1, University Thought House, Alexandria, p.16.

Bassiouni, M, Sh.(2003). *International Documents on Human Rights*, Volume II, Dar Al Shorouk, Egypt, this document was published with the permission of the International Institute of Human Rights at DePaul University, Chicago

Bologna, S, & Hammerli, B, & Gritzalis, D.(2013). Critical Information Infrastructure Security. Berlin; Springer, p. 02-03.

De Franco, J, F.(2014). What Every Engineer Should Know About Cyber Security and Digital Forensics. Boka Raton: CRC press, p40.

Elfeel, A.(2011). Electronic Crime, Comparative Study, Zain Legal Publications, p.66.

Hussein, A, e - terrorism the most dangerous battles of space wars, Al - Watan newspaper of Jordan, Retrieved from: http://alwatan.com/details/166324.

Ibrahim, Kh, M.(2009). Computer Crimes, University Thought House, Alexandria, 2009, p. 100

Janabihi, M, & Janabihi, M.(2005). Cybercrime and the Computer and its Means of Control, Dar Al-Fikr Al-Arabi, Alexandria, p.230.

Jordanian Prevention of Terrorism Law No. 18 of 2014.

Kafi, M, Y.(2012). Electronic Management, Dar Ruslan for Printing, Publishing and Distribution, Damascus, 2012, pp. 440-441.

Kafi, A, I., & Fattah, A.(2007). Terrorism and its Fight in the Contemporary World, The General Environment of Cultural Palaces, Cairo, p.20.

Khalil, E, Ali.(2000). Legal Adaptation of Misuse of Card Numbers via the Internet (Scientific Study under the Jordanian Penal Code) Legal Research, Faculty of Sharia and Law, p. 5.

Khreisat, S.(2006). International Counterterrorism Mechanisms after 9/11, Master Thesis, Amman Arab University, Jordan, p. 53.

Khalil, M.(2015). 50 thousand websites to dame. Terrorism is besieging the Internet, Retrieved from the site: Http://www.alittihad.ae/details.php?id=64991 & y = 2015 & article = full

Mahmoud, A, H.(2013). Theft of information stored in the computer, Dar al-Nahda Arab, Egypt, I 3. P69.

Nawayseh, A, M.(2011). Crimes against State Security, 1, Dar Wael Publishing, Jordan, p.9

Nazmi, R.(2010). Intellectual void and its impact on the misuse of modern communication technology, conference on terrorism and extremism, Medina, Saudi Arabia,

p. 21.

Salama, M, A.(2006). Computer and Internet Crimes, Knowledge Establishment, Alexandria, Egypt, p. 148.

Saqr, N.(2007). Computer Crimes and the Internet in Algerian Legislation, Dar Al-Hilal, Algeria, p 120.

Saghier, J.(2001) Criminal Law and Modern Technology, Crimes arising from the use of computers, Dar al-Nahda al-Arabiya, Egypt, undated, p.17.

Saned, A, A.(2004). The Means of Electronic Terrorism and its Rulings in Islam and its Methods of Control, World Conference on Islam's Position on Terrorism, Imam Muhammad bin Saud Islamic University, Saudi Arabia, p. 8.

Shaimi, M. A.(2015). Introduction to Terrorism in Egypt and Saudi Arabia, Strategic Experiences, *Modern Arab Bureau*, Cairo, pp. 18-19.

Shalala, N, N.(2003). International Terrorism and Criminal Justice, I 1, Lebanon, Halabi Publications, p.63.

Sirohi, M, N.(2015). Cyber Terrorism and Information Warfare. Delhy; Alpha Editions, 2015, P01 Newton Lee, Counterterrorism and Cybersecurity: Total Information Awareness. 2ndEd, Switzerland; Springer International Publishing, p225.

Ushie, H, E.(2013). The Impact of Terrorism) Including Cyber Terrorism (and Threats of Terrorism on International Business) or Nation Sate. (Journal of the International Relations and Affairs Group, Volume 3, Issue 1, p38.

Qadeh, Mahmoudi.(2018). the dangers and manifestations of electronic terrorism, legal research at the Faculty of Law ibn Khaldun University, Algeria, p.24.