المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

Uses of The Internet to Counter Electronic Terrorist Activity

Dr. Nibras Salim Khudhair
Department of Law - Al-Kunooz University College – Basra - Iraq
Email: nibras.s@kunoozu.edu.iq

ABSTRACT

The study aimed at determining the nature of electronic terrorism, its forms and means, as well as clarifying the increasing role played by the Internet in disseminating the ideas and principles of terrorist organizations. The study followed the extrapolation method that formed this study. Targeting the general three different categories, the first category are supporters or current and potential followers, the second category is the international public opinion, or the third category is the enemy masses, the use of terrorists to the means of technology such as the Internet and Intelligence and other devices, for the purposes of promoting their beliefs, directing threat and intimidation messages, for recruitment, mobilization, planning, coordination, financing, information gathering and account penetration, etc., contributing to the implementation of their serious terrorist acts.

Keywords: Internet, Electronic Terrorist.

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

Introduction:

The Internet plays a vital role in our world and societies, however, it is also used for criminal deeds, involving terrorist actions. In the past, using the Internet by terrorists has been discussed, and efforts have been made to involve the Internet terrorist usage in the war against terrorist acts. However, None of these efforts were focused on regular negotiation with the civil society and the private party. Such regime initiatives are only in danger of causing law that is officially impractical and ineffectually assisted by end-users or contrary to major rights and liberties. The Internet is mainly controlled by private institutions, and most Internet expertise is focused on it and in civilian community. However, intelligence agencies and law enforcement have the best awareness of terrorist actions. Thus, Public-private discussion is a rational methodology in recognizing the finest tools to decrease the terrorists' usage of the Internet **(Ministry of Security and Justice,2013)**.

The Internet has changed fundamentally the lives of people. It revolutionized the way of communication. Moreover, it facilitates the way you appoint networks among similar people **(Eurostat,2012)**, This development has caused vital changes in the society organization and its work. As extremists and violent terrorists constitute part of this society, it is vastly assumed that the Internet plays a distinguished role as an instrument of extremism **(Aly,2010)**, Public policy discussions on the Internet role in terrorist activities are developing. However, intense research and informed criminology have stated little about it. Among the notional and narrative writings on the fanatic exercise of the Internet, lessons have normally provided accounts of the affiliations provided by the Internet to fanatic organizations, together with cybernetic public construction, recruitment, data provision, virtual exercise, broadcasting of propaganda, staffing, funding and risk mitigation **(Holt et al.,2015).** These calculations have implicitly considered the communication between the user and the Internet as one-way disclosure to the content of the Internet and can result in behavior changing. However, these accounts do not have the recognition that each possible user would not benefit from the cost and would not use it in the same manner. The degree to which an individual is able to afford is determined by their objectives, procedures, morals, beliefs and skills **(Norman,1988)**

The increasing use of terrorists by the Internet is not surprising and is driven by a number of different fundamental factors. First, the usage of the Internet has dramatically surged over the past years throughout the world and the use of terrorists and other illicit actors has increased. Terrorists use the Internet to raise funds and transform them into part of a wider global shift to the use of technology in international trade. There have also been enormous shifts in how money is transferred from one point to another, with new technological developments. Electronic money transfer - using the Internet to start transactions - is becoming increasingly common through services such as PayPal **(Jacobson,2010)**.

The purpose of the present research is to fill the gaps in awareness through discovering, comprehending and clarifying the perceptions of 10 US terrorist specialists on the way terrorists consume the Internet to shape global act of terrorism.

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

The inferences of the constructive communal modification resulting from this study are addressed to the US information community, which contains 17 organizations and administrations like the DHS, the FBI, the CIA, the National Agency For geographic intelligence information (NGA), and the Office of the Director of National Intelligence (ODNI). Furthermore, the impact is also addressed to the Counter-Terrorism Implementation Task Force (CTITF), which is composed of 31 global units like the system of the United Nations in anti-terrorism actions **(Wilson et al.,2016)**.

Study problem:

The Internet has spread widely around the world and has become an integral part of information technology within many companies as well as homes **(Adetayo et al.,1999)**, The relationship between terrorism and the Internet has come into existence and has been occupied by States and organizations concerned with the fight against terrorism after the September 11, 2001 attacks. Perhaps the dangerous trend that terrorist organizations began to follow him not to represent activity Palace ē a terrorist material on the real sphere, but moved into cyberspace there and became a media campaign to keep up with the military campaigns by both sides was the use of the Internet. Electronic terrorism depends on two important dimensions: the first is to become a catalyst for a traditional terrorist act by providing information about the target locations or as an intermediary in the implementation of the terrorist operation. The second dimension can be said to be a moral dimension intended to incite religious hatred and war of ideas **(Qaisi,2014)**.

The organizations and terrorist groups seek to inflate the mental image of the strength and size of these organizations and groups, and to serve the media and military aspects of these groups. These groups are not interested in how many people have been killed as much as how many people have seen and interacted with the terrorist incident.

The Internet provides a free and relatively unobstructed environment where extremists can formulate and broadcast information over apparently unlimited numbers of websites and public media platforms, commensurate with targeting thousands of possible new employees to seam their association and promote their foundation. Stimulating, particularly, creates the most technically innovative advertising so far. They sponsored the belief that a preacher had effectively proven succession and enlisted thousands of additional followers to be part of the terrorist group through classy digital resources. Dodging movies, ranging from few minutes to hours, using Hollywood-style creation deceptions and special effects to depict a terrorist who advocates as heroes and imagines fighting for a hilarious style of playing in a realistic video game. These vicious and heinous images are directed along with photos and articles that describe the dreamy and thrilling run into and reserves of young people. A propaganda gathering between horror and excitement to intentionally attract young people through communal media, and describing existence in the region as a beautiful and ideal, and its participants as the protagonists and necessary. This advertising

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
مارس 2021 العدد (19)
Volume (19) March 2021
IJOHSS

failed to reveal the ugly truths of living in the atrocities committed by the preacher **(Lieberman,2016)**.

The study objectives:

The present study aims to:

1) To identify the nature of electronic terrorism and its forms and means, as well as to clarify the growing role played by the Internet in spreading the ideas and principles of terrorist organizations
2) To identify this crime and methods of dealing with it form and subject by the police and judiciary in proportion to their risks and consequences
3) Identify the impact of terrorism through the Internet on the community.
4) Identify the most important methods and methods that help in developing the skills necessary to confront terrorist crimes on the Internet.

Study questions:

Through the study problem developed many questions, the most important of which are:

1) What is the nature, forms and means of electronic terrorism, as well as the increasing role played by the Internet in disseminating the ideas and principles of terrorist organizations?
2) What are the crimes and methods taken by the police to deal with them to eliminate them in proportion to their risks and consequences?
3) Is there an impact of online terrorism on society?
4) What are the most important ways and means to help develop the skills needed to combat terrorist crimes on the Internet?

The importance of studying:

The importance of the study of electronic terrorism in educating individuals from all societies in the means and methods used by terrorist organizations to attract and recruit these individuals. The importance of this study is also highlighted in highlighting the role that States, groups and individuals must play in tackling and preventing this phenomenon. The study also draws on the awareness of the researcher that the phenomenon of new crimes, including electronic terrorism, has become a real challenge to the prevailing criminal policies and its legislative, executive and judicial organs.

A glimpse on terrorism's history:

In terms of affecting, various strategic methods and tactics of recent extremism have up to rather lately shadowed those used by Countries in their equipped wars. Specifically, a century ago, it was said that terrorist laws relating to the targeting of fatalities carefully looked a lot like specialized army laws in that they valued the difference between militaries and officers on the one side and guiltless residents on the other (such as the planned murder of Archduke Franz Ferdinand of Austria) 28

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

June 1914) **(Walzer, 1977)**. This has been the situation since the middle of the 19th century, when industrial weapons increasingly facilitated the lack of targeting, meaning that the killing of the opponent turned out to be more unselective and fatal. The industrial and unselective methods and war techniques used through the "total war" of the twentieth century (for example, in an extensive disrespect of the attitude of distinct) have successfully qualified persons who will develop to be postwar radical terrorists who will likewise implement new weaponries and irregular practices of warfare, like urban terrorist war. In the modern world, undiscriminating weapons (such as high-level bombarding capabilities, mass destruction missiles, etc.) are a frequent feature.

With regard to the terrorist policy, a beneficial method of conceiving the development of up-to-date violent act as a refuge for innovatory violence is delivered by David Rapaport's powerful perception of "waves of terror" (terrorism's four waves). For instance, one wave is the late 19th / early 20th century "Anarchic Wave". The other point is the "anti-colonial wave" (beginning with the post-World War I governmental attitude of self-rule, for example, the negotiation of the land Islands in 1921 and its vicious development into a lawful right after the Second World War. Vietnam). In contrast, the tactics used in both waves mostly reflect the ones used among countries in times of military conflicts, not least since released militaries all over the years have eventually come back to their families when the war is ended completely qualified to use power, however the title of every wave Terrorism reveals its main tactical objectives. The theory of waves also reveals that terrorist organizations are rising and falling, and also they can be resolved when they cannot inspire others to carry on malicious fighting to power, to sadistically confront injustice or other grievances, or to violently disapprove the absence of governmental concessions. This topic indicates that terrorism and its drives are obviously affected by the circumstances and the ups and downs in communal and governmental cultures **(UNITED NATIONS,2018)**.

On the contrary, Parker and Sitter **(2016)** assume that vicious terrorist states happen throughout the world not in many waves, but because of differentially stimulating terrorist performers over four target-oriented tensions: nationalism, socialism, religious fanaticism or exclusion. These fundamental motives are not sequenced in chronological order, any single tension perishes and a novel breed ascends. Alternatively, they may work correspondingly, and sometimes interfere, to encourage diverse guerilla activities up to their requirements. This theoretical study provides a flavor for some of the debates and discussions that take place when trying to fully understand or classify "terrorist" organizations.

Motivation factors of terrorism:

1- poverty

The search for the motives of the dissident group is of great concern to societal professors. Aristotle notably declared: "Poverty is the origin of revolution and crime." After the September 11 assaults, a number of sensible political figures declared

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

poverty in the Arab / Muslim world is to be blamed, and some recommended launching a novel Marshall Plan for the world's unfortunates. Since these proposals are commendable because their objective, afterward many efforts is to link scarcity with revolution, scientists have found a diverse collection of perplexing experimental outcomes **(Tyson,2001)**.

2- Income distribution

Researchers have long been looking for an unsatisfactory amount of revenue to be blamed for spreading dissatisfaction in communities. Nevertheless, in spite of long-term uncertainties, real data-based analyses have been rather weakly linked to governmental violent and terrorist actions **(Venieris and Gupta,1986)**. I claim that politic violence is much more prevalent bourgeois nations and that the public is mainly vulnerable to violence acts when it is middle- deflation. Inders, Hoover, and Sandler confirm this conclusion by providing a straightforward correlation between the distribution of income and terrorism **(Enders et al.,2014)**.

3- unemployment

Perhaps there is nothing more harmful to a person's psyche than staying jobless for a longer time. Remaining jobless does not only alienate people from the world, but because their low or no salary decreases the chance rates of an actor to join a splinter association. The turbulent times of the mid-1960s witnessed, for the first time, a great work using regime financial aid, an effort to accumulate digital information about political terrorism. Their set readiness of large numbers of researchers has made it possible to search for experiential confirmation of joblessness as one of the source roots of the political governmental terrorism **(Gupta and Venieris,1981)**.

4- Political variation / absence of democratic liberty

In his launch of the "global war on terror," President George W. Bush superbly mentioned, "They (the terrorists who attack the United States) hate us for our freedom." This commentary assumes that violence is the creation of nations disadvantaged of liberty. However, elected countries like India, Israel and Sri Lanka are suffering from terrorist violence. There are many local extremists in Western elected states, either involving with internal terrorism or being part of extremist organizations grounded in distant countries. Actually, Bueno de Mesquita infered that the two are somehow unconnected, according to Pew Research Center facts, **(See and Li,2005)**.

The methods used by terrorists online:

Terrorists depends on several ways to attract new members to them through the following:

1- Advertising:

Information and communication technology (ICT) occupies an important part of the present networking community. This has impacted virtual communication among individuals who use and understand security applications and their impact on private

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

confidentiality. Many communication tools, particularly social networks over the Internet require highly developed security mechanisms. Confidentiality is important to the policy of security tools. Many providers of social network have provided settings of privacy to permit others to access or block personal information **(Aldhafferi et al.,2013)**.

Without a terrorist connection it would not exist **(Macluhan,1978)**, This tiny line bears the fact which has not changed over the past years. It is not unusual to refer to the connection between the dissemination of guerrilla letters and the presence of the recent mass media. However, before the media existed, terrorism was widespread . An instance of that is the form of violence which has encouraged chaos (the real plague of 19-century communities) that uses murders and new kinds of assaults as a means of getting to whole civilizations. Murdering significant and maybe well-known individuals or further acts before the eyes of hundreds or even thousands of watchers was an influencing way of confirming that these actions were well-known in a period when there was solid government rule the data and the mass media performed within a restricted range. Afterward, advances in technology will consent the spread of guerrilla assaults in methods which could never have been envisaged. Terrorists have found a strong friend in the mass media which will aid them gain social recognition and demands for this association. Terrorists commit acts of violence seeking three universal goals: getting attention, recognition, and even some sort of admiration and justice. These goals are achievable for those persons who are able to get the greatest media exposure. Those that you get have more opportunities to influence others. Terrorists always calculate the impact their actions will have on the media and the overall potential because this will give them the chance to be members of the "political triangle" **(Soriano,2008)**.

Terrorists use Advertising by:

A. Recruitment:

The way in which social media have influenced the widespread recruitment practices of terrorist organizations is that these techniques have provided the ability to digitally cross the border and have shown them in the home of any potential extremist. Organizational recruitment can be seen from two points, namely, overcoming distances and sovereign boundaries **(Labi, 2006)**, In addition to the significantly increased ability to distribute advertising **(Aly et al.,2016)**, The recruitment of potential terrorists and the spread of mass propaganda are interrelated activities, where propaganda is very likely to be an important factor in terrorist extremism, and these issues will therefore be discussed side by side **(The Clarion Project, 2014)**, Labi **(2006)** supports the idea that by harnessing advances in digital communications technology, terrorist groups have managed to make terrorism without limits within electronic environments. However, this is not how much the social media has brought to recruitment and extremism. With regard to extremism, Aly et al. **(2016)** refers to phased progress through an online platform, which first presents potential jihadists to the ideology of the organization, through registration, and advances to methods of

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

participation in the organization through new jihadist activity and communication to others within the organization.

B. Incitement:

The debate on freedom of expression and incitement to terrorism is being actively conducted on the Internet. In recent years, Islamic fundamentalists have used the Internet as a tool to alienate disaffected citizens throughout Europe **(Internet Jihad,2007)**. Many of these extremist citizens have committed terrorist attacks **(Rotella,2013)**, In response, the European Union took strong action to monitor the Internet. European specialized agencies have developed sophisticated ways to control cyber terrorism. Clean IT is the most popular online security control program: it seeks to close websites linked to the dissemination of terrorist information. Increased law enforcement has been accompanied by international and regional initiatives to criminalize cyber terrorism. In 2004, the European Council coordinated the Convention against Cybercrime, which imposed criminal penalties for cybercrime and hate speech **(cleanitproject,N.D.)**, Following the Convention, the European Union issued a framework resolution aimed at criminalizing incitement to terrorism. There has been widespread skepticism about what constitutes incitement to terrorism in the EU. The European Union took half of the regrettable procedure of calling for Member States to criminalize glorification of terrorism, but gave little guidance on what constitutes terrorism or glorification. As a result, countries have adopted cracked approaches. The law must be clear enough for anyone to judge whether their speech may be violated or not, but the rift approach makes it impossible. National courts have responded to the incitement trials by interpreting them as the language of broad legislation **(Council of Europe Convention on Cybercrime,2001)**.

C. The Push for extremism:

Terrorism is extremism in its most violent form. It is an attempt to intimidate societies, through severe violence against civilians, into political changes. In this context, some fundamentalist Muslims use terrorism as a tool to solve existential uncertainty by convincing the West to stop its perceived war on Islam. For example, Muhammad Siddiq Khan, one of the perpetrators of the London bombings of July 7, 2005, pointed out in his latest statement that his violence was a response to the atrocities committed by the West against his fellow Muslims. In this statement, Khan pledged that violence would continue until Muslims felt safe **(Khan, 2005)**. Moreover, terrorism also helps fundamentalist groups secure their existence by improving their recruitment because terrorist attacks attract attention to the fundamentalist cause. It is important to note that we are not discussing whether terrorism is a rational strategy to keep the group. It is undeniable that terrorism and violence have suppressed fundamentalist groups that are already undermining their existence. However, the latest wave of terrorist attacks over the past decade shows that fundamentalists use terrorism as a strategy to protect groups even if they have the opposite effect in some cases. Thus, we see that collective uncertainty and

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

fundamentalist fundamentalist extremism 257 Muslims respond to collective uncertainty with extremism, in this case, with fatal consequences.

2- Finance:

In the wake of the tragedies of September 11, 2001, the United States' first financial strike in the Global War on Terror (GWOT) came in the form of an Executive Order (EO), which targeted the financial rules of 27 different entities linked to terrorism **(Kiser,2005)**, to include organizations and individuals closely linked to al-Qaeda **(Comments of President Bush,2001)**. Following the EO, both domestic and international policymaking bodies have formulated nearly ten major initiatives and established nearly several new organizations, all with the aim of attacking terrorist financial networks. The international community then identified 315 entities as terrorist organizations or groups / entities associated with them, confiscating more than $ 136 million in funds and other assets in more than 1,400 accounts worldwide, making the financial dimension one of the most active fronts in World War II On terrorism **(National Money Laundering Strategy,2003)**.

3- Training

In the last few years, terrorist organizations have become increasingly sophisticated and are increasingly used as terrorists. There is a growing set of tools that will provide practical advice on how to print electronic manuals, audio and video clips, information, and tips. These instructions allow for the use of any form of information, especially if you take the form of a multi-media device that is easy to read, and cannot use it, such as how to join terrorist organizations, and how to Manufacture of explosives, firearms, other weapons or dangerous materials, and how to plan and implement terrorist attacks. Thus, these exercises serve as a training ground for the infant. They also use, inter alia, the exchange of specific techniques, techniques or practical information in order to commit a terrorist act.

4- Planning:

The publication of jihadism has made an important contribution to terrorists' ability to communicate, plan, recruit, organize and train through social media. Internet resources facilitate planning an attack. Intelligence gathering can be done from social media (such as Google Earth) and the use of encryption cannot be detected **(Willis et al.,2005)**.

It is also possible to take steps on the Internet to identify a possible target for a terrorist attack and to identify the most effective means of achieving terrorist infiltration. These legislative steps may include instructions on the methods used to carry out the attack and gather information about a proposed purpose from public sources and other sources. The possibilities offered by the Internet to approximate distances and the vast amount of information available to the public in remote areas make this network a key tool in the planning of terrorist acts, The planning process includes **(Counter-Terrorism Implementation Task Force (CTITF),2009)**:

A. Secret communication:

Three countries mentioned secret communication among the most important uses of the Internet for terrorist purposes, but not necessarily at a high level of sophistication.

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

The normal e-mail, sent from public computers at Internet cafes, was an example of how terrorists connected anonymously via the Internet.

B. Data mining:

Three States have written that online data mining is an important use of a medium by terrorists or for terrorist purposes. Al-Qaeda's terrorist guide captured in Afghanistan notes that "using publicly available sources, at least 80 per cent of all information obtained from the enemy can be collected.

5- Terrorist implementation:

One of the above categories has been used in the context of the use of the Internet for terrorist acts. For example, on the Internet, explicit threats of violence, including threats to use weapons, can be transmitted to cause fear, fear or panic among members of society. Or a group of communities. In many developing countries, these threats, if not implemented, can be considered a crime.

Cyber-Terrorism Definition:

Virtual violence was viewed as illegal assaults hostile to computers, telecommunications systems, data systems and saved data to intimidate the regime or its folks to promote societal or political goals. The assaults have led to violent acts hostile to persons, organizations, property or damage that have caused fear **(Denning, 2000)**. A new research considered that virtual terrorist action was an action carried out by means of data technology systems by administrative or non-administrative establishments against persons to intimidate a political or **(Macdonald et al., 2013)**, the broader approach to the definition of cyber terrorism concerns the simple meaning of terrorist action but the using the Internet; that is, cyber or virtual terrorism is any governmentally or communally driven usage of information technology by terrorists to carry out attacks against PCs Cat and systems information, leading to viciousness against non-combatant aims, producing injuries or massacre or severe injury or panic **(Samuel et al., 2014)**. The previous definition restricts objectives and widens the tool. Moreover, there is a different definition of the general sense of terrorism under local rule, practiced primarily in Canada, Australia, and New Zealand, was to state cyber-terrorism as three conditions besides the usage of technological equipment. The objective to carry out this action and impact or threaten the regime or the people; the existence of some kind of religious or political motives or objectives; the cause of harm, death or physical injury. Some studies agreed with this clarification and argued that most definitions of electronic terrorism share two main components : Political or ideological motivation or goal, intent to generate public danger or fear **(Macdonald et al., 2013)**.

Lewis **(2002)** defines cyber terrorism as a shutdown because of outbreaks on serious countrywide infrastructures or terrorization of citizens or government officials, using computer networks and techniques

Warren **(2002)** also defines cyber terrorism as an cyber-attack from cyberspace conducted with different and purpose-oriented internal and external networks. This

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

definition focuses on the basis of the attack that may come from within or out the association. It has been stated that terrorists' attacking is more risky when carried out using insiders because in-house extremists have great entree to systems and networks since they are employees (Jalil, 2003).

Cybercrime **(DCSINT, 2006)** has also been stated as the intentional usage or threat of subversive actions on computers and / or networks for the purpose of causing harm or social, ideological, religious, political or other similar objectives, DCSINT **(2006)** defines cyber terrorism as a new phenomenon or form of cybercrime that has its own objectives, characteristics and other attributes.

Samuel et al. **(2014)** defined cyber-terrorism differently by researchers and industry correspondents. In the early 1980s, cyber terrorism was seen as a combination of physical threats and a cyber-world involving computer interactions and online networks where users could exchange information in real time.

The motives of cyber terrorism:

In addition to the absence of one agreed definition of terrorism, there is a similar lack of unanimity regarding the causes of terrorism or the motives behind it. Several studies have identified some common behavioral and situational characteristics, perhaps causation, as a result of terrorism, and a specific analysis of case studies has led to suggested motives for individual historical acts, A report by Paul Gill, John Horgan, and Big Deckert on behalf of the UK Department of Security highlights the vast contradictions between individual cases of terrorism. First of all, 43% of wolf-only terrorism is motivated by religious beliefs. The same report notes that less than a third (32 per cent) suffer from mental health disorders before, while many others suffer from these problems at the time of arrest. At least 37% were living alone at the time of planning and / or carrying out the event, 26% were living with others, and no data were available for the remaining cases. 40 percent were unemployed at the time of their arrest or a terrorist event. 19 percent of personal experience are respected by others, while 14 percent of them have been verbally or physically assaulted **(Gill et al.,2014)**.

1- Intimidation:

Attacking "collaborators" is a strategy applied to make collaborators retreat from helping the government. This, as a result, leads to undermine the government control. Countries like Kenya, Cyprus, Ireland and Algeria all faced, during their quest for independence, such a strategy. **(Madigan,2017)**.

2- International attention:

This strategy was applied by Al Qaeda to attack the World Trade Center and the Pentagon in the United States on September 11, 2001. Al Qaeda used the attacks as weapon to draw the worldwide attention to unmanaged battles like the Dutch hostage crisis in 1975 and hijacking of Palestinian aircraft. **(https://en.wikipedia.org/wiki)**.

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
مارس 2021 العدد (19)
Volume (19) March 2021
IJOHSS

3- Social / internal status:

Ibrahim proposes that organizations of terrorism do not select terrorism for its political advantage. What really aspires terrorists to join the organizations is group unanimity with other individuals of the organization and not political programs or strategic objectives, which are regularly ambiguous and indefinite. **(Abrahms,2008)**.

4- Cultural tolerance of violence:

In addition, Michael Mossau illustrates the potential relations between the form of economy in the state and the belief related to terrorist acts. Several terrorists have a past of home violence **(Mousseau,2002)**.

5- The illegality of the state is seen:

Particular terrorists as Timothy McVeigh were driven by retaliation by a government for its acts against its residents **(https://en.wikipedia.org/wiki)**.

6- Religious views / intolerance:

From the viewpoint of Paul Jill, John Horgan and Big Dickert on behalf of the UK Department of Security, 43 percent of the wolf's only terrorism is the motivation for religious beliefs. The same report notes that less than a third (32 per cent) suffer from mental health disorders before, while many of them suffer from these problems when arrested. At least 37% were living alone at the time of planning and / or carrying out the event, 26% were living with others, and no data were available for the remaining cases. 40 percent were unemployed at the time of their arrest or a terrorist event. Many of them were chronically unemployed and constantly struggling to retain any form of work for a long period of time. 19 percent of self-experienced people are respected by others, while 14.3 percent of them have been verbally or physically assaulted **(Gill et al.,2014)**.

7- Psychological health:

Ariel Marari, a psychologist who has studied the psychological characteristics of suicide bombers since 1983 through media reports including biographical details, interviews with suicide families, and interviews with potential suicide bombers, concluded that they were unlikely to be psychologically normal **(Merari,2006),** In comparison to the economic theories of criminal behavior, Scott Atran found that suicide terrorists do not show any socially dysfunctional traits - such as parental attitudes, without friends, the unemployed - or suicidal symptoms. It means that they do not simply kill themselves because of despair or a sense of "nothing to lose **(Atran,2004)**.

8- nationalism

Although there is a common factor in terrorism is the strong religious belief, there are other factors such as culture, social and political that completely inhibit religion. For example, the motivation behind these Chechen terrorists is unique and unique. Many Chechens considered themselves secular freedom fighters, nationalist rebels seeking an independent secular state in Chechnya. Although there should be a distinction between Chechen national terrorists and non-Chechen fighters who have adopted the idea from abroad. Few Chechen fighters fought for jihad while most non-Chechen fighters did **(Janeczko,2014)**.

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

9- Family financial support

Another factor is the guaranteed assurances of financial stability to the representative's families, which are presented when they join a terrorist organization or complete a terrorist attempt. An additional grant is provided to families of suicide bombers **(Hoffman,2006)**.

Types of electronic breakthroughs used by terrorists:

For the sake of electronic protection, the individual needs to recognize the various methods in which his\her computer might be compromised and his privacy violated. In this section, we will discuss some of the known devices and procedures used by cybercriminals.

1- Hacking:

In simple words, hacking is done by an intruder by accessing your computer system without your permission. Hackers ("hackers") are essentially computer programmers who have an advanced understanding of computers and commonly misuse this knowledge for deceptive reasons. They are usually technology enthusiasts who have expert level skills in a specific program or language. For motives, there can be many, but the most common is very simple and can be explained by human inclination such as greed, fame, power, etc. Some people do so purely to review their experiences - ranging from relatively harmless activities such as modifying programs (even hardware) to carrying out the creator's unintentional tasks, while others want to cause destruction **(Jensen and Klein,2010)**.

Greed and bias may sometimes cause intruders to gain access to systems to take private banking information, company economic statements, and so forth. They also try and adjust systems so they can carry out tasks however they like. Hackers who display such damaging behavior are sometimes referred to as "crackers" also known as "Black Hat" pirates. However, motivated by intellectual curiosity, there are those who develop curiosity in computer hacking. Some corporations employ these computer devotees to discover failings in their security systems and assist repair them. Named as "white hat" hackers, these men fight contrary to the misapplication of computer systems. They try to access into network systems only to warn owners of defects. It is not always noble, although many do so for reputation also, to get jobs with major establishments, or just call them safekeeping specialists. "Gray Hat" is another word used to point to hacking actions that represent a cross between dark and white piracy **(Jensen and Klein,2010)**.

It is carried out through:

A- SQL injection:

SQL injection is a technology that enables intruders to manipulate the security susceptibilities of a program that controls a website. It might be employed to strike any kind of SQL databases that are not properly protected or protected. This procedure entails entering parts of the SQL cipher into the Web form input section - the most common usernames and passwords - to enable the intruder to access the backend of the site, or to a specific site, User account. When you write information of

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

the logon in the logon fields, this piece of information is usually transformed into a SQL order. This order verifies the information entered by you compared to the related table in the databank. You are granted access if your input data matches the data in the table, but you will get the type of mistake you could see once you entered the incorrect secret code if the data entered by you doesn't match. SQL injection is generally an added command which tries when you enter it in a network system to alter the database information to reproduce a efficacious login. Information like numbers or passwords of credit cards from insecure sites can also be retrieved in the same way **(Rubidha et al.,2016)**.

B- Stealing FTP passwords:

Interfere with Web sites is another quite known way. FTP password hacking benefits from the point that several webmasters save login information to their Web sites on their vulnerable computers. The scammer hacker looks for the target system to obtain the FTP login information, and then transfers these information to his or her inaccessible computer. After that s\he logs on to the Web site through the faraway computer and changes the Web pages the way s\he pleases **(Nelson,2016)**.

C- Cross-site scripting:

Also known as XSS (previously CSS, but retitled because of misperception with cascading style sheets). It is an extremely simple way to circumvent the security system. Cross-site scripting is vulnerable to attack because it is hard-to-detect gap in the web site. In a classic XSS attack, an intruder strikes a Web page with a script or malevolent client-side application. The script is automatically downloaded to and implemented by your browser when you visit this webpage. Attackers usually insert HTML, JavaScript, VBScript, ActiveX, or Flash into a program that is prone to tricking you into collecting private data. So in order for you to be able to shield your computer from malevolent intruders, you must invest in a worthy firewall in the first place. Piracy is done over a network, therefore it is crucial to keep your security safe during the use of the Internet **(Kaur and Kaur,2017)**.

2- Virus spreading:

Viruses are infecting computer programs which link or contaminate files or applications, and tend to link them to the other computers on a specific network. It disables the operation of your computer and affects stored information - either by changing it or by erasing it completely. Unlike viruses, warms do not requisite a host to hold on it. It is just a replication so it consumes all accessible memory in the system. The word "worm" is occasionally used to imply self-replicating malicious software (malware). These two words are frequently used exchangeably within the setting of viruses / mixed worms that control although the greatest invent of mankind, but the web is still a minefield of dangers **(Onlamoon,2011)**.

3- Logic bombs:

A logical bomb, known as "slag code" too, is a malevolent part of the code that is injected on purpose into a program to perform a malevolent mission when activated via a particular event. It is not a virus but it generally performs like one. It is hidden in the program where it remains intact until the specific circumstances are met. Malware,

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

like warms and viruses, mainly contains logical bombs that run at a specified load or at a predetermined time. The logical bomb load is unfamiliar to the program user, and the task performed by the unwanted. Codes of programs that are programmed for execution at a given time are called "time bombs". For instance, the ill-famed "13th Friday" virus that dominated host systems merely on particular times; "exploded" (repeated itself) every single Friday in which the thirteenth of the month occurred, causing the system to slow down **(Sharma,2017)**.

Logical bombs are generally used by discontented staffs employed in the IT division. You might have known of "disgruntled employee syndrome" where mad staffs who are separated by logical bombs use to erase their employers' databases, leak the network for a while, or even trade from within. The activates related to the implementation of logical bombs can be an exact time and date, a missing entrance from a database or a failure to place an order at the usual time, meaning that the person is no longer working there. Most logical bombs remain only in the network where they work. So in most cases, it is an internal function. This makes them easier to create and implement than any virus. To protect your network from logical bombs, you must continuously monitor data and effective anti-virus programs on every computer in your network **(Bist,2014)**.

4- Denial-of-Service attack

Through an explicit try, attackers attempt to deny the service to particular users of this service. It entails dumping the computer source with further applications than it can operate the bandwidth consumption available to it leading to overloading the server. This disables the resource (such as the web server) or significantly deactivates it so that nobody is able to access it. Via this method, an attacker could make the Web site invalid by transferring huge sums of traffic to the aimed site. A site may be shortly disabled or disabled, which in both ways may result in the system failing to connect effectively. The attacks of DoS violate the conventional usage rules of almost all ISPs **(Elleithy,N.D.)**.

5- Phishing

This method attempts to remove trusted data like numbers of credit cards and user name password sets by disguising as legal. Phishing is usually phishing e-mail. You may have received an email with links to authentic web pages. You may have seen it doubtful and did not open the link. Clever movement **(Purkait,2012)**.

6- Email bombing and spamming

It is hard to control this kind of attack due to the manifold addresses of the source and the automatic computers that send dissimilar mails to overthrow filters that detect spam. "Junk Mail" is a different kind of blasts via email. Unwanted mass messages are directed to so many users, randomly. Clicking on the links that you might find in spam messages can results in phishing websites. Spam can also enclose infected documents. The e-mail gets worse when the recipient receives an e-mail, causing all recipients to accept the original answer. Email addresses are collected by spammers through lists of the client, discussion channels, newsgroups, websites, and bugs that

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

collect computer documents of users and retail those to new spammers too. A huge volume of junk mail is directed to unknown e-mail addresses **(Nagamalai,2007)**.

7- Website jacking

In this method, the attacker dominates the Web site in a fraudulent manner. It may change the novel site content or even readdress the client to a parallel search page similar to fake control. The original owner of the website is no longer controlling the site so the hijacker can control the website for their own benefits. People have testified many cases in which the assailant requested a money, and even displayed indecent material on the site **(Jain and Shrivastava,2014)**.

8- Virtual hunting

Online chasing is a novel practice of cybercrime in the world when someone is followed up or tracked online. A stalker on the internet does not actually track his prey; he actually does this by tracking his virtual movement to collect data about the victim and hassle him or threaten verbal intimidation. It is a violation of a person's privacy on the Internet **(Hazelwood & Magnin,2013)**.

9- Information diddling

Information cheating is an unapproved change of information before or throughout PC system logon, and it is changed again once processing is completed. By resorting to this method, the intruder may change the predictable information and be hard to trace. That is to say, the authentic data to be used is altered either by somebody writing the information, a programmer's infection to alter information, a database IT worker, the application, or anybody else participating in the practice of forming, registering, encrypting, observing, transferring or transferring data **(Vadza,2013)**.

10- Personality Stealing and Credit Card Faking

Stealing of identity happens when somebody bargains the identity of yours and acts as if he is you yourself accessing your possessions like bank accounts, credit cards, and other advantages in the name of yours. Also other crimes might be committed by the fraudster in your name.. "Credit Card Fraud" is a broad name for identity stealing crimes where a scammer makes use of your credit card to finance his businesses. Credit card scam is personality stealing in its humblest formulation. Your previously accepted card that falls into the hands of somebody else is the most common credit card fraud is **(https://www.bartleby.com)**.

11- Rule back attack

"Salami attack" or "Salami scam" is a method in which Internet intruders take a few cash or possessions every time in such a way that there is no obvious change in total volume. The offender avoids huge numbers of wealth and by so doing collects a large amount over quite long period of time. The failure to discover the fraud is the core of this technique. The "round collection" method is the best standard technique. Most accounts are executed in a specific currency and curved to the nearest amount about part of the time and the rest of the time. There does not appear to be a net loss of the system, if a computer operator chooses to accumulate these extra portions from the

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

rupees into a distinct account. This kind of fraud is accomplished by cautiously transmitting money to the bank account of the offender **(Srikanth et al.,2017)**.

12- Piracy of Software

Due to the Internet and Torrent, nearly any program, song or movie from any source can be found for free. Internet piracy constitutes an essential part of our world that we all contribute intentionally or unknowingly. In this way, developers' profits are reduced. It is not limited to consuming the IP of someone else illegally but also transferring it to friends of yours which reduces the profits they deserve **(Harran et al.,2015)**.

Forms and patterns of cybercrime offenses (Razzo,2006):

1- Cyber Crimes: These crimes are as follows:

Hacking, destroying, destroying, modifying or tampering with data and information available on the Internet.

Fill in the address (link to the site or convert it to another website address.

Break email, grab it, and use it to impersonate others

Hacking or altering the information contained therein, or taking the highest information available to them such as user names, confidential numbers, contact addresses and use for illegal purposes, or selling them to beneficiaries (economic, commercial, political or security entities)

2- Cybercrime: This type of crime is as follows:

The penetration of websites and pages on the Internet for the purpose of espionage or eavesdropping on data and information (text, audio or visual) of the beneficiary of espionage (economic, commercial, political or security).

Send e-mail messages to Internet users that contain software files that have the ability to automatically transmit the information available on the user's device from files (text, audio or video). It also has the ability to send any information associated with the internet usage such as log of visits to websites and data entered by the user in the Internet sites as user name and password, in addition to the search words entered by the user in the global search engines

Use specialized software to hack computers connected to the Internet to spy on its information and data. There are many examples of these programs, most notably a program called Subseven.

One of the most important crimes under the name of electronic espionage crimes include:

A- Commercial and economic espionage crimes: espionage crimes that are intended to obtain economic and commercial information.

B- The crimes of spy, security, political and political: These are espionage crimes that are intended to obtain military, security or political information.

C- Cultural and educational espionage crimes: espionage crimes, which are intended to obtain cultural and educational information, such as espionage, shields, scientific studies and cultural and educational cooperation in countries.

3- Electronic financial and economic crimes: These crimes are as follows:

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

Fraud and seizure of banking information for bank customers through the Internet and exploitation of the purchase.
Access, capture and take advantage of quarterly credit card data online.
The establishment of a website and an online website that mimics the official websites of banks on the Internet with the aim of occupying the customers of these banks and taking possession of their bank statements. This kind of corruption is categorized by the sending of e-mails to Internet users in a region or country containing statements and the official logo of the bank and the official email address of your targeted target, in order to request the customers of these banks to the imaginary address of the bank, and then to enter their bank statements and The World Banks in the fight against this type of crime by warning not to receive messages containing the top fake addresses of their websites on the Internet, and to seek to understand the electronic disgraceful shame of their websites. And at the level of banks in Saudi Arabia. Most of the Saudi banks also received communications and e-mails from their customers. They received e-mails containing fake e-mail addresses for you banks. The purpose of the acquisition of card data and their exploitation in online purchasing is money laundering through the Internet: the use of illegal, locally and internationally (or irregularly) illegal funds that violate local regulations and to transfer, transfer, transfer, replace or trade online. E-commerce has contributed to the widespread spread of money-laundering offenses.
Examples include the following
D- The trafficking of illegal or illegal funds through the Internet through legitimate activities such as the circulation of shares and local and international currencies with a view to passing them and replacing them with legitimate and regular funds
E- The trafficking of illicit funds in illicit activities through the Internet such as drugs, gambling and pornography.

4- Electronic Terrorism Crimes:
This type of crime consists of the following: the creation or hosting of websites and pages on the Internet that call for terrorism, violence, extremism and discrimination among members of society and its various artists.
Methods of prevention of electronic terrorism (Qaisi,2014):
In light of the difficulties facing the investigation of cyber-terrorism crimes, the prevention of this crime is of great importance among men of jurisprudence and law as a means of combating electronic terrorism, in accordance with the rule of "prevention dirhams better than quintals of treatment". If we want to talk about ways to prevent cyber terrorism crimes, highlights into being the role that can be played by the official media and informal in the face of sites that promote the thought of extremist and terrorism on the Internet, The media plays a pivotal role important in the fight against cyber terrorism. The researcher believes that the role of the media should focus primarily on the humanitarian aspects of citizens and individuals in the countries. In this context, the media focuses on the victims of terrorism, their families and their preparation, focusing on the victims of children and women, so that the

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

media message in this regard is strong, effective and influential in the public and citizens. In this regard, we refer to a very important point: the need to create and establish a complete and absolute cooperation between the media and the Arab security forces of different names to confront cyber terrorism. Hence, the role of the security services in the event of monitoring such sites that feed extremist ideology and terrorism, to provide the security services and the media with all the information in this regard. In this regard, we emphasize that the role of the media should not be limited to media directed against extremist or terrorist groups, but should be extended to include controls on media coverage of terrorist or extremist groups. In the opinion of the researcher that such controls must be taken into account, but not limited to the following:

1- Do not exaggerate the expansion and dissemination of data and threats from terrorist groups through the Internet, what does this have negative effects in the hearts of the public, and fear may leave their rush to embrace their ideas and engage in their ranks

2- Failure to hand over to the media all information published by terrorists or extremist groups on the websites, and not to be considered as a basis of trustworthy data. The focus of the media on the victims of terrorism, children, women and the elderly, and the negative impact that this leaves on the families of the victims

3- To highlight the participation of the security agencies in the battle against electronic terrorist actions and to address it, and in a way that generates greater confidence among the public in the ability of the security services to deal with cyber terrorism and to promote the idea that the security services are the bastion that must be supported to eliminate this type of crime

4- Maximize the citizen's role in dealing with cybercrime crimes, and create a sense among the public that this role is no less important than the role of the rest of the state organs, but that the role played by the citizen outweighs the importance of other roles. Because the citizen is one of the most important groups targeted by electronic terrorism, which terrorist groups or extremists from behind the use of the Internet to lure and recruit to serve their interests and goals.

Methods of treatment of electronic terrorism (Qaisi,2014):

In this regard, we must mention that the efforts of the security agencies in countries in the prevention of electronic terrorism must go hand in hand with efforts to track these crimes, arrest and investigate them and refer them to the competent judicial authorities. In the opinion of the researcher that it is necessary to talk before the methods of investigating the crimes of electronic terrorism and address the need to have a legislative environment to address this type of crime. If there is no legislative cover or a legal text that imposes acts, it is impossible to talk about the mechanisms of investigating the crimes of electronic terrorism. The investigation in terms of origin is intended to reveal the circumstances and the nature of a crime committed. If the act to which the description of electronic terrorism applies is not criminal, there is no room

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

to talk about the investigation of this type of act. The researcher believes that the procedures of investigating electronic terrorism crimes are not very different from the procedures for investigating other crimes in terms of formal legal procedures and techniques used in detecting crimes and collecting evidence. However, the complexities associated with the crimes of electronic terrorism, the difficulty of proving them, and the collection of evidence, makes it difficult to investigate these crimes, and places considerable burdens on investigative teams. Electronic terrorist crimes do not end with the arrest of the perpetrator or the perpetrators. The crimes persist even after their discovery and the arrest of their agents for the presence of other elements that have not been arrested. Where those elements begin to act to conceal, conceal and destroy facts and evidence from which they condemn the perpetrators of their arrested accomplices. Not to mention the role that these groups can play in influencing the course of the investigation by fabricating artificial evidence leading the investigation in a certain direction, or by torturing investigators or witnesses.

Results:

Through this study, cybercrime has become a concern for countries that have become vulnerable to attacks by terrorists and extremist groups over the Internet. These groups have become terrorist activities from anywhere in the world. These dangers are exacerbated by the passing of day because modern technology alone is incapable of protecting people. Of electronic terrorist operations that have caused serious damage to individuals, organizations and States. Many States have sought to take measures and precautions to counter cyber terrorism, but these efforts are few and we still need more efforts to address this serious offense, The study, through theoretical reviews, reached a number of results, the most important of which are the following:

1- That electronic terrorism is generally targeting three different categories, the first category is the supporters or current and potential followers, the second category is the international public opinion, or the third category is the enemy masses.

2- Terrorist uses of technological means such as the Internet, smart devices, etc. are used to promote their beliefs, channel threat and intimidation messages, recruit, mobilize, plan, coordinate, fund, collect information, break accounts,

3- Information is an important role in all cybercrime. It is either used as an instrument and a means of misuse, in order to execute terrorists for their crimes or information is an end in itself, ie the crime is to steal, attack, change or permanently delete this information

4- Arab states are now seeking to join together to criminalize the use of information technology by terrorists to commit their terrorist crimes.

References

1. Abrahms, Max (2008). "What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy", International Security. 32 (4).

DOI: 10.33193/IJoHSS.19.2021.213

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal of Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (19) مارس 2021
Volume (19) March 2021
IJOHSS

2. Adetayo, J. O., S.A. Sanni, and M.O. Ilori (1999). The Impact of Information Technology on Product Marketing: A Case Study of Multinational Company in Nigeria, Technovation, Elsevier Science Ltd.
3. Aldhafferi, Nahier, Charles Watson and A.S.M Sajeev (2013). Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices
4. Aly, A., Macdonald, S., Jarvis, L. & Chen, T. M. (2016) Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization. Studies in Terrorism and Conflict. 2016, VOL. 0, NO. 0, 1–9.
5. Aly, Anne (2010). The Internet as Ideological Battleground, Edith Cowan University Research Online, As of 28/5/2019: http://ro.ecu.edu.au/act/9.
6. Atran, Scott (2004). "Mishandling Suicide Terrorism". The Washington Quarterly. 27 (3).
7. Bist, Ankur Singh (2014). Detection of Logic Bombs, INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCHTECHNOLOGY, 3(2).
8. Cleanitproject, About the Project, The Cleanit Project: Reducing The Impact of Terrorist Use of Internet, http://www.cleanitproject.eu/about-the-project/ (last visited 28/5/2019).
9. Comments of President Bush (2001), Delivered at the Department of Treasury, 7 Nov 2001. Available on-line at http://www.whitehouse.gov/news/releases/2001/11/20011107-4.html as of 28/5/2019.
10. Council of Europe Convention on Cybercrime (2001). Nov. 11, ETS No. 185.
11. Counter-Terrorism Implementation Task Force (CTITF) (2009). Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes.
12. DCSINT (2006) Critical Infrastructure Threats and Terrorism: Handbook Kansas, Deputy Chief of Staff for Intelligence.
13. Denning, D. E. (2000) Cyber terrorism, Testimony before the Special Oversight Panel on Terrorism. IN SERVICES, C. O. A. (Ed.) US, U.S. House of Representatives.
14. Elleithy, Khaled M. (N.D.). Denial of Service Attack Techniques: Analysis, Implementation and Comparison, SYSTEMICS, CYBERNETICS AND INFORMATICS Vol. 3 – No. 1 .
15. Enders, Walter, Gary A. Hoover, Todd Sandler (2014). “The Changing Nonlinear Relationship between Income and Terrorism.” Journal of Conflict Resolution.
16. Gill, Paul; Horgan, John; Deckert, Paige (2014). "Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists". Journal of Forensic Sciences. 59 (2).
17. Gupta, Dipak K. and Yiannis P. Venieris (1981). “Introducing New Dimentions in Macro Models: The Sociopolitical and Institutional Environment.” Economic Development and Cultural Change. 29.
18. Harran, Martin , Nigel McKelvey, Kevin Curran, Nadarajah Subaginy (2015). Software Piracy, Category: Cyber and Network Security Software Piracy.

DOI: 10.33193/IJoHSS.19.2021.213

19. Hazelwood, Steven D. & Sarah Koon-Magnin (2013). Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis, International Journal of Cyber Criminology, Vol. 7, Issue 2.
20. Hoffman, Bruce (2006), Inside Terrorism, 2 ed., Columbia University Press.
21. Holt, Tom, Joshua D. Freilich, Steven Chermak, and Clark McCauley (2015). Political radicalization on the Internet: Extremist content, government control, and the power of victim and jihad videos. Dynamics of Asymmetric Conflict, 8: 107–120.
22. https://en.wikipedia.org/wiki/Terrorism#Types.
23. https://www.bartleby.com/essay/Identifying-The-Identity-Theft-And-Credit-Card-PKVFUXZ9J5Q.
24. Internet Jihad: A World Wide Web of Terror, ECONOMIST, July 12, 2007 [hereinafter Internet Jihad] available at http://www.economist.com/node/9472498.
25. Jacobson, Michael (2010). Terrorist Financing and the Internet, Journal Studies in Conflict & Terrorism Vol. 33, Issue 4.
26. Jain, Neelesh, Vibhash Shrivastava (2014). "CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY", International Journal of Computer Application Issue 4, Vol. 1.
27. Janeczko, Matthew (2014). "'Faced with death, even a mouse bites': Social and religious motivations behind terrorism in Chechnya".
28. Jensen, Bill and Josh Klein (2010). HACKING WORK, Breaking Stupid rules FOR SMART RESULTS, Printed in the United States of America.
29. Kaur, Daljit, Parminder Kaur (2017). Cross-Site-Scripting Attacks and Their Prevention during Development, IJEDR, Vol. 5, Issue 3.
30. Khan, M. S. (2005). Martyrdom Video [Motion picture]. Retrieved from http://www.liveleak.com/view?i¼af8_1181469330.
31. Kiser, Steve (2005). Financing Terror An Analysis and Simulation for Affecting Al Qaeda's Financial Infrastructure, Published by the RAND Corporation.
32. Labi, N. (2006). Jihad 2.0: With the loss of training camps in Afghanistan, terrorists have turned to the Internet to find and train recruits. The story of one pioneer of this effort—the enigmatic "Irhabi 007"—shows how. The Atlantic.
33. Lewis, J. (2002) Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. United State, Center for Strategic and International Studies.
34. Lieberman, Ariel Victoria (2016). Terrorism, the Internet, and Propaganda: A Deadly Combination, Journal of National Security Law & Policy, Vol. 9:95.
35. Macdonald, S., Jarvis, L. & Chen, T. (2013) A Multidisciplinary Conference on Cyberterrorism: Final Report, Cyberterrorism Project Research Report. A Multidisciplinary Conference on Cyberterrorism. Swansea University.
36. Macluhan, Marshall (1978). Interview of Marshall Macluhan with the Italian newspaper Il Tempo, February 19, 1978.
37. Madigan, Michael L. (2017). Handbook of Emergency Management Concepts: A Step-by-Step Approach. CRC Press.
38. Merari, Ariel (2006). "Psychological Aspects of Suicide Terrorism," in Bruce Bongar et al., Psychology of Terrorism. New York: Oxford University Press.

DOI: 10.33193/IJoHSS.19.2021.213

39. Ministry of Security and Justice (2013). Reducing terrorist use of the Internet, The result of a structured public-private dialogue between government representatives, academics, Internet industry, Internet users and non-governmental organizations in the European Union. http://www.rijksoverheid.nl/venj.
40. Mousseau, Michael (2002). "Market Civilization and its Clash with Terror". International Security. 27 (3).
41. Nagamalai, Dhinaharan (2007). Novel Mechanism to Defend DDoS Attacks Caused by Spam, International Journal of Smart Home Vol. 1, No. 2.
42. National Money Laundering Strategy (2003). Departments of the Treasury and Justice. July 2003. Available on-line at www.ustreas.gov/offices/eotffc/publications/ml2003.pdf as of 28/5/2019.
43. Nelson, Anthony (2016). Sandnet++ - A framework for analysing and visualising network traffic from malware, Information Security Group, Royal Holloway, University of London, Egham, Surrey, TW20 0EX United Kingdom.
44. Norman, Don A. (1988). The Design of Everyday Things. New York: Basic Books.
45. Onlamoon, Nattawat, Jaydip Das Gupta, Prachi Sharma, Kenneth Rogers, Suganthi Suppiah, Jeanne Rhea, Ross J. Molinaro, Christina Gaughan, Beihua Dong, Eric A. Klein, Xiaoxing Qiu, Sushil Devare, Gerald Schochetman, John Hackett, Jr., Robert H. Silverman, and Franc¸ois Villinger (2011). Infection, Viral Dissemination, and Antibody Responses of Rhesus Macaques Exposed to the Human Gammaretrovirus XMRV, JOURNAL OF VIROLOGY, Vol. 85, No. 9.
46. Parker, Tom, and Nick Sitter (2016). "The Four Horsemen of Terrorism: It's Not Waves, It's Strains." Terrorism and Political Violence, vol. 28, issue 2.
47. Purkait, Swapan (2012). Phishing counter measures and their effectiveness – literature review, Information Management & Computer Security, Vol. 20, No. 5.
48. Qaisi, Isser Mohammed Attia (2014). Modern Mechanisms for Reducing Recent Crimes "Electronic Terrorism and the Methods of Confrontation", Scientific Forum "Crimes Emerged in the Light of Regional and International Changes and Changes During the period from 2-4 / 9/2014, Amman, Jordan.
49. Qaisi, Isser Mohammed Attia (2014). Modern Mechanisms for Reducing Recent Crimes "Electronic Terrorism and the Methods of Confrontation", Scientific Forum Crimes that were created in light of regional and international changes and changes during the period from 2-4 / 9/2014, College of Strategic Sciences, Amman, Jordan
50. Razzo, Muzaffar Hassan (2006). Information security, preliminary legal treatment, Journal of Law and Security, Academy of Dubai, No. 1.
51. Rotella, Sebastien (2013). Syria's Jihadi Migration Emerges as Top Terror Threat in Europe, Beyond, PROPUBLICA, (July 24, 2013, 11:56 AM), http://www.propublica.org/article/ syrias-jihadi-migration-emerges-as-top-terror-threat-in-europe-beyond.
52. Rubidha Devi.D , R.Venkatesan, Raghuraman.K (2016). A STUDY ON SQL INJECTION TECHNIQUES, International Journal of Pharmacy & Technology, Vol. 8, No.4.
53. Samuel, K. O., Osman, W. R. S., Al-Khasawneh, Y. & Duhaim, S. (2014) Cyber Terrorism Attack of the Contemporary Information Technology Age: Issues,

DOI: 10.33193/IJoHSS.19.2021.213

Consequences and Panacea. International Journal of Computer Science and Mobile Computing (IJCSMC), 3.
54. See, Also, Quann Li (2005). "Dies Democracy Promote or Reduce Terrorist Incidents?" Journal of Conflict Resolution. 49.
55. Sharma, Bobby (2017). A Pragmatic Way of Logic Bomb Attack Detection Methodology, Indian Journal of Science and Technology, Vol 10(20).
56. Soriano, Manuel R. Torres (2008). Terrorism and the Mass Media after Al Qaeda: A Change of Course?, Athena Intelligence Journal Vol. 3, No 1, pp. 1-20.
57. SRIKANTH T N, AISHWARYA J S, IRSHAD JABEEN, SHRUTHI B, BHOOMIKA G Y (2017). EXPLICIT STUDY ON CYBER CRIMES USING INTERNET, International Journal of Management and Applied Science, Vol.-3, Issue-9.
58. The Clarion Project. (2014). The Islamic State's (ISIS, ISIL) Magazine: All of the issues of the Islamic State's glossy propaganda magazine 'Dabiq,' named after a key site in Muslim apocalypse mythology can be found here.
59. Tyson, Laura (2001). "It's Time to Set Up the Global War on Poverty." Business Week.
60. UNITED NATIONS (2018). Introduction to International Terrorism, Counter-Terrorism 1, University Module Series.
61. Vadza, Kejal Chintan (2013). Cyber Crime & its Categories, INDIAN JOURNAL OF APPLIED RESEARCH, Vol. 3, Issue 5.
62. Venieris, Yiannis P. and Dipak K. Gupta (1986). "Income Distribution and Sociopolitical Instability as Determinants of Savings: A Cross-sectional Model," Journal of Political Economy. 94.
63. Walzer, Michael (1977). Just and Unjust Wars: A Moral Argument with Historical Illustrations. Basic Books.
64. Warren, A. C. (2002) Security Against Cyber Terrorism.
65. Willis, H.H., A.R. Morral, T.K. Kellyand J. Medby (2005). Estimating Terrorism Risk. MG-388-RC. Santa Monica, CA, RAND Corporation.
66. Wilson, Samuel F., Teresa M. Lao and Ernesto Escobedo (2016). Terrorist Experts' Perceptions of How the Internet Has Shaped International Terrorism, Journal of Information Assurance & Cyber security, Vol. 2016.

DOI: 10.33193/IJoHSS.19.2021.213