E.ISSN: 2661-7404 La revue académique des chercheurs juridiques et politiques P.ISSN:2571-9971
Année : 2022 Vol : six The second Page : 797-808

The use of information and communication technologies in terrorism

Baadji abdennour *
Faculty of law, Algiers-1-
Abdennour.bdj@gmail.com

Received: 02/02 /2022 Accepted: 06/06 /2022 Published: 15/09/2022

Abstract:
With the spread of globalization in societies and the continued flow of fighters to the organization "ISIS" and Al-Qaeda and its associated groups, Security Council Resolution 2322 (2016) binded states to criminalize the use of ICT, especially the Internet in facilitating terrorist acts and inciting the commission or the recruitment of criminal acts. The objective of this paper is to analyse and review the effectiveness of the current national response to cyber terrorism, this paper concluded that despite the criminalization in compliance with the Security Council resolution, cyberterrorism must be subject to a special law.

Keywords: cyberterrorism, foreign terrorists, ICT, penal law, globalization, electronic means.

Introduction:

The growing role of cyberspace in society has opened up new opportunities, a growing number of individuals and groups are looking to use it, the internet has also changed—and continues to change—the very nature of terrorism. it's well suited to the nature of terrorism and the psyche of the terrorist. In particular, the ability to remain anonymous makes the internet attractive to the terrorist plotter. Terrorists use the internet to propagate their ideologies, motives and grievances as well as mounting cyber-attacks on critical infrastructures.

Modern terrorism has rapidly evolved, becoming increasingly nonphysical, with vulnerable "home grown" citizens being recruited, radicalized, trained and tasked online in the virtual and ungoverned domain of cyber space.

Security Council Resolution 2178 (2014) was passed, which marks a "turning point in efforts undertaken at the global level to reduce the threat of foreign terrorist fighters", it was adopted unanimously, therefore obliged all countries to enact laws criminalizing travel or attempting to travel for terrorist purposes, and requiring countries to suppress and prevent the organization, recruitment, transfer and equipping of foreign terrorist fighters, also to financing their activities, we can define the cyberterrorism is a convergence of cyberspace and terrorism, It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to

* **Corresponding author**

intimidate or coerce a government or its people in furtherance of political or social objectives.

Finally, the national security machinery of governments has no choice but to find ways to confront and overcome these threats if they are to flourish in an increasingly competitive and globalized world. *so, the general question is: how the Algerian domestic law act with the phenomenon of use the ICT in terrorism?*

THE FIRST TOPIC: ICT a tool of terrorism

Modern terrorism depends on information and communication technology, given the opportunities it provides that do not exist in the real world, as follows;

FIRST REQUIREMENT: Definition of ICT and cyberterrorism

we try to determine the definition of ICT as well as cyber terrorism, for purpose to know the nature of concepts.

Firstly: **ICT is a technical or legal concept?**

Societies rely on technologies to organise and administer themselves, offer services to citizens, educate and communicate, economic globalisation is enhanced by new technologies, which provide opportunities in international markets.

Multinational enterprises, and also small and medium companies, are carrying out their businesses more easily, without spatial barriers. Technologies allow them to invest in new activities or enter new markets and free them to invent new ways of presenting themselves and offering their services/goods. A boundless, unlimited flow of information, together with the possibility to establish international networks, facilitates the reduction of economic costs, and direct and indirect risks, this is no different from what ICT allows criminals to do. They use new technologies to communicate, to organise themselves better, to widen the spectrum of their businesses, to update their modus operandi and techniques, and to avoid law enforcement risk[1].

The ICT revolution can be defined as a veritable ‘Pandora’s box’ of criminal offences and challenges, it have been known by several names, it described as the new information and communication technologies NTIC, Then the word “new” was deleted from the label to become information and communication technology ICT, then with the beginning of the use of the Internet in the nineties, it was shortened to the name TI**,** in addition ICT is sometimes used synonymously with IT (for information technology); however, it is generally used to represent a broader, more comprehensive list of all components related to computer and digital technologies than IT.

ICT is also used to refer to the convergence of audiovisual and telephone networks with computer networks through a single cabling or link system. There are large economic incentives to merge the telephone network with the computer

network system using a single unified system of cabling, signal distribution, and management. it is an umbrella term that includes any communication device, encompassing radio, television, cell phones, computer and network hardware, satellite systems and so on, as well as the various services and appliances with them such as video conferencing and distance learning, it also includes analog technology, such as paper communication, and any mode that transmits communication[2].

it posed a great danger to international peace and security, in this regard the Security Council had the resolution 2161 (2014)[3], that express the increased use, in a globalized society, by terrorists and their supporters, of new information and communications technologies, in particular the Internet, to facilitate terrorist acts, as well as their use to incite, recruit, fund or plan terrorist acts.

In the law n° 09-04 related to "Special rules for the prevention and control of crimes related to ICT"[4] the first item of Article 02, select the means by which these crimes are committed is the information system or a wired communication system, It concluded that the narrow concept of the term "information and communication technologies" is limited to two basic points or concepts, this is what the same article determine that: " B. Information system: any separate system or group of systems connected to each other or linked, one or more of which automatically processes data in implementation of a specific program," and that: "F. Electronic Communications: Any correspondence, transmission, or reception of various signs, signals, writings, images, sounds or information by any electronic means."

Consequently, the legislator hadn't a specific or clear definition of this term because it's considered among the technical terms.

Secondly: Cyber terrorism a complex concept

The term "cyberterrorism" appeared in the mid-eighties, which is consisted of "the Internet" and "terrorism" through a study by the researcher "BARRY COLLIN", he found a difficulty to define the terrorism phenomenon, and the computer role in the terrorist act, then it has been used widely, as it combines two of the century's greatest fears: cyberspace and terrorism[5].

In the year 1980, the term was used to refer to the cyber-attacks that affect the economy of the United States of America by the computer, these risks were demonstrated through studies, perhaps the most prominent of which is the report of the American National Academy of Sciences on computer security, which stated that the United States of America is in danger, due to the increasing used on computers, it's found in the management of power delivery, communications, aviation, financial services, and storing vital information, therefore it can be to a cyber-attack biggest than a bomb[6].

E.ISSN: 2661-7404 La revue académique des chercheurs juridiques et politiques P.ISSN:2571-9971
Année : 2022 Vol : six The second Page : 797-808

In the early 2000s, Cyberterrorism has been a highly fashionable topic, therefore the events of September 11, 2001 had the effect of increasing interest of it, many scientific books and articles deal with this theme, for example, a search on engines for scientific articles reveals a thousand articles written on the subject since 2001, and it reported in the media.

In fact, according to the majority of specialists dealing with the subject cyberterrorism is one of the threats that are often considered as emerging. However, its ill-defined and still relatively obscure, even an opaque character, makes cyberterrorism a threat that is much more floating than tangible.[7]

sooner or eventually, according to many specialists, terrorists will turn to information technology to launch cyberattacks against corporations, another motivation for attacks on computer networks is to further a political, religious or ideological cause Such attacks have the potential to cause considerable harm, possibly disrupting essential services such as water, power, hospitals, financial systems, emergency services, air/shipping control and the like[8].

Given differing views on the meaning of 'terrorism', it is not surprising that the term 'cyberterrorism' is ill-defined, it may be divided into two categories. The first, simply describes those situations where technology is used to facilitate the activities of terrorists, secondly Technology may also be utilised in raising finance.

SECOND REQUIREMENT: Methods of using technology in terrorist activities

Criminal groups operate illegally through corruption, exploitation, violence and commerce with a view to obtaining the power, influence and financial gain, It is neither a specific regulation of their activity, but can vary from hierarchies to clusters and networks, the Organized crimes usually include; drug, migrant smuggling, human trafficking, money laundering and smuggling, As a result of the use of the Internet, New techniques have been developed that have increased opportunities for criminal activity, as well as for spreading threats and glorifying violence.

Online organized crime and cyber terrorism are becoming more important[9], I find a several type of terrorist activities through ICT, I review in what is actually cyberterrorism, according to the definitions that have been clarified, it represented by the attacks that are implemented over the Internet and that target information technology systems or physical property and human lives, Then what cannot be considered a cyberterrorism in the narrow sense, which is the traditional use of Internet, it appears to be harmless and offers a many advantage to the terrorists through the cyberspace.

Firstly: means of cyberterrorism

E.ISSN: 2661-7404 La revue académique des chercheurs juridiques et politiques P.ISSN:2571-9971
Année : 2022 Vol : six The second Page : 797-808

1-Cyberattack: it constitutes what's called the “cybercrime” and their offenders are cybercriminals[10]**,** the most of them are motivated to defeat the information system and experience all problems related the security, they are curious about technology, This does not prevent the existence of groups has a highly competence that use the cyber-attacks as their financial income.

In the recent years, statistics indicate an emerging phenomenon in the field of cybercrime, according to modeling carried out by McAfee[11] and the Center for Strategic and International Studies, it noted that the cost of cybercrime on the global economy increased from $445 billion to $600 billion between the years from 2014 to 2018, and the trend of criminal activities related to government-sponsored bank robberies, the ransom crimes and cybercrime contributed to this increase as a service.

The use of anonymity services and theft of personal data and intellectual property, for example, increasingly targeting mobile phones, Because of its numbers and permanent connection to the Internet, and it’s like a gold mine of information.

Cybercrime poses unprecedented challenges with traditional crimes, it including the use of modern techniques by cyber criminals such as the artificial intelligence, and the multiplication of means of attack resulting from the increased interest in anonymity through the secret web that allows cyber criminals to be unpunished[12].

Online fraudsters can take the victim's data through ransom programs, the personal information of owner is encrypted and its unread, in order to claim money for a password that gives him access to his data, this techniques used to hide identity and provides the payment in virtual currency such as bitcoin[13], the "reasonable ransom" was carefully chosen[14], it led to an explosion of the data extortion, so we can be said that cyber-attacks constitute a huge income for the terrorist to actually finance his terrorist networks.

On the other side, Cyber-attacks constitute a threat to the critical infrastructure, is generally represented in water treatment plants, oil refineries, power systems, gas pipelines, etc. which uses the "SCADA" systems to collect the data and control these systems, because it is difficult for humans to perform these services in the industrial plants and facilities, there may be a production lines or nuclear plant control.

The originally of "SCADA" system was designed to be closed systems means it’s not connected to the Internet, However, increasingly was found connected to the Internet, and there are many malicious programs that threaten these systems, such as Stuxnet, which first appeared in 2009[15], and Dooku is the son of Stuxnet although it has the same code but does not contain any code that can affect

industrial control systems, Its mission seems to be the collect of information such as design documents from the same systems that Stuxnet attacked, and Flame was first identified in 2010, it uses social engineering to trick people into downloading by spoofing Windows Update Service using fake certificates, then users click on the update link and get infected with the virus, which is an attack toolkit, It's an advanced attack kit with electronic espionage has a capability to take a screen footage on, and recording audio conversations, secret numbers, storing packages on the network, it designed to steal information.

Also, there is "Shodan" a search engine launched in November 2009 to detect Internet-connected devices, its able to detect a large number of industrial control computers, which was in fact accessible from the internet, and not only a cyberweapon, but it's a factor that facilitates cyberterrorism[16].

2- Dissemination of terrorist content: Technology has influenced the means of online attack to become more developed, At the same time, Internet has created the possibility of disseminating information to all without any cost, or censorship of content, terrorists are not just using the Internet, Hence, terrorists use the internet not only to launch attacks, but also to spread the "war of ideas", and their beliefs, they exploits the information infrastructure and finance the extremism[17], so the terrorist groups exploit the Internet through websites , to spread extremism and display their criminal operations by recording their attacks for the best results, the element of suspense and enthusiasm is often accomplishment with a mixture of military songs, they are filmed simultaneously from different angles, the subject for distribution to the media and websites and the production of tables glorifying activities and its procedures, the dissemination of anti-extremist messages that constitute incitement to terrorism is the most effective way to combat it, in addition to prohibiting incitement of terrorism in domestic law, its observed that the use of the Internet may be in practice more effective strategy as a positive means of countering such incitement rather the trying to restrict terrorism[18].

Participants in the Riyadh conference on the use of the Internet to fight the call of extremist violence recommended a need to disseminate counter-narratives through all relevant media channels, including social media, to counter the appeal of extremist messages.

Secondly: Traditional use of the Internet

The internet is a means of accessing to a dangerous source for terrorists it seems that some harmless sites provide valuable and substantial information to them where they can uncontrolled, for example, individual contacts between members of terrorist groups via the cyberspace, therefore is different from mobile communications wherever the content is sent without encode, so that local

government agencies keep up instantly hear if the hidden parties are at present under "wiretapping" surveillance, However, the private Internet conversation is encrypted and easy. From this, e-mail typically allows them to communicate efficiently, for example, the principal offenders of the September 11 attacks acted by this effective way, they opened multiple accounts on largely anonymous email services like Hotmail[19].

THE SECOND TOPIC: criminalizing the use of ICT in terrorism

There is a several United Nations resolutions warn the potential danger of internet use by terrorists, especially after 11 September 2001 attacks in USA, according to the Article 02 of Act No. 09-04 on ICT and combat them is specified in key paragraph (a), that: "Offences of infringing on systems for the automatic processing of data specified in the Penal Code and any other crime or it committed easily through a system or electronic communications. ", the text includes a broad legal wording include cybercrime and crimes committed through an electronic means, which is cyber terrorism, referring to the Penal Code, we find that the last clause of Article 87 bis 11 adopted the term "use of information and communication technologies," which is specific to the commission of terrorist acts stipulated in paragraphs 1, 2 and 3 of the similar article, and we treat them as follows:

FIRST REQUIREMENT: Use of ICT to travel terrorist activities

We explain the danger of using technology, as well as the criminalization of the Algerian legislator to these criminal ways, as follows:

Firstly: The danger of using ICT by terrorists

Terrorists acquire the means provided by technology to diversifying their activities, making them efficient, they can be implemented correctly with fewer individuals and better results, and thus one person recruit more recent members, Network technologies characterized by diversity and plurality are largely driven by consumers and commercial markets around the world. It is unpractical to keep these branches of knowledge out of the hands, these technologies can simply be bought off the shelves, From this, the elevated risk of terrorists and their ardent supporters using media technologies to spread extremist ideology that leads to the modern terrorism of all kinds, and to recruit others to commit acts and incite them to do so, through channels including the Internet and financing and facilitating the travel of foreign fighters and the activities they typically attempt after that, Resolution 2178 (2014) adopted by the Security Council in its preamble to Express the grave concern over the acute and growing threat posed by foreign terrorist fighters and defines them as: " individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the

providing or receiving of terrorist training, including in connection with armed conflict, and resolving to address this threat",[20] it underlines the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law.

Secondly: The position taken by the Algerian legislator

In the penal law the article 87 bis 11 identified many forms of terrorist activities, including the first paragraph is criminalization of travel and stipulated that: "... every Algerian or foreigner residing in Algeria legally or illegally travels or attempts to travel to another country for the purpose of committing, planning, preparing, or participating in terrorist acts", And in the last paragraph: "he uses the information and communication technologies to commit the acts mentioned in this article," therefore ICT used to facilitate the travel to do terrorist activities, it specified the scope of the criminalization of travel for the purpose of terrorism, such a thing applies to the Algerian and the foreigner who commits the crime or use the ICT to commit it.

The ISIS, Al-Qaeda and associated groups leads to implement Resolution 2178 (2014) to limit this spread by preventing and suppressing the recruitment, organization, transfer, or equipping of foreign terrorist fighters and financing their travel and activities, a foreigner is considered a legal resident if he has been in possession of a resident card by the mandate of his residence for a period of two years, which shows that he has proven his actual, habitual and permanent residence in Algeria, and a non-resident who is considered to be transiting the Algerian territory or residing in it for a period not exceeding ninety days.

we point out that the Algerian legislator had to define the term training or receiving training, as it was included in the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism[21], where Article 03 in the first clause states: " For the purpose of this Protocol, "receiving training for terrorism" means to receive instruction, including obtaining knowledge or practical skills, from another person in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence".

SECOND REQUIREMENT: use of ICT for the facilitation of terrorist activities

like a means of facilitating travel, through the provision and collection of funds, and financing, as well as organization.

Firstly: **ICT is a means of saving and collecting funds or financing for travel**

Article 87 bis 11 criminalizes the acts of "saving", "collecting" and "financing" in paragraphs 2 and 3, saving money express the finding of sources from which money is collected, while the collecting means compiling of money from different sources.

In addition, the person who collects the funds not the provider of it, for that there is a necessity to criminalize each act separately. On the other hand, saving and collecting funds are acts that fall under the general concept of "finance", if we compare the "saving" is a direct means, while "collection" is an indirect means of financing, this last is confirmed by Article 05, first paragraph of the Additional Protocol of COE, which defined; "funding travelling abroad for the purpose of terrorism means providing or collecting, by any means, directly or indirectly, funds fully or partially enabling any person to travel abroad for the purpose of terrorism".

we can say that what was mentioned in paragraphs 2 and 3 previously is a direct employment of the resolution 1373 (2001)[22], this last adopted under Chapter VII of the United Nations Charter, it's a binded rules urge to: (a) Prevent and suppress the financing of terrorist acts; (b) Criminalize the wilful provision (saving) or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts.

In fact, there is no definition to concept "finance" in the penal law, so its end for the special laws in the field of criminalization.

In this regard, Prevention and Combating Money Laundering law and Terrorist Financing express in Article 03, that: "Anyone who provides, collects, or conducts willingly, in a legitimate or illegal manner, by any means, directly or indirectly, funds for the purpose of using them personally, wholly or partially, to commit or attempt to commit crimes described as terrorist acts or with his knowledge...the financing of terrorism is an act of terrorism".

Secondly: ICT is a means of organizing or facilitating travel

Article 87 bis 11 in the third paragraph criminalizes the organization and facilitation of travel to commit terrorist activities, however, it did not specify the meaning or scope of the activities of organizing and facilitating, therefore it refers to the general principal of criminal law related to the crime contribution by the aid or assistance.

On the contrary the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism in the first paragraph Article 06, defines; "organising or otherwise facilitating travelling abroad for the purpose of terrorism", it means any act of organisation or facilitation that assists any person in travelling abroad for the purpose of terrorism.

Conclusion:

I concluded in the research paper that the Algerian legislator criminalized the use of information and communication technology by terrorists in implementation of the Security Council resolutions, and despite this there are still many legal voids raised by the texts that dealt with the phenomenon, and Crimes. Algeria has not yet ratified the Budbast Convention on cyber.

The results i summarize are as follows:

- Cyber terrorism is one of the newly crimes that use cyberspace to achieve the purposes of classic terrorism through the use of information and communication technologies.
- Cyber terrorism is a global crime that transcends the borders, for this a difficult to detect the cybercriminals, they are usually specialists in the field of information technology or have some knowledge in dealing with information networks.
- The Algerian legislator did not set a specific or clear definition of "information and communication technologies" because it is considered among the technical terms,
- Algeria applied the Resolution 2178 (2014) by including Article 87 bis 11, it criminalizes the use of ICT in terrorism by terrorists and their supporters to spread extremist ideology, and recruiting others to commit acts of terrorism and inciting them, through channels, including the Internet, financing and facilitating the travel of foreign fighters.

Hence, the study made the following recommandations :

- Enacting a general law related to terrorism and criminalizing all acts of cyberterrorism.

-The need to ratify the Budapest Convention on Cybercrime, due to the development of cybercrime.

-Adopting a prevention approach by pressuring technology companies to remove the extremist content and disrupt extremist networks on the Internet in order to create space for alternative messages, and employ young people at the forefront of the war on terrorism, as well as obstructing terrorist travel by collecting data related to passenger name records, its use to prevent cross-border terrorist travel.

- Awareness of youth about the danger of violent and extremist content and their participants in the war on terrorism through seminars, scientific research and advertising on various television channels.

Références :

[1] . Savona, Ernesto U., ed. Crime and technology: New frontiers for regulation, law enforcement and research. Springer Science & Business Media, 2004, p08.

[2] . Wikipedia, Information and communications technology, Available at: https://en.wikipedia.org/wiki/Information_and_communications_technology, accessed10 June 2021.

[3] . UN Security Council, S/RES/2161 (2014), on threats to international peace and security caused by terrorist acts, available at: https://www.undocs.org/S/RES/2161%20(2014), accessed 15 June 2021

[4] . Law 09-04 of August 5, 2009, "the special rules for the prevention and control of crimes related to ICT, Algerian Official Journal, No. 47, issued on August 16, 2009, p. 05.

[5] . COLLIN, Barry C. The future of cyberterrorism: Where the physical and virtual worlds converge. Crime and Justice International, 1997, 13.2: 15-18

[6] . National Research Council, C. O. R. P. O. R. A. T. E. (1991). Computers at risk: Safe computing in the information age. National Academy Press, p07.

[7] . Fortin, Francis. Cybercrimes et enjeux technologiques : Contexte et perspectives, Presses internationales polytechnique, 2020, p285.

[8] . Clough, Jonathan. Principles of cybercrime. Cambridge University Press, 2015, p11

[9] . RUGGIERO, Vincenzo (ed.). Organized crime and terrorist networks. Routledge, 2019, p60.

[10] . Donn B Parker went on to consider people who misuse the information intentionally They cover a range of criminals Although it is impossible to describe these criminals in one definition, However, there are some interesting criminal phenomena, that we need to know in order to be effective in protecting of information, and many of these characteristics distinguish cybercriminals from other criminals, it referred In the word S.K.RAM, as an abbreviation to skills, knowledge, resources, authority, and motives.

[11]. A security and antivirus software company.

[12] . Fortin, Francis, Op. Cit, p302.

[13] . A digital currency, usually abbreviated by (BTC), its prohibited to trade the virtual currencies in Algeria, according to the Article 117 of the Algerian Financial Law of 2018 stipulates that: “It is prohibited to buy, sell, use and possess virtual currency. Virtual currency is the one that Internet users use over the Internet, and it is distinguished In the absence of a physical support such as coins, banknotes and payments by check or bank card.

[14] . Fortin, Francis, Op. Cit, p304.

[15] . MACKINNON, Lachlan, et al. Cyber security countermeasures to combat cyber terrorism. In : Strategic intelligence management. Butterworth-Heinemann, 2013. p240.

[16] . ibid. p243.

[17] . GIACOMELLO, Giampiero. Bangs for the buck: A cost-benefit analysis of cyberterrorism. Studies in conflict & terrorism, 2004, 27.5, p387.

[18] . United Nations, General Assembly, A60/426, p78. Available at: https://undocs.org/pdf?symbol=ar/A/60/426, accessed 9 June 2021.

[19] . BRUNST, Phillip W. Terrorism and the internet: new threats posed by cyberterrorism and terrorist use of the internet. In: A War on Terror? Springer, New York, NY, 2010. p73.

[20] . United Nations, General Assembly, S/RES/2178 (2014). Available at: https://www.undocs.org/en/S/RES/2178%20(2014), accessed19 June 2021.

[21]. Council of Europe, Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, Available at: https://rm.coe.int/168047c5e, accessed20 June 2021.

[22] . United Nations, General Assembly, S/RES/1373(2001), Available at: https://undocs.org/en/S/RES/1373(2001), accessed23 June2021.

Bibliography List setting:

-First: legal texts

1. Law 09-04 of August 5, 2009, "the special rules for the prevention and control of crimes related to ICT, Algerian Official Journal, No. 47, issued on August 16, 2009.

-Second: books

1. Savona, Ernesto U., ed. Crime and technology: New frontiers for regulation, law enforcement and research. Springer Science & Business Media, 2004.
2. Fortin, Francis. Cybercrimes et enjeux technologiques : Contexte et perspectives, Presses internationales polytechnique, 2020.
3. Clough, Jonathan. Principles of cybercrime. Cambridge University Press, 2015.
4. RUGGIERO, Vincenzo (ed.). Organized crime and terrorist networks. Routledge, 2019.
5. MACKINNON, Lachlan, et al. Cyber security countermeasures to combat cyber terrorism. In : Strategic intelligence management. Butterworth-Heinemann, 2013.
6. GIACOMELLO, Giampiero. Bangs for the buck: A cost-benefit analysis of cyberterrorism. Studies in conflict & terrorism, 2004, 27.5.
7. BRUNST, Phillip W. Terrorism and the internet: new threats posed by cyberterrorism and terrorist use of the internet. In: A War on Terror? Springer, New York, NY, 2010.
8. National Research Council, C. O. R. P. O. R. A. T. E. (1991). Computers at risk: Safe computing in the information age. National Academy Press.

- Third: Articles

1. COLLIN, Barry C. The future of cyberterrorism: Where the physical and virtual worlds converge. Crime and Justice International, 1997, 13.2: 15-18.

-Fifth: Websites

1. Wikipedia, Information and communications technology, Available at: https://en.wikipedia.org/wiki/Information_and_communications_technology, accessed10 June 2021.
2. UN Security Council, S/RES/2161 (2014), on threats to international peace and security caused by terrorist acts, available at: https://www.undocs.org/S/RES/2161%20(2014), accessed 15 June 2021
3. United Nations, General Assembly, A60/426, p78. Available at: https://undocs.org/pdf?symbol=ar/A/60/426, accessed 9 June 2021.
4. United Nations, General Assembly, S/RES/2178 (2014). Available at: https://www.undocs.org/en/S/RES/2178%20(2014), accessed19 June 2021.
5. Council of Europe, Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, Available at: https://rm.coe.int/168047c5e, accessed20 June 2021.
6. United Nations, General Assembly, S/RES/1373(2001), Available at: https://undocs.org/en/S/RES/1373(2001), accessed23 June2021.