ESKİŞEHİR TEKNİK ÜNİVERSİTESİ BİLİM VE TEKNOLOJİ DERGİSİ
B- TEORİK BİLİMLER

Eskişehir Technical University Journal of Science and Technology B- Theoretical Sciences

International Conference on Natural Sciences and Technologies
Iconat Special Issue 2021

2021, Vol:9, pp. 113-128, DOI:10.20290/estubtdb.1021324

TERRORIST USE OF CYBER TECHNOLOGY

Mehmet Nesip OGUN [1*], Serdar YURTSEVER [2], Murat ASLAN [3], Mohamed ELBURASI [4]

[1] International Relations, Faculty of Business Administration, University of Mediterrenean Karpasia, Nicosia, TRNC
[2] International Relations, Faculty of Business Administration, University of Mediterrenean Karpasia, Nicosia, TRNC
[3] Political Science and International Relations, Faculty of Humanities and Social Sciences, Istanbul Sabahattin Zaim University, Istanbul, Turkey
[4] International Relations, Faculty of Business Administration, University of Mediterrenean Karpasia, Nicosia, TRNC

ABSTRACT

The risk posed by terrorist use of cyber technology and cyber terrorism have been of great concern to politicians, decision makers, security officials. This article studies terrorist use of cyber technology and cyber terrorism along with history of cyber-terrorism. Moreover some concepts such as between cyber-crime, cyber-terrorism, cyber-warfare and hactivism will be analysed. Furthermore, the challenges faced by international organisations in tackling cyber terrorism will be discussed; measures introduced in some countries to address cyber terrorism treats are presented as well as discussions on the present and the future treat posed by cyber terrorism and terrorist use of cyber technology.

Keywords: Cyber terrorism, Cyber space, Cyber security, Cyber technology, Cyber attacks

1. INTRODUCTION

Technology has become a key factor leading to the use of internet by terrorists' groups and those that support them for carrying out various heinous acts such as financing, recruiting, making propaganda, training, inciting people to carry out acts of terrorism, and the collection and dissemination of information for the purpose of terrorization [1].

Combating terrorism is among the most alarming and important security aspects of any national state. Terrorism is an old phenomenon with a history of over twenty centuries [2], dating back to 48 AD, a period when Sicarii-Zealots, a Jewish resistance group, attacks the Romans. They infiltrated the roman cities so as to assassinate and kidnap Roman soldiers and any Jewish collaborators [3]. Few years back, the horrific events on the United States of America on 11th September 2001 and others across the globe by a group willing to inflict harm on innocent civilians in order to attain their agenda is of a great treat to the world.

The dependency on internet in the 21st century as a channel of communication can be seen throughout the globe. Through the use of internet people have been connected with one another around the globe also business transactions have been simplified through e-commerce. With the aid of the internet, accessibility to a vast amount of information be it past or present by the people has become very easy. Connecting to family, friends, colleagues and loved ones is simplified. Despite the various advantages of the internet, it has also become a tool that is being used by terrorists in spreading their ideologies and also to cause great havoc to the general public and to harm political structures over the world. A new treat called "Cyber terrorism" has evolved from the convergence of this physical and virtual world.

*Corresponding Author: mehmet.gun@akun.edu.tr
Received: 11.11.2021 Published: 24.12.2021

This complex term "Cyber terrorism" was first coined by a senior research fellow by name Berry Collin in the 1980s at the Institute for security and Intelligence situated at California [4]. Two concepts can be derived from the term cyber-terrorism: the first, "cyber", which refers to cyberspace, and the second, "terrorism", which will be discussed in the next chapter. Thus, assumption can be made that cyber-terrorism is a kind of terrorism that is executed in cyberspace [5-6]. Cyberspace refers to the internet and on larger scope computer networks [7-8]. It is a "globally interconnected network of digital information, communication and infrastructures" [9]. Various actions such as online spread of propaganda, distortion of information and the planning and execution of terrorist attack through computer networks are all actions used to describe cyber-terrorism.

2. TERRORIST USE OF INTERNET

Terrorists and terrorist organizations have been exploiting Internet for different purposes. Although different researchers categorize this usage in different ways, in this study main 6 categories have been identified [1]. These categories are:

- Propaganda
- Financing
- Training
- Planning
- Communication
- Execution

2.1. Propaganda

Among the major uses of the internet to terrorist organizations is the spread of propaganda. Through this medium, terrorist organizations are able to provide ideological as well as practical instructions, guides, and to encourage and justify their activities. These could be in the form of pamphlets and magazines, video and audio messages as well as animations made by the terrorist organizations or those in support of their course. Most of these contents find their way easily through the internet under the fundamental human right protection by the international law which gives a person the right to freedom of speech thereby allowing a person to advocate his or her opinion and share contents that might be regarded harmful by others. These rights do not include the dissemination of information that are harmful to national security and those that are likely to cause harm to individuals or a certain community. Also, the distribution of certain pornographic materials is prohibited by this law, a move which is regarded to be in interest of the general public so as to protect certain vulnerable groups [10].

With the aid of the internet, contents that might be screened via the traditional means of disseminating information, such as local television and radio channels that usually go through the steps of verifying the authenticity of information, editing and excluding provocative contents before there are passed to the general public, are seen to find their way to the general public because these restrictions in the form of screening are usually not present with regards to the internet, thus, promotions of violence and the spreading of material such as video games and footage that simulates terrorist acts in order for the targeted audience to emulate the virtual terrorist is achieved easily.

With the presence of platforms such as Facebook, Twitter, YouTube and Instagram, contents encouraging violence and promoting extremist views can be distributed to millions of viewers within a small interval of time. With the help of internet search engines, identification and retrieval of terrorist material has become easy.

The manner and intents in which this propaganda is carried out is of great treat. These propagandas are usually aimed at a wide range of audiences and objectives. Propaganda usually in the form of displaying accomplishments, pride and show casing extremist goals are aimed at actual or potential supporters for radicalization, recruitment and incitement purposes as well as conveying success achieved in the attacks carried out to some of their financial supporters.

Through the spread of rumors and wrong information as well as the use of violent threats, video, audio and images of violent acts, terrorist organizations do manipulate a person's belief in certain aspects of moral and social values and also increase an individual's level of anxiety which also leads to mistrust, thereby spreading fear and causing panic in a population. The targeted audience of these propagandas include the directed viewer/listeners as well as the indirect viewers / listeners that is, those whom are affected by the publicity generated by the contents of the propaganda. Achieving political goals is usually the target of such propaganda by the terrorist organizations in the international realm.

2.2. Financing

The internet plays a role in financing acts of terrorism by terrorist organizations and those supporting their course. Means by which terrorist organization adopt in gathering founds can be;

- Direct solicitation: this is the use of chat groups, websites, targeted communications as well as mass mailings to source donations from supporters.
- Charitable organization channels
- e-commerce
- online payment tools

through the use of online payment facilities such as credit cards, electronic wire transfer and others transfer of found is being made easy. Other ways terrorist organization do utilize online payment systems is through theft of identity, wire fraud, card theft and auction fraud [10].
Terrorist organizations do use cover fronts such as establishing shell cooperation, charities and so on where there do solicit online donations and diverts the funds gotten to execution terrorism operations.

2.3. Training

The internet is also used by terrorist organization as a training ground. This could be in the form of the platform in spreading online audio or video materials, online manuals as well as providing information and advices in various languages with details of how to make explosive devices, making use of firearms and other sophisticated combat equipment. Through this medium, technique and strategies is being shared among members and affiliate in order to execute an act of terrorism [10].

Online manuals providing details of how to hack and counter the activities of intelligence agencies and how to safeguard online illicit activities and communication by using encryption tools and other techniques are made available by terrorist's organizations. Also, due to the interactive nature of online platforms, terrorist organizations find it easy to create network comprising of people from different backgrounds and geographical locations for exchanging tactical and instructional material.

2.4. Planning

The internet has become a key tool in planning acts of terrorism due to the ability is has to bridge borders and distances thereby easing communication between several parties, and of the vast amount of information that is available in cyberspace thereby. With the aid of the internet, terrorist organizations can easy pinpoint their targets and how to attack those targets easily. The steps involved

in planning such attacks might range from acquiring information on attack methods to collecting open source and information of a proposed target.

2.5. Communication

Terrorist organizations over the years have become very powerful at the exploitation of communication technologies to communicate anonymously for the planning of acts of terrorism. Terrorists do make use of online e-mail account for virtual or electronic 'dead dropping' of messages. That is, unsent draft messages are created so as to leave minimal electronic trace. These massages can be accessed through the internet terminals by many individuals with specific passwords.

Also, there is now availability of enhanced technologies such as anonymizing software and encryption tools developed to prevent or minimize the tracing of internet message originator, recipient or contents of messages. Some of these tools are designed to hide the unique Internet Protocol (IP) address, thereby making. Messages could also be hidden in images, a technique known as Steganography [10].

A vast amount of information is usually published by individuals as well as organizations on the internet. Organizations usually do so in order to enhance their interaction with the public and to promote their activities. Through the use of internet search engines, terrorists may gain access to inadequate protected messages from millions of websites. Also, access to applications such as Google Earth and availability of detailed logistical information the likes of real-time closed-circuit television footage whose primary purpose is for legitimate means might be used by terrorists to gain access to maps and satellite imagery so as to gain access to their targets.

With the advent of social media such as Twitter, Facebook, YouTube and others, individuals do publish amount of sensitive information on the internet be it knowingly or unknowingly with the intention of providing news and updates for their audiences, such information might be used by terrorists for carrying out terrorist act [10].

2.6. Execution

For the execution of acts of terrorism, elements of the various categories described above might be employed. The internet can serve as an outlet of disseminating treat of violence as well as causing fear or panic in a population. Many states consider the acts of issuing such treat even when not executed as an offence. In China, the circulation of a fabricated treat of the use of chemical, biological, radioactive material and other weapons for the purpose of disrupting public order is considered as a criminal act [10].

3. CYBERTERRORISM

Threats that arise in the cyber space cannot be limited to damage to physical assets, information theft and espionage. The use of the Internet, which is used as a means of communication, for the purposes of information distortion and propaganda also causes indirect damages [11].

A lot has been documented on the subject of cyber-terrorism, even do a unique acceptable definition for it is lacking and this comes not as a surprise considering the fact that it is a subset of terrorism. One of the obvious source of defining cyber-terrorism is the dictionary, next can be regarded as the academia perspective as well as security agencies.

Professor Dorothy Denning a professor at the Naval Postgraduate School put forward a definition of cyber-terrorism, a definition that has become well known, where she put forward the following requirement in order to define cyber-terrorism:

- Participants are non-state actors.
- Computer based attacks targeted on IT-based infractions.
- Victims are either societies or governments.
- A form of terrorism limited to cyberspace.
- Rather than physical properties or persons, disruption or destruction is done against digital property [12].

Professor Denning's definition of terrorism excludes states sponsored terrorist organization.
Another academia by name Maura Conway described cyber-terrorism as the union between fear of technology and fear of terrorism.

The U.S. Federal Bureau of Investigation defined cyber-terrorism as any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents" [12].

In the year 2010, Robert Mueller, director of the FBI, in his RSA Cyber Security Conference speech in San Francisco raised the following points in regards to cyber-terrorism [13]:

- By 2020, the online presence of al-Qaeda will be equivalent to their physical presence.
- Cyber-space is used by extremists for Recruitment, radicalization as well as other things.
- Cyber-space is used to incite terrorism as well as acts of terrorism.
- A lot of extremist websites promote violence by targeting an undisclosed number of captive audience.
- Through posted videos, viewers of extremist website acquire knowledge of building bombs as well as bio-weapons.
- Social network has play a significant role in linking terrorist plotters and plan.

North Atlantic Treaty Organization defined NATO cyber terrorism as: "A cyber-attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal" [14]. This originates in a NATO document, but the report goes on to concede that due to its non-physical nature, accurate definitions of cyber terrorism are not easy to produce. The NATO Office of Security does recognize that it is becoming increasingly feasible to exploit the many vulnerabilities of cyber space, especially with regard to those services that rely on computer and communication networks.

Adapting the Continental European framework view of defining terrorism to the definition of cyber-terrorism, the three requirements (structure, harm principle and elements) discussed above has to be met for it to be classified as a form of terrorism in Continental European framework perspective.

3.1. Cyber-Terrorism in Terms of Structure

Continental European framework approach is of the view that in contrast to individual cybercrimes (such as computer espionage executed by an individual) or that executed by a group on an ad hoc basis (such as three people executing a computer sabotage: one person develops malware, the second access a database and the last person makes use of the malware in destroying specific data.), cyber-terrorism is a well organized crime.

Some authors are of the view that acts of cyber-terrorism can be executed by an individual [15] a view that is strongly opposed by others and are of the view that cyber-terrorists act under the umbrella of an organization [16].

Cyber-terrorism poses a great "danger" due to its organized nature [17] and consequently, its punishment is severe in comparison to other cyber-crimes. The following doctrine is used to determine whether a crime is associated to cyber-terrorism organization [18].

i. The existence of a set of members.
ii. Access to resources.
iii. The strength to sustain and execute operation over time.

3.2. Cyber-Terrorism in Terms of Structure

In regards to harm principle, cyberterrorism act is directed on institution, state or national interest [19-20] and not on individual interest. Acts of cyber-terrorism that harm individual interest such as life or loss of property is just an indirect effect but not the main goal which is usually directed at democratic settings. Some situations that can be derived from the harm principle ranging from that of lower magnitude to that of higher magnitude are as follows:

First, the treat is only on the collective interest of the order of democratic constitution. This situation exists only when an individual is a member of a cyber-terrorist group with a criminal agenda. In this situation, these interests are at risk when there are indications that any such act on the order of democratic constitution will be dealt with vehemently [16].

Second, is the violation of the collective interest of the order of democratic constitution. An example of such occurrence is the use of propaganda via media in destabilizing a political regime where the health or life of others is put in grave harm's way using credible or plausible treats [21].

Third, the collective interest of the order of democratic constitution is violated as much as one or more individual interests. A case study is when a cyber-terrorist organization in order to carry out a specific political agenda takes control of an airplane and make it collide with another, leading to the loss of lives of the passengers.

3.3. Cyberterrorism in Terms of Elements

Acts of cyber-terrorism comprises of instrumental elements as well as teleological elements

- Teleological element is of the view that;

  - Cyber-terrorism is committed to altering the order of constitution or toppling the government that was elected through legitimate means [16].
  - Cyber-terrorism is politically motivated [12] and disseminate political message [22-23], that is, "it is a radical form of political violence" [21].

- Instrumental element: is of the view that;

  - Cyber-terrorism act must be carried out in a way that instil great fear in the minds of the people [16], thereby sending out the message that anyone at any place could fall a victim of terrorism [24].
  - Act of cyber-terrorism adapt various means such as targeting buildings such as hospital, schools or crops resulting in deaths of people or serious injuries [25-26].

Structure, harm principle as well as elements (instrumental and teleological) are jointly required in a crime for it to be considered as an act of cyber-terrorism [27]. From the definitions presented above it is apparent that the term cyber-terrorism lacks a single universal acceptable definition but do have some common characteristics.

3.4. Cyber-Crime and Cyberterrorism

It is important to differentiate between cybercrime concept in general and cyber-terrorism concept [12]. The key difference between these acts is that cyber-terrorism is very severe in comparison to other cybercrimes thus, just as not all crimes are regarded as terrorism [28] so also not all cybercrimes are regarded as cyber-terrorism. In other to have a clear understanding of the differences we decipher between cybercrime and computer crime.

3.4.1. Computer crime

In a broad sense, computer crimes are traditional crimes (crimes such as sexual abuse or fraud [29] that are committed via internet or computer mechanism while in a strict sense [30] are mainly directed on software which encompasses crimes such sabotage of computer and computer fraud.

3.4.2. Cybercrimes

These crimes are committed via internet [29]. In contrast to computer crimes which are carried out "through" or "against" computer system, cybercrimes are always executed through cyberspace. These two categories are not mutually exclusive and thus, can coexist. Therefore, spread of child pornography via the internet constitute a computer crime as well as a cybercrime in a broad sense whereas, the act of destroying data from computer system via cyberspace constitutes a cybercrime as well as a computer crime in strict sense [21].

3.4.3. Differences between cyberterrorism and cyber-attack

The intent of the perpetrator(s) is the main difference between cyber-terrorism and a cyber-attack. Financial or other motives such as political motives are usually the reasons for cyber-attacks while cyber-terrorism attacks are always social, religious or politically motivated. Thus, the rationales behind the attacks are distinct even do, the metaphysical activity might be the same [31].

3.4.4. Distinction between cyberterrorism and cyber-warfare

Despite cyber-terrorism and cyber-warfare employing same tactics in their mode of execution with similar goals, yet there is a difference between the two. As differentiated by professor [6]:

- Cyber-terrorism is carried out by non-state actors.
- Cyber-warfare is carried out within the context of a declared war.
- Cyber-warfare is carried out by a government's military.

"Cyber-warfare constitutes the conduct of military operations by virtual means" [32].

The same agenda nation -states pursue using conventional military force is achieved through the use of cyberspace. This could be a nation preventing other(s) to achieve certain advantages over itself or by setting itself to achieve advantages over others. In the past, there had been reports that republic of China was lunching cyber-attacks which are targeted on Taiwan's communications, transportation and operational security as well as public utility in order to cripple the infrastructure of Taiwan and to keep

the island's economy and government at a standstill. Cyber-warfare as noted above is in the interest of a particular nation states and like cyber-terrorism, it tends to result in the massive destruction of property and the loss of life and sometimes these cold be non-combatant civilians which is usually termed as collateral damage not as in the case of cyber-terrorism where innocent civilians are intentionally targeted.

3.4.5. Distinction between cyberterrorism and hacktivism

It is important to differentiate "Hacktivism", a term that was coined by Denning [12] in order to describe the convergence of hacking (here hacking refers to activities conducted online and covertly in order to manipulate, reveal and to exploit vulnerabilities in software and computer operating systems) and political activities, from cyber-terrorism. The four main weapons at the disposals of hacktivists are:

- Virtual sit-in and blockade: the cyber version of physical sit-in blockade is called virtual sit-in or blockade, a great amount of traffic is generated by political activist by coordinating visit to websites so that other users cannot access it, thus disrupting normal operations while winning publicity through the media for the cause of the protesters. "Swarming" is a term used to describe a situation when a designated site is attacked by a large number of individuals. Swarming amplifies hactivists' efforts [12].

- Automated e-mail bombs: e-mail bomb campaigns also known as "ping attacks" are situation whereby, a target is bombarded with thousands of messages at once. In 1997, San Francisco based internet service provider (ISP) which goes by the name The Institute for Global Communication (IGC) that hosted the web pages of Euskal Herria, a publication edited by supporters of the Basque separatist group Homeland and Liberty (ETA). The goal of the attacks is for the ETA site to be pulled from the internet. In order to achieve this, the hackers bombarded IGC with thousands of spurious e-mails via hundreds of different mail relays, clogged IGC's web page with bogus credit cards orders, spammed IGC customers and staff accounts, and threatened to use the same method against other organizations. The Euskal Herria site was pulled down by IGC few days later [12].

- Web hacks and computer break-ins: this method is used by a lot of cyber-protesters where by the gain accesses to stored information, financial information and communication facilities, and others through hacking into the computers. An instance of such a case is the Emergency Response Team Coordination Centre (CERT/CC), a federally funded research and development center govern by Carnegie Mellon University which in the year 1997 reported upto 2.134 computer security incidents such as hacks and break-ins, an number which catapulted to 21,756 in the year 2000 and as at early 2001 almost amount to 35,000. Over five hundred thousand e-mails were received by CERT/CE in 2003 and over 900,000 hotline calls reporting incidents or requesting information. The same year witnessed the report of at least 137,529 computer security incidents. These reported numbers can be regarded to be insignificant due to the facts that most incidents are not reported to CERT/CE or some other third party. Also, each reported case might correspond to an attack that involve hundreds of victims. In 2002, hackers were able to gain access to bank account information, home addresses and Social Security numbers of 265,000 employees. Several factors can lead lead to the increase in computer-based attacks, such factors can be the rapid growth of the internet, increase in the numbers of potential targets and attackers and the increased in sophisticated software hacking tools that can pave way to devastating attacks [12].

- Computer viruses and worms: These are malicious codes that have the ability to affect computers and propagate over networks of computers. They can have a devastating impact. An instance of such a devastating impact is the Code Red worm which in 2001 affected about a million servers with an estimated damage of 2.6 billion dollars to computer software, hardware and networks.

Also another devastating instance is the year 2000 I LOVE YOU virus that affected over twenty billion users of internet and caused damages which has be estimated to the tone of billions of dollars. The spread of the Code Red virus and the I LOVE YOU virus were not politically motivated. In some instances attacks were politically motivated. One of such politically motivated attack is that targeted at NATO member-states in retaliation to its move to evict the Serbian forces from Kosovo. Businesses, academics, and public entities in NATO member-states were attacked with virus-laden e-mails from a range of Eastern European countries.

- The year 2002, witnessed a major DoS attack which targeted the root server that is responsible for providing road maps for most of the world-wide internet communication. The incident, which according to most experts was executed by concentrating the power of many computers against a single network i9n order to prevent it from operating. Due to the safe guards built into the internet's architecture, ordinary internet users experienced no outages or slowdowns, however, if the attacks had persisted, it would have resulted in grievous damages to the world wide electronic communications. World giants companies the likes of Yahoo, Amazon.com and e-Bay, and a host of others had been targeted.

- "Hactivism" despite being politically motivated does not amount to cyber-terrorism, their aim is not to spreat terror,kill or maim but rather the aim is to protest and disrupt. Sometimes the lines between hactivism and cyber-terrorism do blurs, especially in situations where terrorist organizations hire or recruit hactivists or a situation whereby, hacktivists decide to increase the magnitude of their attacks by attacking systems that are responsible for the operations of critical elements of the national infracstructure, such as emergency services and electric power networks [12].

3.5. Cyber-Attacks

Cyber-attacks as discussed in the previous chapter can be seen as a deliberate use of computer networks in order to launch an attack. It is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network. Such attacks are carried through activities such as hacking, computer viruses and so on in order to cripple the functioning of a computer systems, servers as well as underlying infrastructure.

3.6. Cyber-Terrorist Targets

Infrastructures that are of prime target to cyber-terrorist organizations include:

- Medical
- Financial
- Gas
- Transportation
- Communication
- Offshore oil rig
- Power
- Water

By targeting one or more of the infrastructures listed above, the efficiency of businesses and operation can be severely crippled by a cyber-terrorist organization [13].

Sensitive data is another target of cyber-terrorist organizations. By gaining access to data of organizations such as banks, federal agencies and that of social media, sensitive information can be stolen, exposed and posted online by terrorist organizations thereby, causing social turmoil, putting security agencies as well as other persons at financial or physical risk.

3.7. Reasons for the Attraction of Cyber-terrorism by Terrorist Organizations

Modern terrorists find cyber-terrorism attractive due to several reasons of which few are presented below:

- First, cyber-terrorism in comparison to traditional terrorist method is cheaper. A personal computer with an online connection is all what the terrorist needs, the buying of weapons such as guns and explosives are not required. Through a wireless connection, a telephone line or cable viruses can be delivered.
- Second, in comparison to traditional terrorism methods, cyber-terrorism is more anonymous. Security agencies find it difficult to track down a lot of cyber-terrorists because most of them hide their identities by using nicknames, or by logging unto a website as an unidentified guest. And due to the lack of presence of physical barriers the likes of checkpoints to navigate, no customs agents to outsmart and no borders to cross.
- Third, the numbers of targets are so much. The computers and computer networks of public utilities, governments, individuals, private airline, and so on could be the targets of cyber-terrorist. These vast amounts of potential targets to the cyber-terrorist make it possible to locate exploitable vulnerabilities. As indicated by several studies, critical infrastructures such as emergency services and electric power grids are vulnerable to cyber-terrorist attacks due to the fact that they possess a highly complex computer system which makes it extremely difficult to eliminate all weakness.
- Fourth, one of the appealing futures of cyber-terrorism that makes it so appealing to the terrorist is that it can be conducted remotely. Less physical training, risk of mortality and so on is required by the terrorist thus, making it easier to retain and recruit followers by terrorists' organizations.
- Fifth, cyber-terrorist has the ability to generate great media coverage due to its potential to affect a large number of people which is something of great importance to terrorist organizations [12].

3.8. Tools used by Cyber-Terrorist Organizations

Means by which cyber-terrorist carried out their attacks comes in various forms; these attacks can either be untargeted or targeted.

3.8.1. Untargeted attacks

- Water Hole: This is a situation whereby terrorist organizations compromises original website by deploying fake website with the intention of attacking visiting users.
- Phishing: This is a case where by terrorist organizations obtain private information of a user or an organization by through the use of fraudulent emails.
- Ransomware: This is a case where by terrorist organizations denies the users access to a system or infect the system through the encryption of files and then requesting a ransom.
- Scanning: This is a case where by terrorist organizations capitalize on vulnerabilities in systems or specific internet networks in order to deploy attacks on a wider scale to attack at random [33].

3.8.2. Targeted attacks

- Distributed Denial of Service (DDoS): this is a case where by mass amount of packet requests usually from a Botnet is deployed to a network or website so as to overload the system thereby, preventing legitimate users access to the site.

- Spear-Phishing: The main difference of these attacks with Phishing mentioned earlier is that it is targeted at individual or organization.
- Zero-day: Bespoke exploitation of a system with specific vulnerability not yet identified by the author.
- Supply chain: This is a situation whereby terrorist organizations attack lunch an attack against an element of an organization before its arrival [33].

3.9. Cyber-Terrorism: A look into the Current and Future Scenario

Cyber-terrorism has gained a huge amount of publicity and exaggeration from all angles be it the media, academics as well as the political realm even do, it is difficult to point out the occurrence of a single cyber-terrorism attack which took place over the years. Thus, the question to be answered is why the great amount coverage, publicity and exaggeration on the issue of cyber-terrorism. A reason given by Denning is that "Cyberterrorism and cyberattacks are sexy right now…[Cyberterrorism is] novel, original, it captures people's imagination". Another reason is that the mass media hardly differentiates between cyber-terrorism and hacking thereby, exaggerating the cyber-terrorism and hacking thereby, exaggeration cyber-terrorism threat.

Several horrific scenarios were described by Collin in his vision of "The Future of Cyberterrorism" as follows:

- Banks, stock exchanges, internal financial transactions will be disrupted by cyber-terrorists. The key: all confidence will be lost in the economic system by the people of a country. Would attempt be made by the cyber-terrorist to gain access the Federal Reserve structure or equivalent? Unlikely, due to the reason that immediate arrest will follow. In addition, a truck parking outside the building will not go unnoticed. However, in regards to cyber-terrorism attacks, the cyber-terrorist may be sitting in another continent while halting the economic system grid of a nation which will result to a great destabilization.
- A cyber-terrorism will attack the next generation of air traffic control system resulting in the collision of two large civilian aircraft. This is a realistic scenario, since the cyber-terrorist will also crack the aircraft's in-cockpit sensors. Such can also happen in the case of rail lines.
- Formulas of medication at pharmaceutical manufacturer will be remotely altered by cyber-terrorists which will result to an unimaginable loss of lives.
- The pressure in the gas lines may then be changed by cyber-terrorists, leading to a valve failure, and a block of a sleepy suburb detonates and burns. Likewise, the electrical grid is becoming more vulnerable [12].

The National Security Agency (NASA) in 1997 performed an exercise code named "Eligible Receiver" which presented a chilling result. The exercise began when NASA officials briefed a thirty-five person "Red Team" of NASA computer hackers on the ground rules. There were requested to hack and disrupt United State national security system. Their main target was to hack into the United States Pacific Command in Hawaii, which is responsible for all military contingencies and operations conducted in the Pacific theatre, including the tension-wracked Korean peninsula. The Red Team members were given the permission to make use of only software tools and other hacking utilities that can be accessed through free download from the internet from hacker websites. The Red Team was allowed penetrations to various networks of Pentagon except the arsenal of secrete offensive information warfare tools and also they were to abide by U.S laws.
The Red Team posed as hackers hired by North Korean intelligence service, dispersing around the country they began digging their way into military networks and with ease, they find their way through. By using "brute-force cracking" (a trail-and-error method of decoding encrypted data such as encryption keys and passwords by trying all possible combinations) they were able to gain access to mapping networks and logging password and the subtler tactic of social engineering. Dozens of

critical Pentagon computer system were accessed by the Red Team. There were able to create legitimate user accounts for other hackers, reformat server hard drives and scramble the data, delete accounts belonging to authorized officials, or simply shut systems down. There were able to gain access through network defences without difficulty, after which they could conduct DoS attacks, read or make small changes to sensitive e-mail messages, and they were able to disrupt telephone services. All these were done by the Red Team without being traced or identified [12].

All those that were involved were stunned by the result of this exercise. The U.S military's command-and-control system for the entire Pacific theatre of operations was would have been crippled by the Red Team using hacking tools that were available to anybody on the internet. A situation that was appalling from military perspective. Much broader vulnerability was revealed by this exercise. NSA officials during the course of analysing the accomplishing of the Red Team discovered that much of the private-sector infrastructure in the U.S, such as electric power grid and the telecommunication, could easily hijacked using the same techniques and tools.

Increased focus on profitability as well as deregulation has forces companies and utilities to move most of their operations to the internet in order to improve efficiency and reduce cost. The energy industry as well as a lot of other industrial sector by creating inadvertent internet link (both wireless and physical) between the digital crown jewel of a lot of industrial process and their cooperate network (the supervisory control and data acquisition (SCADA) system have made their cooperate network vulnerable. The actual flow of gas and electricity as well as other critical functions in many industrial control settings such as delivery and water purification system, wastewater management facilities, chemical processing plants, and a host of manufacturing firms is managed by this system. The ability of a terrorist to gain access to alter, control or disrupt the monitoring and command functions performed by these systems could threatened regional as well as national security.

New vulnerability that could pave way for cyber-attacks are being discussed all the time: with the growing number of "software holes" (software security flaws that allow malicious hackers to exploit the system) on infrastructures across the globe one great fear is when those that are inclined to commit acts of terrorism possesses a significant knowledge to inflict high impact damage, or the terrorist themselves designing computer software for government agencies. One of such occurrence happened in the year 2000 when Japan's Metropolitan Police Department made the announcement that Aum Shinryko cult that was responsible for the Tokyo 1995 subway attacks that resulted in the death of twelve people and injuring six thousand more. Also members of the Aum Shinryko cult have developed software for no less than ten government agencies and eight Japanese firms. They worked as subcontractors for other firms, making it almost impossible for the end users to know the developer of the software they bought.

In 2007, Idaho National Labs made a demonstration which shows how a 27 ton power generator can be made to ripped itself apart and blow up by using the internet if the right set of commands were set in a project which was called Aurora. In other for a person to realize the consequence of this type of attack one has to know that generators are:

- Very expensive
- No longer made domestically
- Need a lead time of about three to four months when ordering new ones

Realizing what destroying a generator at a power plant encompasses, the potential for a cascading effect now begins to be fully realized [12].

What if cyber-terrorists could take control of transportation infrastructure? Planes, trains, automobile could be made to have a dead on collision. As a result of an automated system failure which leads to

lack of detention of a train already on track, two Washington D.C metro trains collided with one another, a disaster which was as a result of human error. What will be the impact if a terrorist was to have control over the automated system?

In the year 2000, a hacker by name Maroochy Shire in Queensland Australia as mentioned earlier was arrested and jailed for dumping raw sewage via taking control of the automated waste management control system into local parks and water out of revenge for not being given a job. This act resulted not only in foul stench but marine lives were lost in hundreds of thousands. What if terrorists were to execute similar attacks on portable drinking water?

What if the financial system of a whole nation is hijacked by cyber terrorists instead of a mere individual bank account? If the internet, satellite / cable / cellular service providers were hacked by cyber-terrorist and compromised, how will this have a troll on the people's life? How will businesses be conducted? How will the people communicate?

Offshore oil rigs were not left out. A demonstration that was made by Sandia National Laboratories shows that by setting things to manual control, automated safeguards can be willfully circumvented. Medical service provider can be vulnerable to cyber-terrorists' attacks in two ways. One of the ways is that some patients do receive death and life medication by mail. Any alteration in the prescribed delivery mode of medication can leads to the death of a patient, also the realization that insulin pumps are "hackable" is an issue of great concern [13].

The second way in which medical service providers are vulnerable is seen in the way medical equipment evolved before the evolution of Windows 95/ Windows 2000, a lot of hospital equipment were highly specialized and design using proprietary operating systems. When medical equipment companies try to reduce cost and improve efficiency, a lot of them resort to using MS windows operating system in their equipment. This might result to problem due to how windows viruses are spread [13].

3.10. Preventing and Mitigation of Future Attacks

Due to the vulnerability experienced over the years in software and new technologies, one begins to wonder whether security is not the forefront of priority during the development. As reported by Lucian Constantin [13], the research was performed by a team from application security firm Veracode for six up-to-date devices acquired in December and found serious issues in five of them". Also, MIT Sloan Management Reviewed reported that companied alarmingly do not show concern with such devices security. It also appears that most organizations are not fully aware of the vulnerability of the technology there are using. Therefore, security implementation should be considered as part of the most important priorities while developing software as well as devices in general. Despite many deterrents set up by various governments to tackle acts of terrorism, terrorists unlike other criminals, the probability of getting caught is not usually a primary concern to them. Thus method of preventing cyber-terrorism attacks as opposed to cyber-crime must be considered differently due to the attack's perspective. Usually, terrorists do not abide by legislation and careless about consequences of being identified prior or during an attack. Therefore, it is of paramount important to be able to identify attackers within the shortest period of time. Of the most important areas of cyber terrorism research over the years is intrusion detection. The creation of safe barriers within our systems is absolutely necessary so as to identify occurring attacks and thus moving swiftly to implement the proper method of mitigation. In order to be as effective as possible in repelling an attack, new and updated intrusion detention system must be developed constantly. In addition to mitigation improvement, it paves way for the compartmentalization of a system thereby limiting possible damage and thus protecting valued assets before the occurrence of irreparable damage. Also, by focusing more attention on data

preservation during an attack, response to cyber-attacks can be improved. Having updated versions of system or databases always is very essential as advised by security professionals.

4. CONCLUSION

Information technologies are systems created by using computer and communication technologies together. Information technologies; In addition to micro-electronic and data transmission, they are technologies that include fax machines, mobile phones, cable television, computers, information networks, videotex, software and on-line databases. In organizational correspondence, data obtained with the help of information technologies are collected, classified, recorded and processed in a way to be converted into information and used in decision processes [34]. As can be seen from the various definition of cyber-terrorism presented in this work, it lacks a single universal acceptable definition but do have some common characteristics and one of its features is that it a crime of great magnitude executed in order to achieve political or ideological gains. Despite the fact that it is quite difficult to point out to a single cyber-terrorist attack that has led to loss of lives and property at a large scale, there is alarming evidence that modern terrorist seriously considers the addition of cyber-terrorism to their arsenal. And as pointed out by Denning, "at least for now, hijacked vehicles, truck bombs, and biological weapon seem to pose a greater threat than cyber terrorism. However, just as the events of September 11th caught us by surprise, so could a major cyber assault. We cannot afford to shrug off the threat".

Future terrorists may utilize the cyber-space for their attacks than the terrorists of today considering the facts that the next generations of terrorists are being brought up in the digital world and the globe is becoming more and more dependent on the cyber-space in almost all fields. Paradoxically, the success of "war on terror" is likely to make terrorist organizations to turn up to unconventional weapon such as cyber-terrorism therefor there is a great need for both national and international measures to be increased and more protective measures to be taken in order to safeguard our cyber-space from the hands of terrorist organization.

- Terrorists' organizations activities should be combated by providing systems and programs necessary to protect our cyber-space.
- Fundamental rights and human freedom should not be prejudice through the exploitation of the fear of electronic terrorism by monitoring emails, blocking websites, and so on without tangible evidence pointing to Security Bridge.
- Members of the society should be educated through the media and various channels of communication on the dangers of cyber-terrorism.
- Organizations and tools to strengthen the capabilities of information security in all aspects such as the judiciary and police should be provided.
- Government should not use its powers in oppressing a particular segment of the society as that might lead to the radicalization of members of such segments by joining terrorists' organizations.

CONFLICT OF INTEREST

The authors stated that there are no conflicts of interest regarding the publication of this article.

REFERENCES

[1] Öğün MN. Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes. Journal of Applied Security Research, 2012;7(2), 203-217.

[2] Garrison A Terrorism: The nature of its history. Criminal Justice Studies, 2003; 16(1), 39-52.

[3] Hudson R. The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why? Federal Research Devision. Library of Congress. Retrieved from http://www.loc.gov/rr/frd/pdf-files/Soc_Psych_of_Terrorism.pdf., 1999.

[4] Collin B Future of Cyberterrorism: The Physical and Virtual Worlds Converge. Crime and Justice International, 1997; 13(2), 15-18.

[5] Conway M. Reality Check: Assessing the (Un)Likelihood of Cyberterrorism. In J. L. Chen T. (Ed.), Cyberterrorism; pp. 103-121. New York, NY: Springer, 2014.

[6] Denning D. Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Retrieved from http://bit.ly/2Er9ZLt.; 2000

[7] Ambos K. Responsabilidad penal internacional en el ciberespacio. Retrieved from https://bit.ly/2QNF1D5.; 2015.

[8] Yannakogeorgos P. Rethinking the Threat of Cyberterrorism. In T. J. En Chen (Ed.), Cyberterrorism; pp. 43-62. New York: Springer, 2014.

[9] Melzer N. Cyberwarfare and International Law. Unidir Resources. Retrieved from https://bit.ly/2UxGmwV., 2011.

[10] UNODC. The use of the Internet for Terrorist Purposes. New York: United Nations. Retrieved from https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.; 2012.

[11] Öğün MN, Kaya A. Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirle, Güvenlik Stratejileri Dergisi, 2013; Volume 9, Issue 18, ss.145-181.

[12] Weimann G. Cyberterrorism: The Sum of All Fears. Studies in Conflict and Terrorism, 2005; 28(2), 129-1. doi:/abs/10.1080/10576100590905110.

[13] Jarvis G. Comprehensive Survey of Cyber-Terrorism. Retrieved from https://www.cse.wustl.edu/~jain/cse571-11/ftp/terror/index.html.; 2011.

[14] Terrorism C. o. (Ed.). Responses to Cyber Terrorism (1 ed., Vol. 34). Ankara, Turkey: IOS Press., 2008.

[15] Goodman S, Kirk J, Kirk M Cyberspace as a medium for terrorists. Technological Forecasting and Social Change, 2007; 74(2), 193-210. Retrieved from 10.1016/j.techfore.2006.07.007.

[16] Villegas DM. Contribuciones para un concepto de terrorismo en el derecho penal chileno. Política Criminal, 2016; 11(21). Retrieved from 10.4067/S0718-33992016000100006.

[17] Cancio MM. El delito de pertenencia a una organización terrorista en el código penal español. Revista de Estudios de la Justicia, 2010; (12), 147-164. Retrieved from 10.5354/0718-4735.2011.15233.

[18] Mañalich J. El terrorismo ante el derecho penal: la propuesta legislativa del gobierno como retroceso. Anuario de Derecho Público UDP, 2015; 154-171.

[19] Gillespie A. Cybercrime: Key Issues and Debates. London : Routledge 2016.

[20] Jones A. Cyber Terrorism: Fact or Fiction. Computer Fraud and Security(6), 4-7. Retrieved from 10.1016/S1361-3723(05)70220-7. 2005.

[21] Laura ML. Retrieved September 22, 2019, from google: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000200005#aff1.

[22] Crenshaw M.. The Causes of Terrorism. Comparative Politics, 1981; 13(4), 379-399.

[23] González CE. Los estudios sobre terrorismo: Balance de los últimos 25 años. Espacio Abierto, Cuaderno Venezolano de Sociología, 2016; 25(4), 61-76. Retrieved from http://bit.ly/2ErZnvH.

[24] Carnevali R. El derecho penal frente al terrorismo: Hacia un modelo punitivo particular y sobre el tratamiento de la tortura. Revista de Derecho, 2010; 109-145.

[25] Gibbs J. Conceptualization of Terrorism. American Sociological Review, 1989; 54(3), 329-340.

[26] Ganor B. Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter? Police Practice and Research, 2002; 3(4), 287-304.

[27] Boeckmann R. Turpin-Petrosino C. Understanding the Harm of Hate Crime. Journal of Social Issues, 2002; 58(2), 207-225.

[28] Poveda Criado, M. Torrente Barredo, Opción B. Redes sociales y ciberterrorismo: Las TIC como herramienta terrorista, 2016; 32(8), 509-518.

[29] Clough J. Principles of Cybercrime. New York: Cambridge University Press, 2010.

[30] D'Aiuto, G. En Levita, L. I reati informatici. Milan: Giuffrè, 2012.

[31] Alexander DC. Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses, 2014. Retrieved 10 31, 2019, from https://dergipark.org.tr/tr/download/article-file/89251.

[32] Brenner SW. Cybercrime, cyberterrorism and cyberwarfare. Revue internationale de droit pénal, 2006; 77, 453-471.

[33] littl3field. Cyber Terrorism: understanding and preventing acts of terror within our cyber space, 2011. Retrieved from littlefield.co: https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb.

[34] Öğün MN. et all Information Technologies and Reaching to Information Society. Revista Electrónica de Investigación en Ciencias Económicas, 2020; Vol. 8, No. 16, pp:412-448.