2023 Usman, Tabbasum, Ahmad & Shahzad. This is an Open Access article distributed under the terms of the Creative Commons-Attribution-Noncommercial-Share Alike License 4.0 International (http://creativecommons.org/licenses/by-nc-sa/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly attributed, not used for commercial purposes, and, if transformed, the resulting work is redistributed under the same or similar license to this one.

Received: November 02, 2023

Revised: November 27, 2023

Published: December 10, 2023

Journal of Politics and International Studies
Vol. 9, No. 2, July–December 2023, pp.139–155

Cyber-warfare Versus Cyber-terrorism: An Emerging 21st Century Trend

Muhammad Tayyab Usman
Lecturer (Civics), Govt. Islamia Associate College,
Lahore Cantt
Correspondence: tayyabusman866h@gmail.com

Ammara Tabbasum
Assistant Professor, Department of Politics and International Relations,
University of Sialkot, Pakistan
Email: ammara.tabassum@uskt.edu.pk

Dr. Mukhtar Ahmad
Deputy Director Colleges, District Nankana Sahib, Pakistan
Email: malikmukhtar1963@gmail.com

Kashif Shahzad
Independent Researcher,
Email: ks410488@gmail.com

Abstract

Cyber-warfare attacks are not commonly found like cyber-attacks yet it done by countries, organizations or institutions to disrupt the activities of their enemies in the cyberspace also safeguarding their own information assets. The current study has adopted documentary analysis by using content analysis as method of analysis. The researcher has searched through relevant databases; Google Scholar, JStor and Emerlad Insight by formulating key-terms for search. The study found that the measures taken by the governments usually can be categorized into two types; repressive measures and soft measures. The repressive measures can be defined as denial of access of internet services and blockage of websites and social media pages run by the terrorists. This also includes the blockage and restriction of the promotion of radical content and ideas to the common people.

Key Words: Cyber security, Cyber-warfare, Data breaching, Cyber-terrorism, Organizations

Introduction

Panetta (2012) has warned that United States of America have to face many attacks from violent extremist groups through computers to "derail passenger trains…contaminate the water supply in major cities, or shut down the power grid across large parts of the country." The secretary has warned the nation that combined attacked by these groups can cause "cyber Pearl Harbor" that "would paralyze and shock the nation and create a new, profound sense of vulnerability." Green

(November, 2002) described the term of 'cyber terrorist' as the people behind the scene are working on computer, sitting somewhere, trying to demolish the banking system, national security system or other judicial or national assembly websites. Weimann (2005) said that these are actually hackers using exploiting networks to kill anyone virtually. It can best be described as "Terrorists can sit at one computer connected to one network and can create worldwide havoc…[they] don't necessarily need a bomb or explosives to cripple a sector of the economy, or shutdown a power grid" (p. 65).

Cyber Attack

Kenney, (2015) Cyber-attack is most commonly used word for computer-to-computer attacking through internet by creating disruption, data stealing, disorder or destroying the whole system (Kissel, 2013; National Research Council, 2009). Many common methods employed during cyber-attacks included; slow downing the system, inserting virus, junking communication of websites, and exploiting spyware to steal required information and overwhelming websites. However, cyber-attacks do not include physical or conventional attacks to the computer as destroying the computers with hammers. It can be defined as "cyber-attacks are computer attacks on other computers carried out in cyberspace, including the Internet, telecommunications infrastructures, and computer systems" (Kissel, 2013, p. 58; National Research Council, 2009, p. 11). The major objective of the cyber-attack may be to harm the computer, stealing data from the computer or simply continuously observing the system for consequent attacks. In other words, the attacker interrupts into other system without the prior permission or taking into the knowledge of the victim. The cyber-attackers who are may be states or non-states actors intended to get any economic, political, religious or psychological benefits from the victims (Nicholson, et. al., 2012; Weinberger, March 20, 2012).

Hacktivism

Hacktivism is defined by McAdam, Tarrow and Tilly (2001) as this is war which taken place in cyberspace where people are hacking computers with inclination of harmful activity. These activities have been done with the purpose of disrupting, disabling or stealing data from other computers. Hacktivism has many characteristics which make it different from cyber-terrorism, cyber-attacks or cyber-warfare. In other words, Denning (2001) described hactivism as it is a form of "contentious politics" which taken place by usually religious or anti-state actors to capture to oppose the policies of the government. Hacktivists are well organized, trained, having knowledge of tools and techniques to use to capture the passwords and key pins of other systems. They are usually working for not only data stealing yet they want a reasonable notice of their group and cause of their action. Hacktivism is usually associated with cyber-terrorism wrongly as most of the times hackers are just threatening their victims, posting their data, demanding some money or other harmful activities. Yet, it can be associated with cyber-terrorism if it can be done to hack the government agencies, government websites, business corporations, law and judiciary websites or other related government institutions' websites.

Cyber-Terrorism

Commonly cyber-terrorism consisted of cyber-attacks encountered by computers to the other computers to harm or steal their data. Cyber-warfare, cyber-hactivism and

cyber-terrorism are taken place in cyber space. It can best be defined as "convergence of terrorism and cyberspace" by using computer to attack the other one (Collin, 1997). This distinguishes the traditional terrorism to cyber-terrorism in terms of use of cyber-space as place of war and computer as weapon or tool for war. When cyber-terrorists attacked to get information of their targets to bomb or attack them, they actually not only attacking their victims but they are exploiting computer technology also.

Conversely with conventional or traditional terrorism, cyber-terrorism can be distinguished by the motives and intentions of the cyber-terrorist. In contrast of cyber-attacks, cyber-terrorism has encountered due to non-state acts of terrorist to religiously / politically oppressing the victims rather their economic outfits.

Cyber-warfare

Cyber-warfare attacks are not commonly found like cyber-attacks yet it done by countries, organizations or institutions to disrupt the activities of their enemies in the cyberspace also safeguarding their own information assets. Cyber-warfare can be defined as computer attacks and or computer assaults to destroy the infrastructure, information domain or steal any important information from enemy's network using computer (Hildreth, June 19, 2001). Cyber-warfare is different from traditional war as it occurs in cyberspace only. The author used the term "Kinetic" which refers to physical damages made to the networks, telecommunication settings, or network cables which do not include in the cyber-warfare (Hathaway, et. al., 2012).

Nicholson, Webber, Dyer, Patel, and Janicke, (2012) demonstrated that cyber-warfare cannot exclusively consider as the domain of states. Many times, private backers do the same things to safeguard their interest or to gain upper hand on their rivals. Langner, (2011) revealed that due to virtual activity of cyber-warfare it has been considered less violent, not real or ignored activity. Cyber-warfare attackers do not attack directly rather indirectly by exploiting the energy and force generated by computers. It usually consisted of serious of attacks or action rather than one two isolated attacks to deteriorate the front enemy.

Markoff (2008) described that the cyber-warfare attacks are not very common like cyber-attacks yet it happens in special circumstances as example taken of Georgian government was victimized during Russian-Georgian war in year 2008. However, both the countries are now living with peace formally yet the hackers are believed to consistently targeting the services and security system of Georgian government. After that, when bombing started, other targets as transportation and media are also included. It was the first time when during war, computer was used to initiate a cyber-warfare against enemy. Here is a table presented with attributes of cyber-attack, cyber-warfare, hacktivism and cyber-terrorism:

Background of the Study

These all aspects of cyber enforcements should be considered in the light of the UN peacekeeping principles which are providing guidance towards the intuition of peace among conflicting parties.

UN Peacekeeping Principles

UN peacekeeping principles have been widely considered suitable for the peace building guided by a number of core principles in consideration of Brahimi report (United Nations, 2000). These principles are followed as:

- **Consent of the Parties:** The consent of the both conflicted parties has been considered necessary to act upon the peacekeeping process. Otherwise, the involvement of the institution taken as interruption.
- **Impartiality:** The institution showed its involvement with the matter with ensuring the objectivity in the whole process. Impartiality considered very important as both parties are giving trustworthiness.
- **Ensuring Non-use of Force:** The principles guide the both parties to avoid use of force else defense of one of the parties. It also provides vigilance towards use of force against who is going to use force and trying to destroy peace building process.

Significance of the Study

Cyber-warfare has been taken very serious by media as well as research community describing the challenges posed by cyber-warfare, its legality, ethical considerations and doctrine of its uses (Robinson et al., 2015). The extensive research has been done on the topic yet the peacekeeping aftermaths of cyber-warfare has not been dealt yet in the literature. The ethical consideration has been considered by (Taddeo, 2012) while how to deal with weapons and tools of cyber-warfare carried out by Tyugu, (2012). However, there is dire need to address raised questions by the current study as; ambiguity removal of terms among cyber-attack, cyber-terrorism, hacktivism and cyber-warfare dealing with the case studies of America, China and Russia. Further, the study has dealt with issues and challenges caused by cyber-warfare and investigated into the matter of peacekeeping aftermaths of cyber-warfare.

Research Objectives

The study has been carried out to achieve following objectives:

- To differentiate among cyber-attack, hacktivism, cyber-terrorism and cyber-warfare
- To deal with the case studies of cyber-warfare including America, China and Russia
- To incorporate issues and challenges caused by cyber-warfare
- To investigate peacekeeping aftermath of cyber-warfare in the world

Research Design

The current study has adopted documentary analysis by using content analysis as method of analysis. The researcher has searched through relevant databases; Google Scholar, JStor and Emerlad Insight by formulating key-terms for search. These key terms included; 'cyber-warfare', cyber-warfare and peacekeeping', 'cyber-crime, cyber-attack, cyber-terrorism and cyber-warfare'.

The result found many of research articles, books, book chapters, conference papers and reports which are analyzed on the basis of research objectives of the study and included accordingly. The studies have been analyzed by scrutinizing the objectives of the study, method employed by the research and major findings and implications of the study.

Emerging Cyber-Warfare Strategies and Counter Strategies

Now the world is more self-sufficient in making life easier with the help of emerging technologies. The machines are helpful in making complex tasks very easy to be done. The cyberspace is now going beyond from mere concept of integration of computers rather focused on the evolvement of various devices as well as machines. Cyberspace has been defined as "an environment where storage, processing and communication are carried over computer and networking infrastructures" (Wikipedia, Accessed on October 16, 2019).

Cyberspace has further been used Cyber Physical System where the operators are taking place their actions through preprogramed instructions and controlling systems. Tzipora, Haoyu, Nitesh, Jonathan, and Tuo, (2014) argued that today Cyber Physical Systems have been used in chemical procedures, healthcare infrastructure, entertainment industry, manufacturing, military operations and transportation. Cyber Physical Systems are not only used in complex technological areas yet they are also used in automotive and in creation of most complex cyber warfare tools.

Jan, Oscar, and Klaus, (2014) said that by the emergence of new technologies cyber-attacks are not limited to computers only yet they are expanded to industrial as well as military level. However, emerged now tools "SCADA (Supervisory Control and Data Acquisition)" are considered necessary for the control and monitor appropriately (Goodman, 1997). In this world, every system is interconnected with IoT (Internet of Things) which is a common technology where cyber-attack is expected. (Aditya, & Richard, 2013; Aditya, Rohit, & Richard, 2013; Ross, & Log, 2015).

SCADA systems usually adopt IoT technology to connect with the cyberspace with the purpose of controlling and monitory physical infrastructure. The interconnection of IoT and SCADA provides a very supportive and secure environment. Another technology RFID (Radio Frequency Identification Device) has widely been used to keep track of the devices as attackers are found in search of personal information for their personal interests Andrew, Stuart, Shaun, Tanuja, & Helge, 2012).

Further, cyber threat can be defined as it is an act of making huge damage to the computer network of any communication system with the effort of malicious tools. The attack or series of cyber-attacks can be initiated by the help of any organization, individual or even government from remote location (Juels, 2006). While, cyber defense is a technique to safeguard oneself from the cyber-attack however the preventive measures which are taken before considered more appropriate rather initiating an enquiry after cyber-attack (Daniele, Velio, Giovanni, & Aurelio, 2003; John, & Andres, 2005). These measures are also called cyber security and it can best be defined as taken measures to avoid any damage or malicious control over computers through hardware, software or any other human activity (Anita, Kirsten, Daniel, Brianne, & Emilie, 2005; Pin-Yu, & Kwang-Cheng, 2012; Pin-Yu, Shin-

Ming, & Kwang-Cheng, 2014). Another term in this regard used is 'cyber forensic' which is also called 'computer forensic science' which dealt with the evidences found on the computers and storage media. It aimed at knowing the reasons and evidences which further led to the enquiry of interruption with computers or computer networks (Re ´ka, Hawoong, & Albert-Lazlo, 2000).

Emerging Cyber Strategies Used

Now days, cybercrimes are being committed with more organized way to interrupt the communication systems of the victims. The attackers are mostly applying these three steps before initiating any cyber-attack:

- **Information Collection:** The first and most important step considered is information gathering. In this regard, Open Source Intelligence (OSINT) method has been widely applied using DNS query. This information is collected using open ports and employing the XSS (Cross Site Scripting), SQL injections etc.
- **Threat Modeling:** In this second step the attackers are mapping the victim's machine and trying to access and also trying to measure the level success and risk.
- **Attack and Exploitation:** The final step taken to attack and exploit the communication system of the victim (Shui, Song, & Ivan, 2015).

Here are some advanced and emerging methodologies used in cyber-attacks:

APT (Advanced Persistent Threat)

This is the most dangerous methodology used in cyber-attacks. These types of methodologies are usually applied in social, economic and online or social media. APT ensures the persistent access to the victims' machines rather focused only on entry. The historic investigation of the methodology reveals that it has been used as ghost attack by sending an email to the victim with malicious material through different codes. It ensures the activation of Remote Administration Tool (RAT) kit (Shui, Song, & Ivan, 2015).

The major objective gained through this method is acquisition of properties information and sensitive personal information gained through Internet Explorer. Then the attackers are able to damage the system of the designated victim using BGP (Border Gateway Protocol) (Rogers, 2006). In year 2010, the new emerged method STUXNET to indulge into the SCADA's PLC (Programmable Logic Controller) with the help of DUQU (Ahmed, Mona, Kaveh, & Joaquim, 2013).

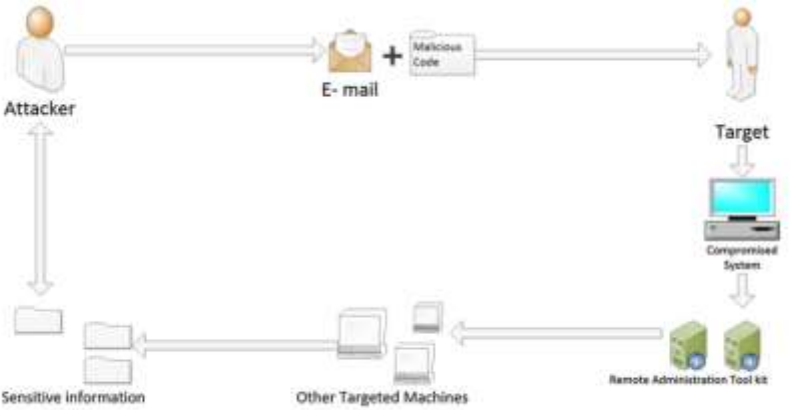

Fig. 1 Attack mechanism by embedding a malicious code on to an email

The figure1 it clearly shows that the attacker has sending an email to the victim's machine with malicious code to its compromised system which is already decoded through Remote Administration Tool kit. In this whole process, the attackers are also targeting other targeted machines to obtain sensitive information of the victims. Miao and Junshan (2011) said that this type of attacks also called Island Hoping which is maintained to get access to the confidential and sensitive information of the target machines.

Attacking Strategy BYOD (Bring Your Own Device)

The second most employed methodology or strategy in cyber-attack is BYOD. This methodology is mostly used by industrialists to ensure their cost enhancing benefits with reduced use of human resources. The major threat to this method is that most of the times employees are using devices in their offices as well as their homes and installing third party software which resulted in high risk. The third party software is mostly used to steal the data of any specific industry which led inverse results to the industrial profits (Oliver, Liyan, Robert, & Lang, 2011).

Use of SCADA in Cyber-attacks

SCADA (Supervisory Control and Data Acquisition) are most commonly applied in industrial sectors. Nuclear power plants and oil treatments have been treated with the help of SCADA. The remote connection has been established with SCADA technology and thus the SCADA is most targeted machines by the attackers. SQL injection and script kiddies are used to interrupt and get access to the SCADA based machines (Klaus, 2013).

In this type of attacks, the insiders are hard to determine as authorized systems are responsible for distribution of the systems. Another method is used in crafted packets which used to deceive the State Estimator and Bad Data Detector. It is also known as Stealth Attack (Buyens, & Joosen, 2007). SCADA most commonly used attacks include power disruption which also used even in grown countries Angelyn, & Sherali, 2014). In this way, Physical Security Systems are hanged by the effective applications. The case study presented in Chapter 2 of Ukraine is also an example of power disruption.

Moreover, the profit sharing life cycle among mule agents, malware writers and attackers is also very important to understand the character of the attackers and mule agents. There is a malware writer who is working on codes and attackers is working at the mid between the target. The gained profits has been divided among attackers and mule agents which gained by the third party or the victims. It has best been described through figure 2.

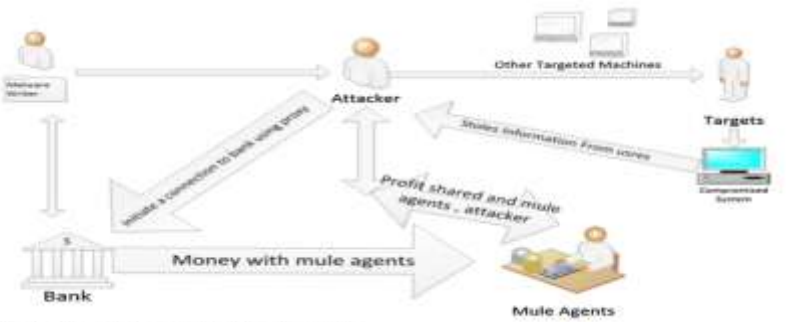

Fig. 2 Lifecycle of profit sharing among attacker and mule agents

Use of Smart Grids, Smart Devices and Smart Cities

The wider use of smart devices among people is seen in this era. These smart devices are not only used personally yet these are applied in healthcare, automobiles, telecommunication sector etc. The PKI used through the application of Key Less Entry (KLE) applying RFID tags (Amir, & Haya, 2013). There are other attacking strategies used including vulnerability attack: this methodology is used to interrupt the functions of any communication system and de-synchronizing the feedback. Data injection is also used to influence the measurement meters and manipulate its information (Saar, & Steven, 2007).

These type of attacks resulted in huge loss of electricity transfer and power supply. Another type of attack is International Attack in which an attacker which is able to disrupt the whole system of SCADA as having complete knowledge of computer technology and the case of Maroochy Water Services incident used an evident.

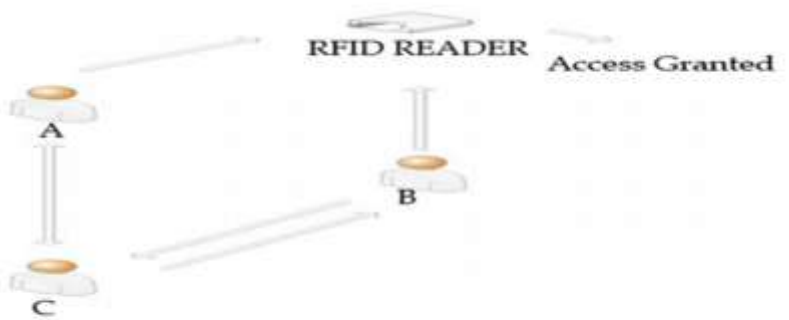

Fig. 3 Attack scenario for RFID

The figure 3 reveals a physical breakage of the systems as Person A has decoded the RFID tags and gets unauthorized entry into the building as RFID tags automatically detected that Person A has card. While Person B has also with not genuine card to

enter into the building yet simulating card and Person B applies for the access which is actually granted to B but also enters Person A who is with Person C. This access granted process is deceiving of the RFID system.

IoT (Internet of Things) Attacks

In this Internet era, everyone is on the internet with the help of different devices. These are usually common devices which are easy to tackle by the attacks and caused Sybil Attack and Privacy Attack (Cuijpers, & Bert-Jaap, 2012).

Mimicking Attacks

This kind of attacks can only be determined in presence of large scale botnets. In discrimination process, there are many active bots found while very few of the inactive users found. DDoS attacks which includes the information publishing or email hacking it also considered as DSNXbot, Evilbot, G- symbol, Sdbot, Spybot etc.

Defensive / Counter Strategies against Cyber-warfare

The secure cyber defense system ensures the existence and sustainability of any individual or party in cyber space. There are certain steps taken to ensure cyber defense. These steps include: "Preparation, Monitoring, Detection, Analysis and Response. Preparation, monitoring and response are known as Triage Analysis" (Katherine, 2003). It is most important to know before taking these steps the type of common and emerging attacks and attack methodologies which are described in following table 1.

Table 1

Table 1 Common attacks and attack methodology

Common attacks	APT	Island hopping	Attacks to BYOD	Attacks to SCADA	Attacks to smart devices	Attacks to IoT	Mimicking attacks
Attacking methodologies used							
DOS	✔			✔	✔	✔	✔
RAT	✔	✔	✔	✔	✔	✔	
Code injection	✔		✔	✔	✔	✔	
Information theft	✔		✔	✔	✔	✔	✔
Insider			✔	✔			
Anonymity	✔			✔		✔	
Inducing fake identity				✔	✔	✔	
Spams	✔			✔			✔

Further, the table 2 shows the type of hackers, their motives to initiate attacks or series of attacks and also considers their skills level.

Table 2

Table 2 Common hacker types along with their motivation and skill levels

Hacker types	Motivations						Skill level
	Ideology	Recreation	Prestige	Revenge	Profit	Curiosity	
Novices						✔	Low
Crowd sourcers		✔		✔			Below intermediate
Cyberpunk (hightech outsiders)						✔	Very low
Hacktivists	✔			✔			Very high
Insiders				✔	✔		Intermediate
Coders			✔	✔			Upper intermediate
Cyber warriors	✔				✔		High

By considering the attackers' strategies, motives and their skills level there are some counter strategies employed to avoid any type of loss to the organization as well as any individual.

Denial and deception against zero-day exploit

The firewall era, installation of different virus detection software and use of IDPS (Intrusion Detection and Prevention System) does not ensure the Zero Day Exploit and automatic up gradation of the IDs **(**Parunak, Paul, Sven, & Rafael, 2007). So, the usage of Denial and deception can ensure the secure cyberspace setup (Kristin, Frank, Ben, & Roshan, 2015). The major goal of the D&D has employed by giving an advantage to the deceiver to convert the psychological state into the physical behaviors. This cyber degradation enables to fights or deceives (Ryan, 2015). The deception is a chain which works from planning to the execution of the process (Parunak, Paul, Sven, & Rafael, 2007).

The first phase of planning of deception consisted of looking the whole effect of the process and available resources for execution. The second phase adds further deception with reinforcement of cover story (Andre, Saurabh, Henrik, Karl, & Shankar, 2010).

Support vector machine (SVM) method

Another method which is widely employed to ensure zero exploit day with the integration of Self-Organized Ant Colony Network (CSOACN) method. The method first learned the method of data trails of the activity.

Table 3
Defense methods employed commonly to counter cyber-warfare

Defense methods	Attacks				
	APT	BYOD	IoT	Smart grid	RFID
Denial and deception	✔				
SVM and CSOACN	✔			✔	
Security intelligence		✔			
Two player sum game			✔	✔	
Moving target defense (MTD)			✔	✔	
Ant based defense			✔	✔	
Fusion based defense			✔		
Privacy policy enforcement			✔		
Sensor data correlation					✔

DEFIDENT

A common method of Intrusion Detection Network (IDN) (Adams, & Lloyd, 2003) also used as DEFIDNET is employed to counter the cyber-attacks (Sergio, Juan, Agustin, & Pedro, 2015). In this method, a multi-tasking algorithm is used to counter the risk of the continuing projects in any industrial area of any type of organization. This is very helpful in at least getting the overall picture of the attack and estimation of the caused damage.

The evolution of the emerging technologies and penetration of the information and communication technologies make it questionable as how the security of the cyberspace is sure? The whole information technology infrastructure and World Wide Web is interconnected with each other and can be accessed from any remote location and even misused. In this cyber world, water industry to telecommunication sector is considered vulnerable to the cyber-attacks.

Cyber-Terrorism Term

There are two claims regarding cyber-terrorism as one school of thought acclaimed that there is no cyber-terrorism yet another school of thought has evidences of wider use of internet by terrorists. This is because of disagreement on the clear definition of terrorism and cyber-terrorism. The word "Terror" originated from the Latin word "terrere" which means to "to frighten, to terrorize, to intimidate" (Wilkinson, 1974). Normally, a series of these terrorist attacks with some designated motives led to the terrorism. Bozdemir (1981) defined terrorism as "Terrorism is a strategic approach which, for political purposes, identifies itself with a method which includes the use of organized, systematic and continuous terror" (p. 23). Most of the times, cyber-terrorism is intermixed with the concept of information warfare which is however different in terms. Denning (2000) defines cyber-terrorism in these words "It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear" (p. 189). Further, cyber-terrorism defined in recent times as "unlawful attacks and threats of attack against computers, networks, and the information stored therein" in order to "intimidate or coerce a government or its people in furtherance of political or social objectives" (Manap., & Tehrani, 2012: 409).

Ten Emerging Information Warfare Trends

The emerging trends of cyber-warfare and information warfare towards the information industry have changed the concept of military operations and actions. Cronin and Crawford (2007) have suggested four solutions towards these emerging trends:

1. **Computer-related security incidents are widespread:** The number of cases related to computer crimes has been increased in coming year as analyzing 6 cases in 1988 while 137,529 cases reported in the year 2003. The actual cases are however more than reported as most of the cases did not get public interest and acknowledgement. In year 2005, 20% more cases reported to cybercrime branch of America than to the physical abuse (Gordon, Loeb, Lucyshyn, & Richardson, 2005).

2. **Entry barriers are low for cyber attackers:** In before times, the hackers are well knowledgeable as some hackers were found students of MIT who were involved in attacks of 1960 (PC World, 2001). In coming years of 1970, the hackers were considered with high profile educational and experience level who were involved in school or business sector (Parker, 2012). Yet, the hackers' systems were changed in 1990s. A Solar Sunrise incident was happening in 1990 by the teenagers under guidance of 18-year boy who got access to the websites of government as well as military sites. In 2002, a website was launched by hackers to introduce the tools and techniques of hacking (Jones, Kovacich, & Luzwick, 2014).

3. **Dangerous forms of cyber weapons have emerged:** In 1980, the board for the sharing of tools and techniques of hacking was introduced which helped the hackers to enhance their power through sharing and communicating. Through this communication, distributed denial-of-service (DDOS) was the most employed method found. The software was considered responsible for the attacks of February 7, 2000 in which major websites and search engines were shut down including Yahoo, eBay, Amazon, E-Trade, and CNN.

4. **Many nations have information warfare capabilities:** In early 1990s very few nations were found involved in getting capabilities of information warfare. But in coming years Adams (2016) found many nations like China, India, Taiwan, France, Russia, Israel etc. were capable of information warfare. In the survey of CSI/FBI held on 2003 found that 28% foreign governments are likely to be attacked by the other governments in context of information warfare.

5. **Increased economic dependency on information infrastructures:** The society has been grown from industrial to information based society (Toffler, 2011). Meall (2015) found that Americans were worried about the so much economic dependency on the computers in their report *Computers at risk*. Here

are the economic impacts of virus attacks on the economy of the world year wise:

6. **The private sector is the primary target:** The growing economy and its dependency on the computers and computer networks led the hackers to target the civilian and private sector (Poulsen, 2004).
7. **Cyber technology is increasingly used in perception management**: Perception management can be defined as catchall phrase which is based on the pubic opinions and perceptions regarding cyber technology (Callamari & Reveron, 2016). The wider use of internet and computer technologies has influenced the common people in making perceptions and sharing them all around (Rattray, 2017).
8. **Cyber technology is increasingly used in corporate espionage:** In March 2001, former French Defence Minister has argued that Americans are stealing their information through sending devices secretly to their country (Cohen, 2001). The FBI sources said that the average cost of hackers' attack is around $150,000 while the caused damage is much more than the cost (Cohen, 2001).
9. **Cyber technology is increasingly used by organized crime:** Federal News Service (2003) acclaimed that they have committed an action against the internet economic treasurers who are victimizing the common people. Now days, internet crime has gained a growing crime in whole world. Legard (2013) noted that majority of the accounts were hacked through sending an email to the account and requesting linked website to provide account number and password which could cause huge fraud.
10. **Cyber technology is increasingly used against individuals and small businesses:** Stafford and Urbaczewski (2014) argued that majority of the common people were being victimizing through spyware and adware. According to *Microsoft* there are almost 70000 spywares were existed and caused the loss and crash of 91% home appliances and PCs.

Use of Cyberspace by Terrorists as Cyber warfare

There are many evidences found in cyberspace that terrorists and their activists are using cyberspace to for the promotion of their ideas as well as for fund raising purposes. Here are some given evidences:

Fundraising

A mentor of Osama Bin Laden, Ozzam has launched *Ozzam Publications* website which was built with the purpose to promote the agenda of Al Qaeda and also generate funds for them. The website contained Jihadi material from books to videos to promote agenda of Al Qaeda. Once the website was blocked and showed no content yet in 2002 the websites was again available to its users and offering the material for purchase.

Information Warfare

Warran (2015) presented case study of Hezbollah group as their first presence was found with limited and minor level information. They were providing their message with the interruption of outer world as seen in figure 2.

Conclusion, Discussion and Recommendations

The broadcasting of information has now been widespread due to evolution of emerging technologies day by day. The massive communication has new been possible through social media platforms such as Facebook, Flicker, YouTube, Instagram etc. In this environment, it is however not surprising to find terrorist activities and wider use of these applications for terrorist activities (Weimann, 2014).

Conclusion

Few years ago, it has been seen that majority of the *Jihadists* were doing their activities using internet and social media applications to support their agenda. Even though, they were found promoting radicalization and recruiting new *Jihadists* using "seal the deal". The *Jihadism Online* published and owned by Norwegian Defence Research Establishment (NDRE) found that although there is wider use of internet has been evidenced by terrorists yet there is few evidences found of recruitment through internet (Rogan, 2006, p. 29).

A study conducted in year 2012 revealed through Dutch Intelligence Service that 99.8% terrorist activities took place under cover and at hidden level called "Deep Web or Darknet". The Jihadists were finding the person through their discussion on online forums, promotion of radicalization activities and searching for Jihadist's agendas. Weggemans, Bakker and Grol (2014) said that the reasons of individuals' interest in Jihadists' activities are still vague and unclear to the researchers. Yet in some Western countries experiences it has been found that the youth is taking interest within very short time.

The recent cases happened in West like "lone wolf"[1] or "virtual packs of wolfs" led the thinking of the authorities towards the open use of social media sites and outlets. Behr, Reding, Edwards and Gribbon (2013) described that persons are looking on the internet when they have already a mentality of radicalization yet a clear evidence of use of social media or internet for these purposes need to be found.

Another study conducted in 2013 by the RAND Corporation also revealed that there are little evidences found for the promotion of radicalization through internet otherwise physical contact is created. Although causal relationship could not found yet online use for terrorist activities is evidenced.

Discussions

Now the raised question is that how governments can affectively counter this emerging cyber warfare? The taken measures by the governments usually can be categorized into two types; repressive measures and soft measures. The repressive measures can be defined as denial of access of internet services and blockage of

[1] "The term "lone wolf" refers to those individuals who, without any physical social contact with extremist individuals or organisations, go to the process of radicalisation on their own, even to the point where they decide to commit terrorist attacks that they conduct on their own".

websites and social media pages run by the terrorists. This also includes the blockage and restriction of the promotion of radical content and ideas to the common people.

The prominent strategy in this respect "take down measures" has been employed to stop the accounts of ISIS yet it was also observed that they were creating new account further. The impact of this strategy was felt significant as many of the accounts were stopped yet a new number of accounts were created. Moreover, among soft measures it is also assured that use of effective communication methods to balance the "counter-narrative" of cyber warfare.

Recommendations

The study has posed relevant recommendations for governments, policy makers and decision makers of cyber warfare. These are:

- In cyber space it is very important to take these four parts clearly, the message, the messenger, channel used and communication.
- There should be proper infrastructure and adequate government efforts to counter the cyber warfare and also effective use of emerging technologies to counter cyber warfare attacks
- Cyber defense is also on the risk due to the deficiencies of net neutrality which can be countered by employing privileged high speed internet connections to the concerned departments, media sets and government websites.
- A clear and concise definition of cyber terrorism at government level is need of the time which is interchangeably used as "(e.g. hacking, propaganda, attacking to infrastructures etc.)"
- The nations should work in coordination with the signature of bilateral as well as multilateral agreements to work in cyber security issues
- A collaborative intelligence service should be initiated among working nations to collect and share information before any type of cyber attack
- A team of cyber experts as well as quick response teams should be initiated to counter the cyber-attack and response to the cyber-attacks in quicker way.

References

[1] Adams, J. (2016). Virtual defense. *Foreign Affairs, 80*(3), 98112.

[2] Algemene Inlichtingen en Veiligheidsdienst (AIVD). (February 2012), *Jihadism on the Web: A Breeding Ground for Jihad in the Modern Age*.

[3] Bozdemir, M. (1981). What Is Terror and Terrorism?," School of Political Sciences Press and Publication College, 1981, v, vi. See also Wilkinson, P., (op. cit.), p. 17, and Crenshaw, M., 'The Concept of Revolutionary Terrorism', Journal of Conflict Resolution, September 1972, pp. 384.

[4] Callamari, P., & Reveron, D. (2016). China's use of perception management. *International Journal of Intelligence & Counter Intelligence, 16*(1), 115.

[5] Cohen, W. (2001, March 6). *Former Defense Secretary Cohen's remarks at the 2001 summit*. George Mason University. Retrieved August 10, 2019, from http://www.gmu.edu/departments/law/////techcenter/programs/summit/cohen's_2001_remarks.html

[6] Coolsaet, R. (2015). *What drives Europeans to Syria, and to IS? Insights from the Belgian case*. Academia Press.

[7] Cronin, B., & Crawford, H. (2007). Information warfare: Its applications in military and civilian contexts. *Information Society, 15*(4), 257264.

[8] Denning, D. (2000, May). Cyber terrorism. Testimony before the Special Oversight Panel on Terrorism," Committee on Armed Services U.S. House of Representatives, Georgetown University, May 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[9] Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *Tenth Annual, 2005 CSI/FBI Computer Crime and Security Survey*. San Francisco: Computer Security Institute (www.gocsi.com).

[10] Jones, A., Kovacich, G. L., & Luzwick, P. G. (2014). *Global information warfare: How businesses, governments, and others achieve objectives and attain competitive advantages*. New York: Auerbach Publications.

[11] Legard, D. (2013, May 14). *Fake bank web site scam reaches U.S*. Retrieved August 10, 2019, from http://www.itworld.com/Tech/2987/030514fakebank

[12] Manap., N.A., & Tehrani, P.M. (2012). Cyber Terrorism: Issues in Its Interpretation and Enforcement. *International Journal of Information and Electronics Engineering*, 2(3), 409-413

[13] Meall, L. (2015). Survival of the fittest. *Accountancy (UK), 103*(1147), 140141.

[14] Parker, D. B. (2012). *Crime by computer*. New York: Scribners.

[15] PCWorld. (2001, November 19). Timeline: A 40-year history of hacking. *IDG News Service*. Retrieved August 10, 2019, from http://www.cnn.com/2001/TECH/internet/11/19/hack.history.idg/

[16] Poulsen, K. (2004, September 27). U.N. warns of nuclear cyber attack risk. *SecurityFocus*. Retrieved August 10, 2019, from http://www.securityfocus.com/news/9592

[17] Rattray, G. J. (2017). *Strategic warfare in cyberspace*. Cambridge, MA: MIT Press.

[18] Stafford, T. F., & Urbaczewski, A. (2014). Spyware: The ghost in the machine. *Communications of the Association for Information Systems, 14*, 291306.

[19] Rogan, H. (2006). Jihadism Online-A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes.

[20] Toffler, A. (2011). *The third wave*. New York: Bantam Books.

[21] Von Behr, I. (2013). Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism.

[22] Warren, M. J. (2013). *The impact of hackers*. Presented at the Second European Information Warfare Conference, Reading, UK.

[23] Warren, M. J. (2015). *Cyber terrorism*. Presented at the Annual Police Summit, Melbourne, Australia.

[24] Weggemans, D., Bakker, E., & Grol, P. (2014). Who are they and why do they go? The radicalization and preparatory processes of Dutch jihadist foreign fighters. *Perspectives on Terrorism, 8*(4), 100–110.

[25] Weimann, G. (2014). *New terrorism and new media* (Vol. 2). Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars.

[26] Wilkinson, P. (1974). *Political terrorism*, London.