2015

Cyberspace: A Venue for Terrorism

David Bieda
Embry-Riddle Aeronautical University, biedad@my.erau.edu

Leila Halawi
Embry-Riddle Aeronautical University, halawil@erau.edu

Issues in Information Systems
Volume 16, Issue III, pp. 33-42, 2015

CYBERSPACE: A VENUE FOR TERRORISM

David Bieda, Embry Riddle Aeronautical University, biedad@my.erau.edu
Leila Halawi, Embry Riddle Aeronautical University, halawil@erau.edu

ABSTRACT

This paper discusses how cyberspace has become a venue for terrorists groups for recruiting and proliferating propaganda and terrorism. Moreover, this study explores how the low cost Internet infrastructure and social media sites (such as Facebook, Twitter, and YouTube) have contributed to their networking and operations due to the convenience, in terms of availability, accessibility, message redundancy, ease of use, and the inability to censor content. Concepts such as cyber-weapons, cyber-attacks, cyber-war, and cyber-terrorism are presented and explored to assess how terrorist groups are exploiting cyberspace.

Keywords: Cyberspace, Social Media, Cyber- Terrorism, Internet Censorship

INTRODUCTION

Society is constantly striving to develop more effective and efficient ways to communicate using technology. However, alongside the race for technology advancement technology, abuse has also increased, particularly cyberspace advanced concepts. Cyberspace is a common site of meeting and interaction between cyberterrorists from multiple cultural backgrounds [27]. Cyberspace is a decentralized global communication platform, where social media and networks are specifically designed to process information flows in real time. Events like 9/11 and the constant threat from extremist groups have made us more aware of the implication of terror and terrorism. By definition, acts of terrorism are a way of coercing an individual or groups into taking particular actions [15]. Organizations that track terrorist acts and hostile groups in the Middle East and Asia report that such groups have been working for years to become skillful in the more advanced technologies in cyberspace [25].

The social network space, including social media and social networking web sites, has heavily influenced the way the Internet is used, and has also affected culture, business, politics and virtually every aspect of modern life [2, 41].In general, the purpose of social media and social networking sites are to enable people to stay informed and connected with their interests or with other people instantly. Social media and networking has become a norm for online collaboration and accessing information instantaneously. The majority of end users are able to stay connected with friends, family, relatives, interest groups, companies, and media outlets. The fast growth of social media data has developed into one of the most active and challenging areas of computer research.

It is expected that terrorist action or threats will leave ripples in the social media landscape. Nearly 90% of organized terrorism in Cyberspace is proliferated through social media [30]. It would seem appropriate that social media and social networking corporations would have a social responsibility to ensure the public is protected from harm, violence, and criminal acts while using their products and services. Yet, social media has been exploited for unlawful use and illegal activities, such as terrorism. For instance, terrorist groups not only use social networking and media sites for posting propaganda and terrorism acts, but for vetting and training new recruits as well [26].

Social media has given us the opportunity to tap into the collective conscience of the Internet and to use that knowledge to enhance national security [15]. As a defensive countermeasure, a number of nations have been prompt to take a proactive stance to protect their culture and national interests through cyberspace censorship, or data content filtering. Different types of censorship have become an acceptable means of blocking content that is not aligned with regulations, culture or values, such examples include but not limited to offensive material or copyright infringement content [4].

The primary focus of this study is to explore how cyberspace has become a venue for terrorist groups to recruit and proliferate propaganda and terrorism. To exacerbate this phenomena, social media corporations are exploring

opportunities to provide third world countries free access to cyberspace. While these efforts are considered capitalistic and could be considered acts of philanthropy, such opportunities may aid, abet, and proliferate terrorism.

The paper begins by reviewing the relevant literature in the area of cyberspace and terrorism. Concepts such as cyber-weapons, cyber-attacks, cyber-war, and cyber-terrorism are analyzed and synthesized into collective definitions attained by authoritative, professional, and academic sources. Preliminary research indicates that these concepts are not consistently defined, therefore, may attribute to mass confusion and inappropriate reactions when such actions are reported to the public. To this point, this research adds to the body of knowledge in this field by recognizing how each cyber attack is currently defined by primary sources. Moreover, this research attempts to discuss the progressive movements made by different parties (corporations, nations, and terrorist groups) using cyberspace to demonstrate how it is being exploited in relation to the proliferation or condemnation of terrorism.

LITERATURE REVIEW

The U.S. government defines cyberspace as "The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, embedded processors, and controllers in critical industries". The focus of this section is on presenting the terminology and concepts recognized and categorized by society as cyber-weapon, cyber-attack, cyber-war, and cyber-terrorism. These concepts are controversial at best, each concept and term will be analyzed in terms of understanding what each means and who performs these actions. Lastly examples will be provided. Table 1 summarizes the main definitions of these concepts.

Table 1. Definitions

Data Breach	A data breach can be a form of cyber-attack into a company's database to extract consumer credit card information, birth dates, medical records, email addresses, logins, passwords, and other personal identifiable data for future criminal use, such as identify theft. 2013 was the year of the mega data breach
Cyber-Weapons	Cyber-weapons as a subdivision of computer code intended to be used with the intention of terrorizing or initiating physical, functional or mental harm to structures, systems, or living beings
Cyberattacks	A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks.
Cyber War	Cyber war is the uses of ICTs within an offensive or defensive military tactic authorized by a government and seeking the direct commotion or domination of the opponents means and sources.
Cyberterrorism	Cyberterrorism commonly implies prohibited assaults and hazards against computer systems, computer networks, and the Internet
Cyber Jihad	A holy war mediated via the Internet
Internet Censorship	Internet censorship is described as a practice or system that inspects content and eliminates items that are deemed aggressive, wicked, damaging to people

2013-2014: The Years of the Mega Breach and the Year of the Hack

A data breach can be a form of cyber-attack into a company's database to extract consumer credit card information, birth dates, medical records, email addresses, logins, passwords, and other personal identifiable data for future criminal use, such as identify theft. 2013 was the year of the mega data breach. Over 552 million identities were stolen in data breaches in 2013, nearly double the count in 2011. The average cost of a data breach was roughly $136 per record [38]. Several big data breaches occurred in 2014. It seemed that no industry went unscathed. The data breaches were broad and deep starting with the high-profile Target breach last December. The US was also rocked by the Michaels data breach, Neiman Marcus, Home Depot, Sally Beauty, PF Changs, UPS, Dairy Queen, Kmart, Staples, USPS, in addition to Sony among others. In other cases, laptops or thumb drives containing information were stolen, in some cases with apparently nothing more than the login password to protect the data. The number of U.S. data breaches tracked in 2014 were 783 in 2014 as released by the Identity Theft Resource

Center (ITRC). This number represents a substantial hike of 27.5 percent over the number of breaches reported in 2013 [47].

Cyber losses may often be of low frequency, but high gravity and in spite of the greatest security restrains money can purchase, no one is really secure. Yet, one thing is definite is that more than one major business took it on the chin in 2014 and additional will certainly follow in the year to come. Keeping a superior multi-year data breach incident database demands continuous care to what is happening in the world of data breaches.
Up to the present time, nobody recognizes the particulars of who the perpetrator was with Sony's case. Queries continue and persist after FBI accuses North Korea with attack on Sony Pictures. What does the Sony breach tell us about what will occur in 2015?

It is important to note though, that attacks or data breaches and terrorism are not the same concept and that cyberattacks are a nuisance and not terrorism [24]. Cyberterrorism, hypothetically, isn't meant to occur. Terrorism, all together, is described as the usage of attacks to initiate instinctive fear. The United States, however, still needs to consider both the risk of future and additional hits like the Sony breach besides additional hasty responses that may result if the glitch of insecurity in cyberspace is pushed into the counterterrorism paradigm.

Cyber-Weapon

One of the main security fears confronting the United States nowadays is how to alleviate its susceptibility to Cyber-weapons [36]. Over the past twenty years, Cyber-threats have progressed from sole hackers inspired by financial reward and fame to planned crime and country actors. The intricacy and abilities of these fears increases in direct fraction to the level of connectivity in society.

There is presently no international agreement concerning the meaning and definition of a Cyber- Weapon as expressed by the Pentagon and the Department of Defense (DoD). Investigators indicate that there are forms of computer code that can be described as a Cyber-Weapon. Rid and McBurney [34] define Cyber-weapons as a subdivision of computer code intended to be used with the intention of terrorizing or initiating physical, functional or mental harm to structures, systems, or living beings [34].

Cyber-weapons may be arranged alongside a scale: on the common low-potential end is malware or malicious software that manipulates a system from the outside but theoretically unable of breaching that system. On the other high-potential end of the scale is malware that operate as an intelligent agent that penetrates protected and physically inaccessible systems and autonomously manipulating output processes.

The data breaches examples presented earlier would count as mental harm to living beings and, at the least, are personally and financially damaging. However, cyber-attacks only caused 34% of the data breaches in 2013; while, 29% were attributed to companies accidentally making sensitive data public [38]. The United States Department of Defense (U.S. DoD) understands these situations and provided further explanation of its lack of recognition of a cyber-weapon as malicious code that can be produced inexpensively and most software could be repurposed for malicious action [8]. As such, the cyber-weapon label is debunked as a misnomer based on this rationale. Hence, the mere fact that computer code can be used for good or bad reasons stresses the significance that intention is the main factor differentiating a cyber-attack from an accident [34].

Because there are no confirmed cases of a large-scale, state-sanctioned cyberattacks except for the speculations that Russia could wage cyber war on the US [42] and the White House Hit of an unclassified Executive Office of the President (EOP) computer network breach [6] , analysts are currently forced to explore different weapon systems and theories to help both the fighter and the politician understand how cyber-weapons can be utilized and what vulnerabilities this new class of weapon create.

Industrial control professionals and academics complain that the information desired to investigate future attacks are being kept out of the public domain. Galante, a past U.S. Department of Defense intelligence analyst stated that cyberweapons provide smaller, poorer countries a means to leverage irregular power against much larger opponents [34]. One sure thing is that the spread of Cyper Weapon will benefit terrorism efforts. The line between what is a cyber weapon and what is not a cyber weapon is subtle though [34].

Cyber-Attack

Approximately, 20% of the cyberattacks listed in the top fifteen countries recorded as the source of cyberattacks by the DTAG sensors originated in the Russian Federation. The first four countries listed, including the U.S., Germany, and Taiwan, accounted for 62% of the cyberattacks represented. The U.S. has been suffering from a "maintained and sustained" cyberattack from China focusing on economic intelligence [48].

Cyberattacks have the ability to disrupt the way in which ordinary individuals live their lives (e.g., the chaos that would arise if none of the automatic teller machines (ATMs) in a country were operational). The interconnectedness of global financial institutions, enabled by modern communications technology, increases this risk [32].

The United States has identified cyberattacks on its critical infrastructure as a matter of national security, and has declared cyberspace a domain of war [31]. Non-kinetic (cyber) cyberattacks appear to be increasing both in frequency and in severity in terms of the potential damage they cause

Most researchers perceived a subjective range assessing the level of severity for a cyber-attack. These severity levels range from low, medium, and high. Low severity level attacks were considered spam, phishing, and denial of service attacks (with and without the use of bots) that were spread to the general public and company websites. Medium severity level attacks were considered targeted malicious intrusions (that do not penetrate or influence a targeted process but can damage it) and spear phishing. High severity level attacks were considered targeted malware using intelligent agents. This type of malware penetrates a protected system and has the system self-inflict damage by shutting down or stopping other processes to keep it inoperable for a period of time [34]. On a side note, it was interesting to find that there was a disagreement about the use of spyware as it not considered a form of cyber-attack, among researchers and the U.S. DoD.

Most if not all researchers also agree with the U.S. DoD about the inexpensive cost of creating malware. Filshtinskiy [12] reported the costs for a number of low severity level cyber-attacks. For example, Denial of Service attacks range from $50- $500 per day, hacking personal email accounts range from $30-$50 per day, fake identification costs less than $30, malware that creates new accounts on popular websites costs less than $500, and custom malware costs $1500 [12]. A key observation is that the prices go up with the customization of the malware. This is in-line with Rid and McBurney's [34] analysis that vicious cyber-attacks pose limited risk. That is, the more finite a cyber-attack target becomes, the more complex coding is required, and the more expensive the malware becomes. "Maximizing the destructive potential…is likely to come with a double effect: It will significantly increase the resources, intelligence and time required to build and deploy…and more destructive potential will significantly decrease the number of targets…" [34]. For these reasons, two significant observations can be made. First, not all cyber-attacks are as severe as broadcasted by the media. Second, high severity level malware is unlikely to be acquired by the common cyber-criminal [34].

The next question becomes who sanctions and performs these cyber-attacks. Most if not all research tend to agree that low severity level cyber-attacks can be sanctioned by anyone, who wants that action performed, and it is usually carried out by a cyber-criminal. When it comes to the medium and high severity level cyber-attacks, most attacks are executed by non-state actors (such as criminal organizations). Seldom, will there be a nation-state associated with a cyber-attack as it is difficult to prove allegations due to the anonymity of the internet. To that point, it is widely known that nation-states stay anonymous and solicit services from non-state organizations. Moreover, cyber-criminals are gathering to work in cyber-crime organizations, instead of working independently, as it reduces the risk of being captured [12].

Cyber-War

Same as all the other wars occurring in the world, cyber war could also be harmful for many people except those who manufacture weapons and profit from the wars. During the previous decades, information and communication technologies (ICTs) did successfully prove that they are useful and convenient to be engaged in war. Therefore, they have been deployed in so many wars since the second Iraq war [33].
According to [39], "Cyber war is the uses of ICTs within an offensive or defensive military tactic authorized by a government and seeking the direct commotion or domination of the opponents means and sources.

Cyber-war is a highly problematic serious concept. Rid and McBurney [34] state that an act of war should be contributory, political and possibly disastrous and fatal, whether in cyberspace or not. No impartial cyber-offence on files meets these principles, consequently 'cyber-war' stays an allegory in the interim [34].

The U.S. DoD seems to be in general agreement with this statement [8]. Yet, other researchers delineate factors leading up to cyber war, which include (but not limited to) system breaching for damage or disruption (sabotage), the preparation of war (cyber-espionage), and cyber-attacks.

There does appear to be general agreement with the concept of using an orchestrated attack sequence of both cyber and physical forms. Moreover, these actions are commonly termed kinetic (physical) and non-kinetic (cyber) actions. An example that is often used to illustrate is the Israeli attack on the Syrian air defense system in 2007. The Israeli military operations orchestrated a two-step attack. First, they shutdown Syrian air defense system using a cyber-attack. The goal was to shut down the entire air defense radar station and make the active system in display as a no approaching airplanes to Syrian operators for a limited time. Then, the Israeli jets flew in to destroy the Syrian targets [34]. However, it should be noted that no nation or state has responded to a lone non-kinetic attack with a retaliatory kinetic attack to date [45].

Cyber-Terrorism

As our reliance on electronic networking has expanded significantly, cyberterrorism is developing into a dangerous threat to both open and secured infrastructures and to any modern state [1, 28]. Every country has its peculiar regulations, protocols and policies to counteract this type of assaults. Terrorist groups drew the interest of several academics, authorities and intelligence officials [3]. There does seem to be contemplation from the U.S. DoD that there could be a 'Cyber Pearl Harbor' in the near future, not performed by a nation-state but by violent extremist groups [14].

Cyberterrorism is hard to describe since this notion lacks a commonly established meaning [19]. Cyberterrorism commonly implies prohibited assaults and hazards against computer systems, computer networks, and the Internet [5]. In the meantime, most descriptions of terrorism defines terrorism as an deliberate action or undertaking that generates terror and distress, propelled by a dogmatic, ideological, or spiritual purpose, compared to a hate offense [19]. Cyber-terrorism may be expressed as the usage of any information technology by terrorists [13].

The objective of cyberterrorists is comparable and that is to initiate terror by threatening or forcing a government or its citizens in continuance of objectives [7, 11].

With fairly recent stories involving serious attacks on Sony and its PlayStation Network, Microsoft's Xbox Live network, alongside other high profile attacks on the Tor project and North Korea's Websites, has cyber-terrorism become a very real and dangerous reality for enterprises to battle alongside other threats?

Social Media

Within the Cyber Warfare society, there are numerous terms that became extremely prevalent. For example, Cyber Jihad/Terrorism, Online Extremist and Radicals.

This is a modern era where societies are more connected than they have ever been and is becoming a predominant part of many culture including the American Culture. The advent of websites like Facebook, Twitter, Instagram, LinkedIn, YouTube and the like revolutionized the mode of connection of people with their close friends and the rest of the world. Social media makes it fast and easy to locate support for almost any group, cause or idea even terrorism.

The increasing number of people and continuous use of social media generates an opportunity for both the government and private businesses to connect and engage with the public in addition to producing countless novel occasions for terrorist groups to enroll and radicalize new supporters [10].

Terrorist groups are cognizant of that and strive to benefit from it. The physical gap is no longer a barrier and does not constraint them and their recruitment attempts. Social media lets terrorist groups recruit without having the need to see the person. Findings have revealed that an individual may be radicalized with the absence of any physical communication. Social networking technologies are free and easy to use, permitting sites to be literally generated in couple minutes. If an extremist social networking site is taken down, another one can be created in less than ten minutes.

Lately, the Islamic State of Iraq and Syria (ISIS) utilized social media widely for both enlistment and to transmit a message. They circulated a number of videos on YouTube highlighting executions they normally perform. ISIS is extremely vigilant with their arrangements and propagation as a lot of their hype on social media is crafted well and has been in English and repeatedly are trying to engage the Western World. Formerly ISIS and different jihadist groups networked in murky online forums that were merely called on by other jihadists. Nowadays, they are exploiting Twitter and Facebook broadly and significantly. This approach has earned them substantial international attention.

Cyber-Jihad

Terrorist groups (such as al-Qaeda and ISIS) have not launched a cyber-attack to cripple the Internet and make it dysfunctional nor a cyber-war such as 'Cyber Pearl Harbor' or 'Cyber 9-11'.

Custom malware (using intelligence agents) on a specific target is quite expensive and the resources and skill levels needed to build such devices are scarce and hard to acquire. Moreover, cyber-attacks need to be continuously innovative and terrorists groups (such as al Qaeda and ISIS) have been downsized over the past decade due to military strikes. Cyber-Jihad is a holy war mediated via the Internet.

An inference can be established that cyberspace is not a primary target for terrorist groups. Rather, cyberspace has become a hot spot for proliferating propaganda and recruiting. It is in the best interests of the terrorists groups for the Internet to thrive and prosper. For instance, the 'Cyber-Jihad' movement is directed against the United States and its allies that oppose a 'pure Islamic nation' [16]. This group is using the Internet to reach ideological and political goals [16].

The proliferation of propaganda has evolved from video, to internet forums and chat rooms, to social media. In 2001, Al-Qaeda needed to find a new way to communicate with the public when it was expelled from Afghanistan. As a result, video tapes were sent to the Al-Jazeera news group for broadcasting. However, over time, Al-Jazeera stopped airing the videos due to public relation concerns. This action forced the group to use closed Internet forums and chat rooms, where participants were vetted and a referral program was used to authorize access. However, these forums and chat rooms were constantly shutdown by governments and under cyber-attacks from opposing parties. Eventually, Al-Qaeda moved to social media where all the news media groups and general public also convened [22]. The *jihadist* rebels in Syria and Iraq exploit all types of social media applications and file-sharing platforms including Ask.fm, Facebook, Instagram,WhatsApp, PalTalk, kik, viper, JustPaste.it, and Tumblr.

According to Marcu & Balteanu, [26], social media offered decentralized control on content and built-in message redundancy. These features are favored by terrorists groups of all kinds as this situation has not only flourished these groups to disseminate propaganda to a worldwide audience, but enabled better communications with their teams and new recruits using encrypted lines as well [22]. In regards to recruitment, terrorist groups use social media to recruit worldwide. Just as with propaganda, recruiting costs are also at low costs as social media sites are advantageous in this aspect. As a result, it appears that more women are recruited to support the intelligence domain [26]. As reported by Klausen [22], Website supervisors in back offices incorporate the twitter feeds of frontline rebels with YouTube uploads and broadcast them to widespread watchers. These back-office supervisors are usually wives and adolescent female followers and defenders [22].

In particular, Twitter has become one of the preferred social media sites of choice by terrorists. Generally, social media sites require either a wireless communications (LTE) or wi-fi access but Twitter can be used without any as the application is designed for cell phones with SMS text messaging. Further, posting can contain images or text, links to other media sites, which may be forwarded to everyone in an address list (redundancy). For instance,

executions are disseminated via Twitter by tweeting pictures and video of these acts. The effectiveness with capturing and distributing these acts of violence using Twitter has been reflected by gaining the attention of the general public (proliferating their propaganda) and with gaining new recruits worldwide [22].

Internet Censorship

Internet censorship has been practiced in many different ways by many different nations in a discrete and secretive manner. Internet censorship is described as a practice or system that inspects content and eliminates items that are deemed aggressive, wicked, damaging to people [29]. On its own right, censorship is lawful when a government does it clearly, defines plainly the matter it impedes, attentively pursues merely banned material, and offers liability in its decision-making to the people it [4].

Internet censorship has gone through three major versions since the internet's inception. The first version of internet censorship prevented access to online material. This version was applied prior to the release of the internet to the general public. The second version was practiced by non-democratic governments, where they controlled how and what content was filtered. However, this version was superseded in 2007 by the third version, where all governments are engaged in content filtering. Today, nations have taken four main approaches to internet censorship – outsourcing, positive information insertion, informal pressures, and relabeling this action to something more acceptable [4].

Previously, governments owned the responsibility of controlling and managing internet censorship. However, nowadays, the activity is outsourced to commercial internet service providers (ISPs) as it became costly to maintain and difficult to uphold in government budgets, for various reasons. Therefore, relationships have formed with ISPs, where ISPs have been tasked to manage censorship practices; while, the government controls what content to censor.

This new relationship afforded governments the flexibility to mandate censorship practices on ISPs instead of gaining approval from other government branches. For example, the Obama administration failed to have a new copyright alert system approved by other U.S. government branches and the European Union. As a result, the administration pushed, by threat, the alert program to the ISPs to enforce. Another example of this flexibility can be seen with the Australian government. The Australian government rejected internet filtering, where again, its residing administration delegated Australian ISPs to enforce internet censorship.

In an effort to mitigate citizen unrest from internet censorship, governments re-branded this act to be in the best interests of the general public. For instance, the Obama government masked its copyright alert system to be labeled as a 'robust intellectual property enforcement'. Likewise, Russia labeled their censorship practice as the 'right to be protected against harmful content' [4].

A different application of internet censorship can be seen with the Chinese government's implementation in an effort to protect its best interests. China's censorship technology is considered the most sophisticated filtering technology in the world. As with other governments, the Chinese government used to have full control of managing the censorship activities. However, unlike other governments, they delegated the work to state-owned ISPs, where the state owns 51% majority share of each ISP. In essence, the Chinese government is in full control of managing these operations [46].

Projects like 'Gold Shield' embarked to filter 'sensitive' internet content, where the definition of 'sensitive' rapidly grew to include many subjects. The software program was designed to interrogate content, locate sensitive words, and block the content from Chinese web surfers. Further, this program even filtered content prior to it posting onto the web and blocked entire web sites and domains. Lastly, the Chinese government also hired internet administrators to act as web crawlers to manually delete or hide 'sensitive' posts and comments against the nation's interests and were authorized to plant positive comments and posts instead. While the Chinese government takes an aggressive position with internet censorship, the question remains if it is in the best interests of the nation to intentionally mislead their citizens as trust issues will likely develop over time [46].

When it comes to internet censorship, it does appear that nations take the position that the ends justify the means. Moreover, this leaves one to posit that this practice could be an effective way to suppress terrorist propaganda and communication system used on social media sites (as was enforced onto ISPs for other subject content). Yet, there is likely a high probability that greater unintentional damage will result due to the sheer disregard of misleading and misinforming the public of the cruel actions and intentions performed by terrorists. So then, it leaves one to wonder if internet censorship provides a worthwhile return on investment or does it do more harm than good.

CONCLUSION & FUTURE RESEARCH

Cyberspace's complexity challenges various conventional notions of security and military strategies. Cyberspace and specifically social media, has been embraced by terrorist groups. As stated by Chris Collison interview [21], social media has become an enabler, a disrupter, and a connector of bringing people together. Terrorist groups illustrated this point by networking, communicating operations, proliferating propaganda, and mass recruiting through social media sites.

While social networks have taken actions against terrorist and extremist groups, outlining usage guidelines and barring the usage of their services to endorse terrorist undertakings, actually there are numerous problems in their attempts to execute these measures, due to the impracticality of censoring and checking in real time a considerable volume of information produced by users [26]

Suggested research in the area includes an assessment on the impact of the terrorist propaganda delivered through social media and how it politically influences governments and its citizens to behave. In addition, it would be interesting to learn the qualitative and quantitative results of recruits joining terrorist groups via social media. This study would centers on the effectiveness of using, or the success rate, social media for recruiting people with different cultures, languages, and diverse skills worldwide. Lastly, research should be done to understand the best defenses to render these types of terrorist group engagement activities ineffective and useless.

A future direction of this topic leads one to venture into understanding the social responsibility of social media companies in regards to terrorist groups. In other words, how should social media sites filter or handle content from terrorist groups, especially since companies are enabling internet access to third world countries [43]. This may also lead the discussion into internet censorship and how some governments may take proactive measures with these practices (with the help of ISPs and social media companies) to deter terrorist groups from exploiting social media.

REFERENCES

1. Axelrod, E. M. (2009). Violence goes to the Internet: Avoiding the snare of the net. Springfield, IL: Charles C. Thomas Publisher.
2. Azimi,A.; Moshfeghi, Y. & Rijsbergen, C. J. (2009), SugarCube: quantification of topic propagation in the blogosphere using percolation theory. SIGIR Pg. Conference Proceedings, 786.
3. Baggili, I. (2009) . "Self-Reported Cyber-crime: An Analysis on the Effects of Anonymity and Pre-Employment Integrity", Cyber Criminology (IJCC), 3, 974–2891.
4. Bambauer, D. E. (2013). Censorship v3.1. Internet Computing, IEEE, 17(3), 26-33. doi:10.1109/MIC.2013.23
5. Bradley, A. K. (2012). *Anatomy of Cyberterrorism: Is America vulnerable?* New York, NY: BiblioScholar
6. Cluley , G. (2014). White House hit by "sustained" cyber attack, hackers breach unclassified network. Available: http://www.welivesecurity.com/2014/10/29/white-house-hack
7. Conway, M. (2002). What is Cyberterrorism? *Current History, 2*, 436–440.
8. Department of Defense. (2011a). Department of Defense Cyberspace Policy Report. Retrieved from Department of Defense website: http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf
9. Department of Defense. (2011b). *Department of Defense Strategy for Operating in Cyberspace*. Retrieved from Department of Defense website:

http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf

10. Department of Homeland Security (2014). http://www.dhs.gov/topic/cybersecurity
11. Dunnigan, J. F. (2003). *The next war zone: Confronting the global threat of cyberterrorism.* New York, NY: Citadel Press.
12. Filshtinskiy, S. (2013). Cybercrime, cyberweapons, cyber wars: Is there too much of it in the air? *Communications of the ACM, 56*(6), 28.
13. Ganji, M., Dehghantanha, A., IzuraUdzir, N., & Damshenas, M. (2013). Cyber warfare trends and future. *Advances in Information Sciences and Service Sciences, 5*(13), 1-10. Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1538588335?accountid=27203
14. Garamone, J. (2012, October 11). Panetta Spells Out DOD Roles in Cyberdefense. *American Forces Press Service* [Washington D.C]. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=118187
15. Gonzalez, S., N. (2012). *Data mining social media networks for terrorist events indicators* (Order No. 1535359). Available from ProQuest Dissertations & Theses Global. (1335897516). Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1335897516?accountid=27203
16. Heickerö, R. (2014). Cyber terrorism: Electronic jihad. *Strategic Analysis, 38*(4), 554-565. doi:10.1080/09700161.2014.918435
17. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993. doi:http://dx.doi.org.ezproxy.libproxy.db.erau.edu/10.1016/j.jcss.2014.02.005
18. Jarvis, L., & Macdonald, S. (2014). What is cyberterrorism? Findings from a survey of researchers. *Terrorism and Political Violence,* , 1; 1-22; 22.
19. Juergensmeyer, M. (2000). Terror in the mind of God. Berkeley, CA: University of California Press
20. Kaplan, 2008; Ante, Grover & Green, 2007; Kelleher, 2008).
21. Kanti, P. (2010, March 8). *Role of Technology in Knowledge Management* [Video file]. Retrieved from https://www.youtube.com/watch?v=jir_x1BXbUw
22. Klausen, J. (2015). Tweeting the jihad: Social media networks of western foreign fighters inSyria and Iraq. *Studies in Conflict & Terrorism, 38*(1), 1-22.doi:10.1080/1057610X.2014.974948
23. Kshetri, N. (2013). Cyber-victimization and cybersecurity in china. *Communications of the ACM,* 56(4), 35-37.
24. Libicki, M. C. (2009). *Cyberdeterrence and cyberwar.* Santa Monica, CA: RAND Corporation
25. Maniscalco, P. & Christen, H.T. (2001). Understanding Terrorism and Managing the Consequences. Prentice Hall Publishing, Upper Saddle River, NJ 07458.
26. Marcu, M., & Balteanu, C. (2014). Social media-a real source of proliferation of international terrorism. Annales Universitatis Apulensis : Series Oeconomica, 16(1), 162-169. Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1555353946?accountid=27203
27. Matusitz, J. (2014). The role of intercultural communication in cyberterrorism. *Journal of Human Behavior in the Social Environment, 24*(7), 775-790. doi:10.1080/10911359.2013.876375
28. Matusitz, J. (2008). Cyberterrorism: Postmodern state of chaos. *Information Security Journal: A Global Perspective, 17*(4), 179–187.
29. Merriam-Webster. (2015). Censorship - Definition and More from the Free Merriam Webster Dictionary. Retrieved from http://www.merriam webster.com/dictionary/censorship
30. Mielach, D. (2012, January 9). Terrorists Seek Out 'Friends' on Facebook. Retrieved from http://www.businessnewsdaily.com/1877-terrorist-social-media.html
31. O'Harrow, R. Jr. (2013). *Zero Day: The Threat in Cyberspace*. New York, NY: Diversion Books, Washington Post E-Book.
32. Orman,L. (2013). "Technology as Risk," *IEEE Technology and Society Magazine*, 23–31.
33. Paul, F. (2012) "Cyber War, Formal Verification and Certified Infrastructure", Springer Berlin Heidelberg, 7152, 1–1.
34. Rid, T & McBurney, P. (2012). Cyber-weapons. *The RUSI Journal, 157*(1), 6.

35. Roberts, P. (2014). If this is a Cyberwar where are the Cyber weapons? *MIT Technology Review*, Retrieved from http://www.technologyreview.com/news/523931/if-this-is-cyberwar-where-are-all-the-cyberweapons/
36. Rustici, R. M. (2011). Cyberweapons: Leveling the international playing field. *Parameters, 41*(3), 32-42. Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/928971315?accountid=27203
37. Shaerpour, K., Dehghantanha, A., & Ramlan, M. (2014). A review on cyber warfare trends. *Journal of Next Generation Information Technology, 5*(1), 65-77. Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1511799159?accountid=27203
38. Symantec. (2014). *Internet Security Threat Report 2014*. Retrieved from Symantec Corporation website: http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v19_21291018.en-us.pdf
39. Taddeo, M. (2012) "Information Warfare: A Philosophical Perspective", Philosophy and Technology, 25(1), 105–120.
40. Twitter. (2015). The Twitter Rules. Retrieved from https://support.twitter.com/articles/18311 the-twitter-rules#
41. Verton; 2013. http://www.hstoday.us/blogs/critical-issues-in-national-cybersecurity/blog/terrorists-use-of-web-social-media-expanding-rapidly/fa6512335287c102954b03e8f2b3c1e2.html
42. Verton, D. (2003). *Black ice: The invisible threat of cyber-terrorism*. New York, NY: McGraw-Hill.
43. Winkler, R., Rusli, E., & Pasztor, A. (2015, January 19). Google Nears $1 Billion Investment in SpaceX. *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/google-nears-1-billion-investment-in-spacex-1421706642
44. Woodyard, 2014 http://www.usatoday.com/story/money/business/2014/04/30/russia-cyber-attack/8500661/
45. Zeadally, S., & Flowers, A. (2014). Cyberwar: The what, when, why, and how [commentary]. *Technology and Society Magazine, IEEE, 33*(3), 14-21. doi:10.1109/MTS.2014.2345196
46. Zheng, H. (2013). Regulating the internet: China's law and practice*. *Beijing Law Review, 4*(1), 37-41. Retrieved from http://search.proquest.com.ezproxy.libproxy.db.erau.edu/docview/1350366855?accountid=27203
47. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html
48. http://www.ibtimes.com/obama-says-cyberterrorism-countrys-biggest-threat-us-government-assembles-cyber-warriors-1556337