

Regis University

ePublications at Regis University

Regis University Student Publications
(comprehensive collection)

Regis University Student Publications

Fall 2014

The Day of the Cyber Wolf

Ryan K. Buch
Regis University

Follow this and additional works at: <https://epublications.regis.edu/theses>



Part of the [Criminology and Criminal Justice Commons](#)

Recommended Citation

Buch, Ryan K., "The Day of the Cyber Wolf" (2014). *Regis University Student Publications (comprehensive collection)*. 210.

<https://epublications.regis.edu/theses/210>

This Thesis - Open Access is brought to you for free and open access by the Regis University Student Publications at ePublications at Regis University. It has been accepted for inclusion in Regis University Student Publications (comprehensive collection) by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

The Day of the Cyber Wolf:
Examining the Danger of Lone Wolf Terrorists and Cyber Terrorism
by
Ryan Sean Krol Buch

A Research Project Proposal Presented in Partial Fulfillment
Of the Requirements for the Degree
Masters of Criminology


REGIS UNIVERSITY

December, 2014

The Day of the Cyber Wolf:
Examining the Danger of Lone Wolf Terrorists and Cyber Terrorism
by
Ryan Sean Krol Buch

has been approved
December, 2014

Approved:


_____, Faculty Facilitator


_____, Thesis Advisor


_____, Faculty Chair

Abstract

Terrorism has become a concern for public safety and security and can take on many appearances. However, in recent years the dilemma that presents the most substantial endangerment to public security comes from the threat of leaderless terrorists, also known as “lone wolves.” Due to the rapid advancement in technology over the past few decades, societies, specifically the United States, have become dependent upon it economically and socially. Terrorist organizations, as well as the lone wolf terrorist, understand that their enemies rely on technology in order to function and have recently redirected their efforts towards cyberspace. As a result, cyber-terrorism has become one of the greatest imminent threats to national security. This literature review presents an analysis of the issues and challenges faced in dealing with modern day terrorism in the forms of lone wolf terrorism and cyber terrorism. Why has this increase in lone wolf attacks occurred? Why are lone wolf terrorists more dangerous than terrorist organizations? What threat do cyber terrorist attacks present to the world, specifically from lone wolves? Why should cyber terrorist attacks be as great a concern as physical attacks? How can both of these forms of terrorism actually have an effect on society and a government’s infrastructure? Lone wolf terrorism presents a clear and imminent threat to national and international security. In light of this, the following research seeks to answer the question: Is there an imminent threat that the next major terrorist attack will come from a lone wolf cyber terrorist? An in-depth understanding of previous lone wolf terrorists and cyber terrorism, as well as the attacks that have been committed, is needed in order to combat future problems.

Keywords: Terrorism, lone wolf, cyberspace, cyber terrorism, leaderless resistance.

TABLE OF CONTENTS

	Page
Abstract.....	2
Chapter	
1. INTRODUCTION.....	4
Statement of the Problem	5
The Problem Significance	6
Definitions.....	7
Limitations.....	8
Chapter Summary.....	12
2. REVIEW OF LITERATURE.....	13
Defining Lone Wolf Terrorism	13
Pyschopathology of Lone Wolves	16
The Rise of Lone Wolf Terrorism	17
Terrorism in Cyberspace	20
The Devastating Capability of Cyber-Attacks	23
Hackers and Hacktivism	23
Chapter Summary.....	28
3. RESEARCH PROCEDURES	29
Research Methodology	29
Sample.....	31
Instrumentation.....	32
Data Collection	33
Data Analysis	33
Chapter Summary.....	34
4. CASE STUDIES	35
Timothy McVeigh	35
Eric Rudolph.....	37
Anders Breivik.....	40
Tsarnaev Brothers	44
Analysis of the Lone Wolves	49
Hacktivism and the “Anonymous” Hacker Network	59
Analysis of the Hacktivist Network.....	60
Analysis of a Potential Lone Wolf Cyber Terrorist Threat.....	62
Chapter Summary.....	72
5. DISCUSSION.....	76
Conclusion.....	82
REFERENCES.....	86

Chapter 1

INTRODUCTION

Terrorism is a problematic topic of discussion causing fear and panic in everyday life. Criminological researchers and law enforcement agencies have treated terrorism as an area of significant interest and a dangerous phenomenon since the dawn of the 21st century. It has become a main focus for law enforcement agencies since the attacks on 9/11. They understand that terrorism is focused on generating fear and causing chaos. Those who utilize terrorism as a tactic want to instill fear in order to alter a social or political outcome. In the past, terrorism focused on military and government officials as targets. American independence came to be as a result of terrorist acts in order to change British rule, as displayed in the Boston Tea Party and attacks on British troops and officials. However, the acts of terrorism have changed over the years. Most attacks we see committed by terrorists today have become brutally violent and involve innocent civilians as victims. Although the victims of these attacks see it as hideous or unjust, the perpetrators view it as liberation in the fight for their cause. “One person’s terrorist is another person’s freedom fighter” (Marsella, 2004, p. 15). Terrorists are highly motivated and use symbolic attacks to make a statement. When most Americans think of terrorism today they think of attacks committed by terrorist organizations similar to the September 11th attacks caused by Al Qaeda or the Islamic Militant State ISIS currently wreaking havoc and attempting to take control in Iraq and Syria. However, most terrorist attacks that are committed in the United States have been carried out by leaderless individuals known as “lone wolves” and have utilized a number of different tactics and devices that were available to them in order to fulfill their goals (Bartol & Bartol, 2011; Spaaij, 2010).

State of the Problem

Since 9/11, terrorism has been a cause of major concern and the main focus for many law enforcement agencies. Terrorism lives and thrives off of fear. Terrorists want to instill fear in order to alter a social or political outcome. This fear is created through propaganda as well as violent attacks towards both government/military personnel and innocent civilians. In the past, attacks were predominately being committed by terrorist organizations and extremist groups. However, a shift has occurred in the past few decades with a number of attacks now being committed by leaderless individuals who seek to create chaos and change the social order of the world. Statistics have shown that a majority of terrorist attacks that are being committed outside the Middle East, and more specifically in the United States, are being committed by lone wolf actors with no direct ties to any organization. These lone wolves, like their terrorist brethren, are highly motivated and organized with a strong conviction to a cause and a willingness to fight and even die for it. But unlike the average terrorist, “lone wolf operators do not rely on group or organization affiliations to validate their missions” (Bartol & Bartol, 2011, p. 337). Lone wolves believe in their cause whole-heartedly and will use any means to have it fulfilled. This has prompted them to branch out and utilize whatever tactics or weapons that are at their disposal. Historically, terrorists have used guerilla warfare, propaganda, violent scare tactics and destruction of supplies to fulfill their agendas and fight their enemies. However, as technology in society has progressively changed, so have the terrorists’ tactics; with the most recent use of homemade elaborate bombs, mass shootings with machine guns in public places and using vehicles in the destruction of buildings. Lone wolves have utilized the same types of tactics to complete their agenda. Still, one of the ultimate goals for a terrorist is to spread their beliefs and

voice their perceived transgressions. This, due to advancements in technology, has caused terrorists to focus their efforts on the platform of cyberspace. They are exploiting this new realm for the purposes of spreading their ideals to a broader audience and launching terroristic attacks against their perceived adversaries. Cyber terrorist attacks have the potential to disrupt the financial market, interfere with services, destroy computer files and networks, and cause widespread panic among citizens and businesses. "The driving force behind cyber terrorism is primarily politically and/or religiously based. Many times, cyber terrorists commit forceful acts via cyber space in order to gain attention for their cause" (Jain, 2005, p. 3). It is then only natural for many lone wolf terrorists to engage in this new form of terrorism as a means to display their frustration or support their cause. Thus, creating the potential threat that certain lone wolves will no longer learn to just be bomb makers but develop into computer hackers.

The Problem Significance

The purpose of this project was to determine the probability that the next significant terrorist attack to occur in the United States will be committed by a lone wolf terrorist(s) who utilizes cyber terrorism or a combination of a cyber-attack with a physical attack to fulfill their cause and create social change. The research question encompasses the realistic threat that both lone wolf terrorism and cyber terrorism present to the world. Though acts of terrorism have occurred throughout history, the attacks committed by lone wolf terrorists have radically increased in recent years with the potential to continue to rise in years to come. Terrorism incorporates many disciplines and as technology advances and society develops, the tactics utilized by terrorists change and become modernized. Not only can technology and the Internet be used to spread the beliefs of a terrorist or terrorist organization, it has the potential to serve as another terroristic tactic. Cyber terrorism has emerged as a new means of engagement in the

name of the terrorist's beliefs. Government agencies and organizations have identified that the infrastructures of both businesses and countries are possible targets for cyber-attacks due to the dependency on technology. The potential, as assessed from previous international computer viruses, can be catastrophic to a country's social and economic system. However, a lone wolf hacker has the potential to present an even greater threat. This is because lone wolves are less likely to care about the damage they will cause to innocent bystanders in the name of their extremist beliefs when committing these acts. Thus, the need to gain a better understanding of these threats and the individuals who engage in these types of activities is vital in order for law enforcement and government agencies to assess the probability of future attacks and formulate viable operational plans to counter them.

Definitions

Terrorism is a social phenomenon which cannot be boiled down to the violation of one law or rejection of a specific view of the world. As a result, law enforcement professionals, government agencies, researchers and political organizations have not agreed upon a way to define terrorism. One of the main reasons for this confusion is due to the fact that terrorism is in the eye of the beholder. What one person or country may view as an act of terrorism another may see viewed as acts of war or liberation (White, 2003). The word and meaning of terrorism can also shift as societies change. However, the one consensual identifiable factor is that terrorism utilizes fear and intimidation in order to create social or political change

For the purpose of this capstone research project, the term lone wolf terrorism will be referred to as an attack committed by an individual or small group of individuals who have no direct ties to a terrorist organization or extremist group. The attack committed by the individual or individuals will be premeditated and designed as a retaliation for a perceived grievance.

Terrorism incorporates many disciplines and has been around for centuries. However, as technology advances and societies develop, the tactics of the terrorists or terrorist organizations evolve and become more efficient for the present day. Technology and the Internet can not only be used to spread the beliefs of a terrorist or terrorist organization to gain support and demoralize enemies, it also has the potential to serve as another venue to launch terroristic attacks. For the purpose of this capstone research project, the term cyber terrorism will refer to the use of digital technology as a means of creating political, religious or ideological changes in the world in the form of cyber-attacks. The term cyber-attack will refer to any digital attack that occurs in cyber-space. These attacks can be in the form of malicious software/computer viruses, email bombings, denial of service attacks, and defacing/disrupting Websites. They are designed to disrupt, alter, cripple or destroy information and infrastructures.

Limitations

In most social research studies, the researcher must address the confidentiality, voluntariness and accuracy of the information. However, due to the fact that this research study was based primarily on secondary qualitative analysis some of the common research practices did not need to be adopted. Still, there were several other limitations that needed to be addressed pertaining to the research on lone wolf and cyber terrorism.

One the biggest concerns with conducting research on lone wolf terrorism and cyber terrorism were the inconsistencies in their description and meaning. Though there is a sufficient amount of research and documentation on lone wolf terrorism, there is still no set definition as to what lone wolf terrorism actually is or entails. Some researchers have identified lone wolves as having no affiliation, direct or indirect, to a terrorist organization; while other researchers have identified some lone wolves as having an affiliation to a terrorist group but whose attack and

activities were conducted alone. There was also an inconsistency in which type of incidents are considered lone wolf attacks. Some authors and researchers have considered attacks by single individuals who were not as high profile as lone wolf terrorist attacks, while other studies have not even acknowledged those incidents in their findings (Chermak, Freilich, & Simone, 2010; Spaaij, 2010). This made it difficult to identify the difference between a lone wolf terrorist and a mass murderer, disgruntled civilian or even serial killer. Though deemed a serial killer by many psychologists and researchers, John Allen Muhammad a.k.a the D. C. sniper, could have been considered by some to be a lone wolf terrorist based on the inconsistent definition among researchers. The one constant characteristic in the studies on lone wolf terrorism was that it involves an individual or small group of individuals who engage in an attack or crime in the name of a cause (Bartol & Bartol, 2011; Chermak et. al, 2010; Spaaij, 2010). The lack of a definition limited the number of individuals who researchers would consensually agree were in fact lone wolf terrorists. This may also cause certain researchers to discredit my findings due to conducting a case study on individuals who they may not deem to be lone wolf terrorists.

There were similar inconsistencies in regards to cyber terrorism. An act of terrorism can be clearly outlined. "Terrorism is defined as the actual or threatened use of violence by an individual or group motivated by ideological or political objectives" (Taylor, Fritsch, Liederbach, & Holt, 2011, p. 20). However, there was no distinct definition of cyber terrorism. Some researchers may consider certain digital attacks such as shutting down email systems and banking networks as acts of terrorism, while others would not because no one is being terrorized (Taylor, et. al, 2011). This potentially skewed the numbers as to how many terroristic attacks have actually occurred in cyber space. Furthermore, some researchers may identify cyber

terrorism as a threat that is drastically on the rise in recent years, while others may see it as a danger that has only slightly increased in recent years.

Another ethical issue that was faced with conducting a case study on lone wolf and cyber terrorism is the dilemma of confidentiality. Due to the fact that my research was an investigation of common themes among four known lone wolf terrorists and comparing and contrasting their criminal behavior and activities, it was impossible to keep their names confidential. This was due to the high profile nature of their attacks as well as the amount of media attention they received. Each of their attacks was publicized across news media outlets and their cases have been and continue to be researched to this day. As a result, specific and general characteristics addressed in each case study would have allowed the reader to identify each terrorist regardless of stating their name. However, confidentiality was not a major issue in regard to my research because all of the material and data used pertaining to each lone wolf terrorist has become public knowledge and is already available to the world.

Secondary analysis has become very useful in the social science community with the examination of qualitative and quantitative research that has already been conducted. Conducting a secondary analysis offers an outside perspective on the study and allows the investigator to look at the research from a different angle (Babbie, 2010). This type of analysis also allowed the researcher to compare and contrast different studies and develop future direction on the subject. Of course, there are certain drawbacks to any form of research. Even though the documents and information obtained for my capstone study includes research and material that was readily available to the general public there are still ethical concerns that come from secondary analysis. For one, is the information accurate? Modern technology has granted both the research community and the general public instant access to a plethora of information. This

research study could have used information obtained through the Internet, social communication networks, digital blogs, search engines and information posted on Web pages. But in doing so I would not have been able to verify if the information obtained from these locations were valid and accurate? Whether or not the information was based more on fact or opinion? If my investigation utilized documents that are not accurate in their findings and were based more on opinions instead of facts, then my research would have become comprised and deemed unethical due to carelessness (Babbie, 2010). However, this issue was resolved by utilizing peer reviewed scholarly journals and published books to conduct my case study research.

Lastly, there is a concern that presents itself that is more of a political issue than an ethical one. This research topic was designed to benefit the world, specifically the law enforcement community, by helping to gain a better understanding of the realistic threat lone wolves present and encourage further discussion on policing the threat and protecting the nation. Unfortunately, this research could also benefit the terrorist community as a whole and more specifically lone wolf terrorists. Just as information, technology, equipment, methods, etc. are developed for the betterment of humanity, the criminal element is able to find a way to exploit it and/or use it to their advantage. The information presented could identify common characteristics among lone wolves and who to target their recruitment efforts towards, as well as learning from the mistakes committed by lone wolves and cyber terrorists in the development of future attacks. Still the benefit of the research outweighs the negative possibilities that can come from it. It is better to know as much information about your enemy and the threats that they present to you than to go around blind eyed to the danger ahead.

Chapter Summary

Is there an imminent threat that the next major terrorist attack will come from a lone wolf cyber terrorist? The phenomenon of lone wolf terrorism and cyber terrorism are threats that have come to fruition in recent years. The rapid increase in lone wolf attacks and the threat level they present to the world has become a concern for national and international safety. In addition, government agencies and organizations have also identified that the infrastructures of both businesses and countries are potential targets for cyber-attacks due to their dependency on technology. Law enforcement and government agencies must evolve their efforts to adapt to the combination of old threats with the new ones they face today. In order for the law enforcement community to better prepare for and defend against such attacks, a more profound understanding of the subject matter must be gained.

Chapter 2

Literature Review

The literature review was accomplished with the assistance of the Regis University online library and the Google search engine, which were able to offer valuable research material. The databases that were utilized as a part of this research include: Academic Search Premier, EBSCOhost, and SAGE Journal. All databases provided resources, articles, data and insight on the topics of lone wolf terrorism and cyber terrorism.

The key words used when conducting the search include “lone wolf terrorism”, “lone wolf terrorists”, “terrorism”, “cyber terrorism”, “cyber attacks”, “leaderless resistance”, “terrorism in cyberspace”, and “hackers.” These keywords allowed for the retrieval of available articles which offered useful information for my research. The articles provided valuable material about lone wolf terrorism and cyber terrorism, the psychopathology of individuals who engage in this type of terroristic activity, information about past lone wolf terrorists, details about past lone wolf and cyber terrorist attacks, and law enforcement perspective on the threat of both.

Defining Lone Wolf Terrorism

A lone wolf terrorist is an individual or small group of individuals who are involved in terroristic activities and attacks but are not tied to a terrorist organization (Spaaij, 2010; Weimann, 2012). Though these types of terrorists may be in agreement with a number of terrorist organization’s views, they do not rely on an affiliation to those organizations in order to validate their missions (Bartol & Bartol, 2011). The term “lone wolf” terrorist was established in Pierce’s 1989 right-wing fantasy novel *Hunter* and later became popularized in the 1990s by white supremacists Tom Metzger and Alex Curtis who promoted leaderless attacks by individuals to support their cause (White, 2003). However, the concept of a leaderless terrorist

engaging in building destruction, assassinations and mass murders in order to inspire others existed long before the phrase lone wolf was coined. In 1877 Russia, Vera Zasulich attempted to assassinate General-Governor Trepov due to his outrage over the political unfairness the Governor demonstrated in St. Petersburg (Moskalenko & McCauley, 2011). George Metesky, also known as the Mad Bomber of New York, sought revenge against big business corporations by setting off 22 pipe bombs from 1940 to 1957 (Bates, 2012). In the past, a majority of the general public may have viewed lone wolf terrorists as nothing more than individuals who are angry at the world and do not pose a real threat to the social structure of society. However, lone wolves have proven to be some of the most innovative and dangerous terrorists throughout history (Post, McGinnis, & Moody; 2014; Spaaij, 2010; Thompson, 2013). Spaaij's (2010) research identified several lone wolf terrorist utilizing elaborate devices which they constructed on their own in order to fulfill their mission. One of the best examples of the destructive ingenuity of a lone wolf terrorist was seen in Theodore Kaczynski's seventeen year campaign of mail bombings. Kaczynski targeted individuals and companies whom he perceived to be promoting the downfall of society due to his view on modern technology and the industrial system as being a curse on humanity. Even though his bombings did not create the social change that he wanted or inflict the damage he so desired, Kaczynski was able to create a state of fear and panic across the country. Lone wolf terrorist attacks, like the ones committed by Kaczynski, are not a new phenomenon. But based on the number of occurrences within the past ten years the imminent threat from these individuals is on the rise. FBI director Robert S. Mueller III identified that there is an increasing threat from a single individual who is sympathetic towards a cause or terrorist group but is acting without any external support or affiliation to an organization (Spaaij, 2010). Even President Barrack Obama acknowledged in 2011 that the biggest concern

to the safety and security of the United States and its citizens is not from an attack launched by a major terrorist campaign, but from a deranged individual filled with hateful ideologies who carries out a wide scale massacre (Madhani, 2011). Both Obama and Mueller's risk assessment proved to be accurate with the most recent bombing at the Boston Marathon committed by the lone wolf terrorists Dzhokhar and Tamerlan Tsarnaev. The Tsarnaev brothers were driven by fulfilling the jihadist belief of terrorist organizations like Al Qaeda and Hezbollah. Since this is a major concern for national security, researchers have focused on trying to be able to identify and locate these terrorists in order to prevent future attacks.

There are certain advantages that lone wolf terrorists have over an extremist group that causes them to be a greater threat to the world. One of the most profound advantages is due to their lack of constraint for violence. Research has shown that lone wolves are innovative and think outside the box without the restraint for violence that some members of terrorist organizations may have (Bakker & de Graaf, 2010; Simon, 2013; Thompson, 2013). "In fact, many join extremist groups only to leave due to conflicting agendas or ideas, which are often too extreme even for the hard-core members of the group" (Bakker & de Graaf, 2010, p. 4). They show no remorse and do not care if they kill innocent civilians in their attacks, identifying everyone as a threat to their beliefs. Spaaij (2010) conducted a comparative analysis on five known lone wolf terrorists which showed that each one was motivated by their own ideological view of the world with an aversion towards a broader political, social or religious aim. Lone wolves consider only the spread of their perceived cause to the masses, which makes them more dangerous and unpredictable when no one is guiding or leading them.

Since lone wolf terrorists predominantly work alone, they are much harder to track or identify than a terrorist organization or cell (Bakker & de Graaf, 2010; 2011; Bates, 2012; Spaaij,

2010; Simon, 2013; Thompson, 2013; Woods & Spaulding, 2005). Bakker and de Graaf's (2010) research found that lone wolves do not require the necessities that extremist groups need in order to plan their attacks. Terrorist organizations require months or years of planning, making sure that every operative understands their responsibility. In doing so, terrorist organizations leave themselves more vulnerable to detection from law enforcement agencies due to the number of variables in play and individuals who could compromise the planned attack. However, lone wolves do not require communication with outside sources for guidance or employ organizations to provide needed funds and equipment. They tend to isolate themselves from the rest of society which makes it even harder to predict what their intentions or what they are planning (Bakker & de Graaf, 2010; Hewitt, 2003). Research has shown that many of these individuals plan every event from start to finish alone and require limited resources for their attacks which mainly consists of firearms or material needed to make home-made explosives which are easily attainable (Barnes, 2012; Bartol & Bartol, 2011; Hewitt, 2003; Spaaij, 2010). Therefore, lone wolves have an easier time staying in the shadows and blending in before they strike.

Psychopathology of Lone Wolves

Lone wolf terrorists generally have a different psychological makeup than those terrorists who belong to extremist groups or organized networks (Bartol & Bartol, 2011; Gruenewalk, Chermak, Freilich, 2013). As mentioned before, they do not rely on an affiliation with a group for the justification of their cause. They normally operate alone or with a few select individuals who also have no affiliation with an organization (McCauley & Moskalenko, 2013; Simon, 2013). Lone wolves develop their own method of operation, targets and decision making. In a Q&A with Thompson (2013), Jeffrey D. Simon, author of "Lone Wolf Terrorism: Understanding

the Growing Threat”, believes that because these terrorists think outside the box and are loners by nature with no one directing them, they pose the greatest threat. “Lone wolves have little or no constraints on their level of violence. They are not concerned with alienating supporters (as would some terrorist groups), nor are they concerned with a potential government crackdown following an attack” (Thompson, 2013, p. 1). Lone wolves have a unique interpretation of the world and only see the spread of the message towards their perceived cause as the ultimate goal and something they wish to bring to the public’s attention (Bartol & Bartol, 2011). They tend to adopt the ideology of an extremist or outside group, whether or not that group engages in terroristic acts (McCauley & Moskalenko, 2013; Simon, 2013). Lone wolf terrorists believe they are acting on behalf of the group or the cause. With that, the most common ideologies followed by the lone wolves in America are white supremacy and anti-abortion (Gruenewalk, Chermak, Freilich, 2013). However, based on recent attacks, the threat of individual jihads is intensifying. Understanding why this form of terrorism has increased in recent years is needed in order to establish preventative measures.

The Rise of Lone Wolf Terrorism

The concept of lone wolf terrorism is not a new phenomenon, nor is it a threat that the American government just realized could happen (Fields & Perez, 2009). However, since the start of the twenty-first century attacks committed by lone wolf terrorists have increased both nationally and internationally. The reason for this increase can be explained in two ways. The first being modern technology, specifically the Internet. An individual does not become a lone wolf terrorist overnight or immediately engage in a terroristic lifestyle. Individuals initially sympathize or feel a connection with an extremist movement and eventually take up the cause as part of their own lifestyle. However, they do not directly engage in the group’s activities or

actions. A majority of lone wolf terrorists are antisocial, demonstrate poor interpersonal and social skills, and adopt an isolationist attitude (Bartol & Bartol, 2011, Nijboer, 2012). They are socially alienated and see themselves as more of an outside medium for the cause (Bartol & Bartol, 2011; Hudson 1999; White, 2003). In the past, potential lone wolves became inspired through readings, movies, speeches, political actions or negatively perceived incidents. Yet, in today's society people no longer have to leave their homes to feel a connection. The use of social media and the Internet allows potential terrorists to become motivated towards specific causes and receive feedback from other likeminded individuals at the brush of a keystroke. The world of cyberspace has led to the proliferation of lone wolf terrorism by allowing anyone to become educated in terroristic tactics, weapons, and high sought after targets through the use of a computer or smartphone (Thompson, 2013). Lone wolf terrorists are able to obtain access to radicalizing material, training manuals, writings from extremist leaders and even videos (Mass, 2013; Weimann, 2012). In addition to viewing online resources from terrorist organizations and developing their extremist views of the world, Dzhokhar and Tamerlan Tsarnaev learned how to construct the bombs they used at the Boston marathon from online manuals provided by Al Qaeda supporters (Cooper, Schmidt, & Schmitt, 2013). Others have been given a motivational push to engage in activities and act upon their internal feelings through online social platforms. Nidal Hasan, who killed 13 people and wounded 43 at the Fort Hood mass shooting in 2009, engaged in email correspondence with individuals who were spreading Al Qaeda ideology (Spaaij, 2010). Lone wolves are no longer isolated in their homes without any means of motivation or enticement, as Internet access offers them a conduit to increase their frustrations and converse with others who have proclaimed similar views. As a result, many terrorist organizations have taken note and found a way to benefit from this new form of communication.

The second reason for the rise in lone wolf terrorism is due to newly developed tactics used by terrorist organizations. Researchers have found that a shift towards a leaderless resistance terroristic strategy occurred in the 1990s due to the United States' crackdown against cellular organizations, as in the case of Ruby Ridge and the Waco siege (Chermak, Freilich, & Simone, 2010; Smith & Damphousse, 2002). The concept of a leaderless resistance departs from previous templates of terroristic warfare and insurgency and has emerged as a new operational tactic exploited by extremist groups to gain an advantage over government agencies (Chermak, Freilich, & Simone, 2010; Michael, 2012). The Animal Liberation Front and the Environmental Liberation Front have claimed to be non-violent, but both have been associated with promoting individual-type terroristic attacks (Bates, 2012; Michael, 2012; Pressman, 2003). Research has also found that other extremist organizations, like anti-abortionist and white supremacist groups, have also exploited individuals and/or promoted lone wolf terrorism. William Pierce, founder of the National Alliance a white separatist political organization, promoted and contributed to the popularity of leaderless resistance through speeches and his published works *The Turner Diaries* and *Hunter* (Michael, 2012; Welner, 2001; White, 2003). Pierce's works became one of the inspirations for both Timothy McVeigh, in the Oklahoma City bombing and David Copeland, who committed a thirteen-day bombing campaign in London in 1999. Originally the spread of this lone wolf mentality was only accomplished through the writings and public speeches by extremist organizations. However, the continuous rise and use of social media has offered them a means of spreading the tactical ideology to a larger audience. Antigovernment, white supremacists, jihadists and other extremist groups began to utilize the Internet to their advantage at the turn of the century. Instead of being directly linked to lone wolves, these terroristic leaders and activist are making use of webpages, web forums, videos and digitally recorded public

speeches to call upon supporters to take it upon themselves and commit terrorist attacks in the name of their perceived beliefs (Bates, 2012; Weimann, 2011; 2012). Bates' (2012) study found that the instantaneous spread of terroristic views through the use of the Internet has resulted in a rapid increase of self-radicalized independent individuals committed to establishing a public spectacle to show their support for the cause. Al Qaeda members have now circulated their teachings through online forums on "How to Fight Alone" and released videos entitled "A Call to Arms" and "Do Not Rely on Others, Take the Task Upon Yourself", all of which ask for individuals to start their own jihad against western government and their supporters (Bakker & de Graaf, 2010; Weimann, 2011; 2012). Terrorist organizations are realizing the potential benefits of promoting lone wolf terrorists to commit acts for their cause. They recognize that lone wolves can present an even bigger danger to their enemies at no cost or direct link to the organization. To this point, the Internet has predominately been used by Islamic terrorist organizations and other extremist groups as a way of spreading their beliefs and perceived transgressions as well as a means of recruiting members to their cause. However, a new threat has emerged as technology and the Internet are not just being used to spread the beliefs of a terrorist or terrorist organization, but as a means of engagement in the names of their cause.

Terrorism in Cyberspace

Modern technology has been a blessing for the masses in today's society. It has made life easier for government entities, law enforcement agencies, businesses, and corporations as well as for almost every individual in American society. Businesses can immediately handle commercial transactions with other companies from around the world, corporations can have video conferences and board meetings without leaving their offices, police officers can query pertinent criminal information right from their patrol car, necessary documents can now be sent

or received at a moment's notice and individual consumers can make purchases right from the comfort of their own home. However, modern technology is a double edged sword and all these digital advancements come at a price. Though the technology of today has made life easier for the general population, it has also made life easier for the terroristic element and created a new domain which they can use to their advantage. Cyber terrorism has emerged as a new means of engagement in the names of the terrorist's beliefs. The introduction of cyber terrorism has become an apparent and imminent threat to national and international security that could potentially be committed by lone wolf terrorists. Traditionally the focus of cyber terrorism has been aimed primarily at disrupting or destroying a crucial infrastructure and important electronic data, as well as a means of facilitating traditional forms of terrorism (Jain, 2005). Tafoya's (2011) research identified cyber terrorism as the use of technology as a means to create political, religious or ideological change through the intimidation of civilian enterprises by disrupting or destroying critical infrastructures in cyberspace. Cyber terrorism does not have to cause death, physical harm or economic devastation to qualify as an act of terrorism, so long as it substantially interferes with some form of infrastructure (Hardy, 2011). Researchers have found that cyber terrorist attacks have the potential to disrupt the financial market, interfere with services, destroy computer files and networks, and cause widespread panic among citizens and businesses (Cassim, 2012; Hardy, 2011; Tafoya, 2011). Previous computer viruses created by hackers, such as the love bug virus created by Reonel Ramones and Onel de Guzman, have the potential to be catastrophic to a country's social and economic system. The love bug virus was designed to infect computers through email accounts and steal the user's internet password (Brenner & Goodman, 2002). The end result caused millions of computers across the world, including the United States, to be infected and resulted in billions of dollars in damages.

Although this virus did not cripple or incapacitate the United States government's infrastructure, the devastation it caused over a decade ago shows the potential that a computer virus is capable of doing. The use of cyber-attacks by terrorist organizations in the past have been largely limited to email bombings of ideological foes, denial of service attacks, and defacing/disrupting websites (Congressional Digest Corp., 2011). In 2012, the Islamist group ad-Din al-Qassam Cyber Fighters was responsible for cyber-attacks which targeted several bank websites including Bank of America and PNC Bank, resulting in their websites being shut down for an extended period of time (Rothman, 2012). In January 2003, the untraceable slammer worm caused 911 emergency systems and ATM machines to shut down, and its code was linked to a hacking group in China. The CIA confirmed that cyber-attacks were the cause of multiple power outages throughout cities in the United States including New Orleans in 2008 (Piggin, 2010). However, Tafoya's (2011) research has found that not only have international terrorist groups like Hamas and Hezbollah undertaken cyber-attacks but "lone wolves" have committed these crimes in recent years. Hackers briefly disrupted a U.S. government website to protest the Chinese embassy bombing (CNN, 1999). While in Australia, Vitek Boden conducted a series of electronic attacks by hacking into the computerized waste management system of his former employer in 2000. Boden caused millions of gallons of raw sewage to spill out into local parks, rivers and hotel grounds, destroying wildlife and disrupting local businesses. In 2010, Google and 20 other companies were hacked by an unidentified hacker with the intention of obtaining high value intellectual property and source code information in order to disrupt their business infrastructure (Kurtz, 2010). Even though a majority of these cyber-attacks were isolated to specific areas of a computer system and created more of an inconvenience the widespread

devastation, the landscape of computer viruses and cyber-attacks forever changed in June of 2010 with the occurrence of the most significant attack in cyberspace to date.

The Devastating Capability of Cyber-Attacks

In 2010, the Stuxnet worm infected the computer systems of Iran's nuclear facilities, shutting down critical system infrastructures which could have potentially caused a nuclear meltdown (Fildes, 2010). The Stuxnet's programming was one of the first of its kind and forever changed the way people would view computer viruses.

James Farwell and Rafal Rohozinski's (2011) research found the following:

Using four 'zero-day vulnerabilities' (vulnerabilities previously unknown, so that there has been no time to develop and distribute patches), the Stuxnet worm employs Siemens' default passwords to access Windows operating systems that run WinCC and PCS 7 programs. These are programmable logic controller (PLC) programs that manage industrial plants. The genius of the worm is that it can strike and reprogram a computer target (p. 22)

This coding allowed the virus to infect certain frequency converters that were responsible for regulating the speed of uranium centrifuges and cause the system to malfunction (Farwell & Rohozinski, 2011; Fildes, 2010; Lindsay, 2013). Although this virus did not result in anyone losing their life, it had the potential to cause a nuclear disaster and kill millions of people in the process.

Hackers and Hacktivism

Hackers are viewed in society as criminals who invade/break into secure computer systems which allows them to manipulate these systems to their advantage; steal money and information from government organizations, alter computer mainframes for vindictive reasons,

and upload malicious software (malware) to disrupt computer systems and cause blackouts. Hollywood and pop culture have made these types of criminals infamous through movies, television programs and video games like the Matrix, 24 and Watch Dogs. However, when hackers were first introduced to the world they were not always seen in such a negative way. “Originally, the word ‘hacker’ referred to an unorthodox problem solver and master programmer; in fact, these original hackers made the machines and the programs that are vital to modern society” (Taylor, et. al, 2011, p. 61). Computer experts like Steve Jobs, Bill Gates and Mark Zuckerberg, who designed and brought to the forefront computer technology and programs that we use on a daily basis, would have considered themselves hackers when they were first beginning their digital empires. Hackers have been hailed as heroes of the computer revolution because of the digital magic they have been able to accomplish (Nikitina, 2012). Hackers first came into existence in the 1960s as a technological counter culture movement who engaged in “phreaking”. Phreaking is a play on the words of phone and freak and involves the study and experimentation of telecommunication systems and telephone networks (Gold, 2014; Hampson, 2012; Penny, 2011; Taylor, 2005). These digital phreakers/hackers did not seek to harm or disrupt computer systems or digital networks. They simply wanted to master the art of computer programming (Taylor et. al, 2011). However, this all changed in the 1980s with the introduction of the personal computer and advancements in modem technology, thus allowing for the development of the criminal hacker to arise in cyberspace.

This new criminal generation of hackers pursues the exploration of the entire cyber-network and the acquisition of digital information by any means necessary. They were not concerned with the ethical dilemma of accessing protected computer systems and whether or not they were breaking the law; they only desired to expand their computer knowledge (Gold, 2014;

Taylor, 2005; Taylor et. al, 2011). “Being referred to as a hack was a clear indication of an individual’s understanding and skill since the development of the computer technology. In fact, the hacker identity is built upon a devotion to learn and understand technology” (Taylor, et. al, 2011, p. 76). This criminal hacker subculture gave way to the creation of hacker groups, like the Legion of Doom (LOD), who prided themselves on being better and smarter than the general public and revolting against law enforcement and government organizations (Taylor, 2005; Taylor et. al, 2011).

Hactivism is an effort to promote political, economic, religious, social, or environmental change in the world through the use of hacking techniques, computers technology and digital networks (Krapp, 2005; Penny, 2011; Taylor, 2005; Taylor, et. al, 2011; Vamosi, 2011). The hactivism movement was coined by the hacker collective known as the Cult of the Dead Cow in the mid-1990s and began as a peaceful campaign, promoting human rights on the Internet and rejecting digital censorship (Krapp, 2005; Vamosi, 2011). The main focus behind the early hactivist movement supported the freedom to share information and computer software in cyberspace. Originally, cyber protests committed by these hackers involved Webpage defacement of targeted organization/government agencies and offering free digital downloads of computer software including music MP3s on established websites (Hampson, 2012; Krapp, 2005; Taylor, 2005; Vamosi, 2011). In 1996, hackers defaced the Department of Justice’s website to protest the passing of the Communications Decency Act (Hampson, 2012). These initial demonstrations could be compared to the equivalent of a sit in or rally by any other activist group, which could lead one to assume that hactivists present no real threat to social order. However, as the Internet has evolved and society has become more dependent on digital technology over the years, the tactics used by hactivist organizations has progressively become

more sophisticated and heinous (Hampson, 2012; Vamosi, 2011). Hacktivist groups have now taken a more aggressive approach in their cyber-attacks in an effort to initiate social change and promote freedom of information. These attacks include Distributed Denial of Service (DDos) attacks, email bombings, diverting Internet traffic to false mirror sites, and writing/uploading computer viruses. In 2010, thousands of hacktivists joined together under the name “Operation Payback” and launched an attack against Visa, Mastercard, and PayPal after they removed their support of journalist organization “WikiLeaks”, who at the time posted secret U.S. government communications. The end result prevented consumers from accessing online banking accounts and knocked their Websites offline for a period of time (Vamosi, 2011). Other hacktivist groups like Level Seven, milw0rm, RedHack, UGNazi and Anonymous have conducted similar attacks, declaring a cyber-war against government establishments and professing world inequalities. Hacktivists networks proficiency with computer and ability to easily navigate through cyberspace is undeniable. However, they are not viewed as a top priority and are only seen as a secondary threat by both law enforcement agencies and government officials. “Most security experts agree that cyberattacks by nation-states, like the Stuxnet attack on an Iranian nuclear facility last year, are a far greater threat to the global security than autonomous hacking collectives knocking out company websites” (Penny, 2011, p. 21).

On the other hand, lone wolves are innovative and think outside the box without restrictions on what they can do (Thompson, 2013). The lone wolf terrorist does not have the constraints that members of terrorist organizations or hacktivist groups do. They are not concerned with alienating their supporters and are only interested in carrying out their beliefs and actions that support the cause (Thompson, 2013). This way of thinking makes a lone wolf terrorist more dangerous in cyberspace. Terrorist organizations and hacktivist groups carefully

plan and take every measure into account when engaging in cyber terrorism; seeing that only certain systems or countries are infected by the cyber-attack, so not to lose their supporters. Unlike these organizations, the lone wolves do not concern themselves with the collateral damage or the risk of upsetting their supporters, just that their message is received. “Based on their unique interpretations of the world, they perceive injustices that they wish to bring to public attention” (Bartol & Bartol, 2011, p. 337). Thus, in the eyes of the lone wolf, the creation of a virus or the hacking of computer programs, no matter who is affected by it, is valuable for their alleged cause.

In conclusion, terrorism has always been and continues to be an area of concern for government officials and law enforcement agencies in order to maintain the public’s welfare and security. However, due to the influx of recent attacks as well as the apparent and imminent threat level they present, lone wolf terrorism has established itself as one of the biggest concerns to national and international safety. Lone wolves have proven that they can create as much devastation and panic as the larger terrorist organizations while having the added ability of remaining out of the watchful eye of government agencies. In addition, government agencies and organizations have identified that the infrastructures of both businesses and countries are potential targets for cyber-attacks due to the United States’ dependency on technology. The potential, as assessed from the outcome of previous international computer viruses, can be catastrophic to a country’s social and economic system. The lone wolf cyber terrorist is an even greater threat when committing these acts because they do not take into account or care about the collateral damage to other supporters of their cause in addition to their intended targets. Based on his research, Jeffery D. Simon believes that these attacks are tailored for the lone wolf terrorist because they have no need to leave their home to create the program and launch the

computer driven attack (Simon, 2013; Thompson, 2013). Lone-wolf hackers have disrupted computer systems in the past and continue to show a presence in cyberspace. It is possible, in the not so distant future, for an individual to become motivated enough over a perceived strife to succeed in the first major cyber-attack on a country's infrastructure. Unfortunately, there is very limited research on lone wolves' involvement in cyber terroristic activity. There is a clear understanding among current and past research on the concept of lone wolf terrorism and the danger it presents to the world. However, no research has made a connection to the possibility of lone wolf terrorists engaging in cyber terrorism or utilizing a combination of a physical and digital attack in future acts of terrorism. As a result there is a gap in information that ought to be explored regarding lone wolf terrorism. The development of cyber terrorism along with the increase in lone wolf terrorist attacks is a cause for major concern to the already existing threat of terrorism and an area that needs to be analyzed and addressed in order to gain a better understanding of the issue at hand.

Chapter Summary

The current literature pertaining to the dilemmas of lone wolf terrorism and cyber terrorism have provided a general understanding on the subject matter. The articles provided valuable insight in regards to what past researchers consider to be an act of lone wolf terrorism and cyber terrorism and a general idea of the individuals who engage in this type of activity. The research articles were also able to provide information on certain incidents that they consider addressing this up and coming phenomenon. The material that is presented in the literature review will be a building block for the research study about how has lone wolf terrorism and cyber terrorism started to flourish and why these forms of terrorism have the potential to present the greatest threat to the safety and security of the United States and the world.

Chapter 3

Research Procedures

My research question was designed to determine: Is there an imminent threat that the next major terrorist attack will come from a lone wolf cyber terrorist? I assessed the threat that a lone wolf cyber terrorist presents to the world and identify the probability that a future attack will be in the form of a cyber-attack or a combination of an attack in the physical and digital world.

Research Methodology

The qualitative methodology that I utilized to conduct the research was based on a qualitative case study on four lone wolf terrorists. This type of study was used to describe, understand and examine the phenomenon of lone wolf terrorism and how they would have used cyber terrorism as a tactic if available to them. The disadvantages to using the type of data collection was that because the focus will be on specific lone wolf terrorists it will not necessarily be comprehensive to all lone wolves. In order to manage this, the four chosen lone wolves spanned from the early 1990's to today, so as to not focus on just one period of time. In addition, the chosen lone wolves did not focus on one belief, but encompass different ideologies.

In addition to the study of the four lone wolf terrorists, I conducted a case study on a hacktivist organization/network. The case study provided better insight and examined the hacktivist culture and their connection with cyber terrorist activity. Though the computer capabilities of hacktivist networks are undeniable, they are viewed by many law enforcement agencies and government officials as a second rate threat to the world. "Most security experts agree that cyberattacks by nation-states, like the Stuxnet attack on an Iranian nuclear facility last year, are a far greater threat to the global security than autonomous hacking collectives knocking out company websites" (Penny, 2011, p. 21). Their security assessment appears to be accurate

due to the fact that no cyber-attack by a hacktivist has caused permanent damage or a loss to human life. But, what would happen if the collective becomes motivated enough to commit an attack similar to the Stuxnet worm? What happens if they see no other way to get their point across and instill change than to create a realistic threat to the public? Several other extremist organizations started out as a collective group of individuals protesting what they viewed as a valid cause. The Animal Liberation Front wants to change U.S. policy on animal testing, the Earth Liberation Front is against the destruction of the environment, and the Army of God is a Christian organization against abortion. Each group is seeking to change a perceived injustice through public protests and activist pursuits. Nevertheless, these as well as other organizations have become more violent over the years, participating in bombings, kidnappings and assaults, and destroying buildings and pieces of equipment. These same groups are now labeled as domestic terrorist organizations. It would stand to reason that a similar course of action could take place among the hacktivist collective.

The case study on the selected hacktivist network was also be utilized to supplement the data collected on the four lone wolf terrorists and the possibility that a lone wolf would utilize cyber-attacks as a part of their strategy. It would also stand to reason that a lone wolf individual or hacker could idealize one of these hacktivist networks and support their cause. That same individual could then take it upon themselves to commit terrorist attacks in the name of the hacktivist cause which could include attacks in cyberspace. However, the disadvantage to conducting a case study on a specific hacktivist network is that the case study could be focused on a network that may never actually engage in violent terroristic activity. In order to manage this, the chosen hacktivist network will be focused on one that has shown to continually profess their grievances, made threats and engaged in protests, both online and in the real world.

Sample

For my research, the chosen lone wolves for the case studies were selected on the basis of their variation in terms of the length of time their reign of terror took place, the cause they believed in, and the number of people hurt and/or killed. This was similar to how Ramon Spaaij (2010) conducted his research case studies on lone wolf terrorists. Furthermore, I utilized the definition of lone wolf terrorism which includes an individual or small group of individuals who are involved in terroristic activities and attacks but are not tied to a terrorist organization. This broadened the pool of lone wolf terrorists and attacks that would be look at for this research project. However, in order to incorporate the likelihood that a lone wolf will utilize cyber terrorism as a tactic, the case studies focused on lone wolves who used more elaborate plans as well as tactics/devices rather than just simply the use of a gun or a non-mechanical weapon (i.e. knife, axe, hammer, etc.) to commit murder/mass murder in the name of a cause. The chosen case studies were used to describe, understand and examine the phenomenon of lone wolf terrorism and how they would have used cyber terrorism as a tactic if it was available to them. The disadvantages to using this type of data collection is that because the focus would be on specific lone wolf terrorists it would not necessarily be comprehensive to all lone wolves. In order to manage this, the four chosen lone wolves spanned from the early 1990s to today, so as to focus on more than one period of time. In addition, the chosen lone wolves did not just focus on one belief, but encompassed different ideologies.

Name	Ideology	Time Span	Type of Attack	Death/Injuries
Timothy McVeigh	Right-Wing	Single Attack 1995	Fertilizer Bomb	168/680
Eric Rudolph	Anti-Abortion/ Anti-Gay	1996-1998	Pipe Bombs	4/150
Anders Breivik	Right-Wing	Two Attacks in One Day 2011	Fertilizer Bomb/ Shooting (Assault Rifle & Handgun)	Bomb- 8/209 Shooting- 69/110
Tamerlan & Dzhokhar Tsarnaev	Islamic Extremist	Single Attack 2013	Pressure Cooker Bomb	3/264

In addition, the chosen hacktivist network for my case study was selected based on their level of activity with protesting their grievances and tribulations in the real world and on the Internet and their involvement in cyber-attacks. As with the lone wolf terrorists, the case study on the selected hacktivist network may not be comprehensive to the entire hacktivist movement. However, in order to manage this, the chosen hacktivist network was one that has been continuously active since their formation, has influenced other hackers and hacktivists and was linked to a number of cybercriminal activities. The chosen case study was used to describe, understand and examine the hacktivist movement and the possibility that a lone wolf could emerge in support of the network's ideology.

Instrumentation

The research method that was used throughout the study was an in-depth description of each case study. The study will utilize historical data as a means of assessing the probability of future attacks being committed by lone wolf terrorists utilizing cyber terrorism. The finding from the analysis will be compared with previous research to determine if the case studies supported previously researched trends on lone wolf terrorists. Theories pertaining to criminal behavior will then be applied to the lone wolf terrorist case studies to further identify what influences them to follow a life of terrorism and how they determine what type of attacks or

tactics will be used for their terror campaign. By focusing on each individual's ideals, causes, common targets and members, the psychopathology of each lone wolf will start to develop. Theories were be applied and an analysis of potential targets, general strategies, means of funding and likelihood to utilize newly developed tactics can be created.

Data Collection

The focus of the research was on a literal text analysis in order to have the study based more on facts instead of opinion. This will also limit the amount of bias that could be displayed in the research. The cases of lone wolf terrorism and the hacktivist network will be examined through a content analysis of secondary source documents. The documents utilized were from peer reviewed journal articles, published books and magazine/newspaper articles pertaining to each individual and their attacks.

Data Analysis

Each lone wolf terrorist was analyzed and assessed based on how they were influenced towards engaging in terroristic activity, how and why they were motivated to commit the attacks that they did, their psychopathology and social personality, how they were influenced to plan and utilize the attacks they committed, and the actual attacks they were involved with. Each lone wolf and the terroristic attack they committed was compared and contrasted with the other individuals and their attacks. Similarities and differences were recorded in order to gain a better assessment towards the research question.

In addition, the case study on a specific hacktivist network was analyzed and assessed based on their level of activity and involvement in protests both in cyberspace and in the real world. The hacktivist network was compared and contrasted with other hacktivist groups and other extremist organizations. Similarities and differences were recorded in order to gain a better

assessment towards the research question and the likelihood that a lone wolf may emerge in the name of the hacktivist network's ideology.

This research utilized content analysis for the attack(s) that each lone wolf terrorist was involved in. Instead of simply obtaining a basic understanding of each terrorist and a description of what occurred, the analysis went more in-depth and looked closely at certain details such as their full biographical history and an extensive analysis of how they were influenced and learned to commit the attacks that they did. Content analysis allowed a better understanding of the lone wolf terrorist's social behavior and the likelihood that they would engage in cyber terrorism to attack people and critical infrastructures.

Chapter Summary

The course of action with conducting a case study on several individuals/groups will be a long investigatory process and required several reviews and alterations before its distribution will be considered. The case studies provided the opportunity to analyze the background information, progression and interaction of each individual/group in order to determine the underlying principles from a holistic perspective. Though this study was only focused on selected lone wolves and a hacktivist network, it will still provide significant material pertaining to the research problem. In order to gain a better understanding on the two forms of terrorism, historical content data collected will be evaluated and analyzed.

Chapter 4

Case Studies and Analysis

Timothy McVeigh

One of the deadliest terrorist attacks, prior to 9/11, to occur in the United States happened on April 19, 1995 in Oklahoma City. On that day, a rental truck containing 13 barrels of explosives was parked and detonated in front of the Alfred P. Murrah Federal Building, which was a regional office for several law enforcement agencies including the United States Secret Service (USSS), the Drug Enforcement Agency (DEA) and the Bureau of Alcohol, Tobacco, and Firearms (ATF) (BBC, 2001; CNN, n.d.; Michel & Herbeck, 2001; Zeff, 1997). The end result of this attack killed 168 people (including 19 children) and injured over 680 people. The attack is still known as the most devastating form of domestic terrorism in the United States. It was initially believed that the attack was committed by Middle Eastern terrorists, but was later identified as being committed by a lone individual who desired vengeance against a perceived oppression of civil liberties by the American government. This lone wolf terrorist was identified as Timothy McVeigh.

Timothy McVeigh grew up in a typical middle class family in rural New York state. His parents divorced when he was ten and he was raised by his father in Pendleton, New York (Michel & Herbeck, 2001; Zeff, 1997). Though viewed by many during his childhood and adolescence as an affable and knowledgeable individual, McVeigh was somewhat of a loner and was the victim of bullying by his peers. He would go on to graduate from Starpoint Central High School and was awarded a scholarship and attended Bryant & Stratton College but eventually dropped out (Michel & Herbeck, 2001; Zeff, 1997). McVeigh would move on to several odd jobs and also made money buying and selling firearms at gun shows. It was also during this time

that he would obtain a copy of the “Turner Diaries” written by William Pierce which depicted the story of a lone individual bombing a federal building in response to the government’s restrictions against private firearms (White, 2003; Zeff, 1997). Pierce was the founder of the National Alliance, a white separatist political organization, and also promoted and contributed to the popularity of leaderless resistance through speeches and his published works (Michael, 2012; Welner, 2001; White, 2003). McVeigh became inspired by this book and would use the knowledge he obtained from it in his attack. Prior to this though, McVeigh joined the U.S. Army in 1988 and became an exceptional soldier according to his peers. McVeigh made the rank of sergeant and was even awarded the Bronze Star during his service in the first Gulf War.

However, after leaving the army he became a wanderer, moving from state to state, peddling guns to make money and spending time with old army buddies. It was during this time that McVeigh and his war buddies started to build up hatred towards the U.S. government, believing that the government was trying to take away their rights as citizens and their freedom to own and purchase firearms (Michel & Herbeck, 2001; White, 2003; Zeff, 1997). This was further surmounted by the Ruby Ridge incident of 1992, which McVeigh viewed as the government trying to hamper the Weaver’s family right to purchase and sell weapons. The following year McVeigh traveled to Waco, Texas to protest against federal law enforcement agencies as they sieged the compound of the Branch Davidians (Michel & Herbeck, 2001; Zeff, 1997). Though McVeigh did not directly follow the Branch Davidians he believed that they had a right to own the firearms that the ATF was trying to remove. The end result of the Waco siege, which involved the death of 76 Branch Davidians, was the last straw in McVeigh’s mind and a turning point in his life (White, 2003; Zeff, 1997). McVeigh started plotting to bomb a federal facility.

Eric Rudolph

From the summer of 1996 to the beginning 1998 the United States experienced four bombings that were caused by a lone wolf terrorist. The first of these bombings was the most publicized due to the fact that it occurred at the Summer Olympics in Atlanta, Georgia. On July 27, 1996 a military book bag containing several pipe bombs and nails was placed in a central area at the Centennial Olympic Park and set on a timer to explode (Gettleman & Halbfinger, 2003; Monsky, 2000; Wyatt, 2005). The explosion resulted in the death of two people (one from a heart attack) and wounded 111. However, the explosion could have been more deadly had it not been for the security guard Richard Jewell who evacuated the area after discovering the bomb during his patrol. Unfortunately, this was only the beginning of the bomber's campaign as he would set off three more bombs in various location; on January 16, 1997 at an abortion clinic in Sandy Springs, GA; on February 21, 1997, at the "Otherside Lounge" (a known lesbian bar) in Atlanta, GA; and on January 29, 1998, at an Abortion Clinic in Birmingham, AL (Gettleman & Halbfinger, 2003; Monsky, 2000; Vollers, 2007; Wyatt, 2005). Though not as devastating, the bombings were still a major concern for public safety and resulted in the injury of 39 people and the death of two individuals including a Birmingham police officer. After his last attack, information was gathered from witnesses identifying a man in a wig walking away from the scene of the bombing and getting into a pickup truck. Law enforcement official were able to identify who the bomber was, resulting in a massive manhunt. Even with his identity known, the lone bomber avoided capture for five years before finally being apprehended in 2003 (Gettleman & Halbfinger, 2003). The lone wolf terrorist responsible for the bombings was identified as the Christian extremist, Eric Robert Rudolph.

Eric Rudolph was born into a loving middle class family in Florida who viewed themselves as Catholic social activists (Monsky, 2000). Eric's parents were once considered left-wing extremists by the U.S. Government earlier in their lives which partially influenced the lives of their children. From a very young age religion became an important part in Rudolph's daily life as his mother wanted them to grow up in the Christian faith. Rudolph was your typical kid; energetic, curious and bright. He loved to go to the ocean and spent most of his childhood near Miami beach. According to school staff, Rudolph was very smart and showed a lot of potential in school. However, when Eric was 15 his father passed away from cancer (Monsky, 2000). Due to this tragedy and no longer being able to afford the urban lifestyle, his mother, Patricia Rudolph, pulled them out of school and moved the six children to the Nantahala Mountains in North Carolina. There they lived the typical self-sufficient backwoods type of lifestyle, living off the land, growing their own food and keeping to themselves. Eric and his siblings would go on to be home school by their mother. Without a father around, Eric became attached to his neighbor, Thomas Wayne Branham, who they first met in Florida but moved up to North Carolina a short time after the Rudolphs (Monsky, 2000). Branham was a self-proclaimed "freeman", who could also be identified as a sovereign citizen, believing he did not have to abide by the rules and regulations of the federal government which he did not support (CNN,2003; Monsky, 2000; Vollers, 2007). Aside from the exchanging of discrepancies with the government, Eric shared an enthusiasm for firearms and learned survivalist techniques from Branham. It was also during this time as a teenager that Eric began to develop his radical views of the world.

Patricia wanted to ensure that her children received the proper Christian education and felt he needed more stimulation then what he got at home. At Branham's suggestion, Patricia,

with Eric and his younger brother Jamie, traveled to Schell City, Missouri and brought her sons to a Christian Identity Church known as the “Church of Isreal” (Monsky, 2000; Vollers, 2007). Christian identity promotes a racial view of Christianity, believing that white Anglo-Saxons are the true Israelites. The pastor of the Church of Israel “believed interracial marriage destroys the genetic pool of brains and talents forever and that gay people who refuse to repent and go straight should be put to death. Eric and his family moved back to North Carolina after a few months.

Eric Rudolph would earn his GED at home and enrolled at Western Carolina University but dropped out after a few semesters to enlist in the army (Monsky, 2000; Vollers, 2007). Rudolph joined the 101st Airborne Division where he learned to handle explosives along with other military and survivalist training. However, he would eventually be discharged from the army for smoking marijuana. After the army, Rudolph reverted back to his self-sufficient lifestyle and traveled the country doing carpentry work and other odd jobs as a way to support himself (Vollers, 2007). It was also during this time that law enforcement believed he started acquiring the supplies, such as smokeless gun powder, that he would use to construct the pipe bombs. Prior to the bombings, Eric sold the family home in 1992 (his mother, brothers and sister were no longer living in it at the time) and spent the summer in a rental home with his mother in Murphy, NC (CNN, 2003; Monsky, 2000). It was at this same time that Eric Rudolph began to construct the pipe bombs that he would use at the Olympics in Atlanta, GA. Eric believed that the American government needed to pay for allowing the perceived despicable act of abortion and saw the bombings at the Olympics as a way to embarrass the United States on the world stage.

Anders Breivik

In July 22, 2011, the country of Norway was faced with one of the deadliest attacks in their country's history which came in the form of two separate incidents committed by a lone wolf terrorist. The first of these attacks was the detonation of a car bomb that was parked in front of the Regjeringskvartalet, an assortment of buildings making up the Government quarter, in Oslo (Appleton, 2014; Keane & Loock, 2011; Messenger, 2011; Pidd, 2012). The bomb was a 950kg mixture of ammonium nitrate fertilizer and diesel fuel, similar to the concoction made by Timothy McVeigh but a lesser quantity (Pidd, 2012). The end result of this explosion killed 8 people and injured 209 individuals in addition to destroying several of the surrounding buildings, including the Prime Minister's office (Appleton, 2014). However, this was not the only attack the lone individual would succeed. Approximately two hours later an attack occurred on the island of Utoya at a summer camp organized by the Workers' Youth League (AUF). A lone gunman gained access to the island by disguising himself in a police uniform and possessing false credentials. Once the lone wolf gained access to the island he opened fire on those partaking in the festivities. The massacre resulted in the death of 69 people (including friends of the Prime Minister) and injuries to 110. The lone wolf who committed these attacks was identified as the right wing extremist Anders Behring Breivik.

Anders Breivik was born in Oslo, Norway on February 13, 1979 into a liberal middle class family and the son of a nurse and Norwegian diplomat. When he was one year old his parents divorced and he was raised by his mother but frequently visited his father. However, by age four Breivik began to display aggressive and violent behavior. His mother was having difficulty disciplining and controlling Breivik which resulted in him being sent to Norway's National Center for Child and Adolescent Psychiatry (Appleton, 2014; Keane & Loock, 2011;

Messenger, 2011). Breivik was diagnosed with having an emotional detachment to life which could have been contributed by his harsh upbringing. "By the time he was four years old, she "sexualised" the young Breivik, hit him, and frequently told him that she wished that he were dead" (Orange, 2013, p. 1). There was a give and take between mother and son, as Breivik's mother would display hatred towards her son while he would be condescending and hostile towards her. As Breivik grew older he would constantly reject his parents' view of the world and became a rebellious individual, eventually cutting all ties from his father.

Despite his issues from childhood, Breivik was very well educated and in school he was described by former classmates as a very intelligent individual. Breivik was also viewed by many former colleagues as an exceptional co-worker and very persistent in his work. However, under this façade was a darker entity which he was able to keep hidden until his attacks. Though Breivik was not considered a loner as a child/young adult, he was more concerned about his own wellbeing and appearance to the point that he would use anabolic steroids and have plastic surgery done to appear tough and strong (Appleton, 2014; Keane & Looock, 2011; Messenger, 2011). Breivik was later diagnosed during court ordered psychiatric tests as having a narcissistic personality disorder as well as Asperger's Syndrome. This was evident in the fact that he interviewed himself in his manifesto, portrayed no emotion when talking about the victims of the attacks and believed that he was the savior of Christianity. Breivik's psychological state of mind and the resentment he had towards his family and their view of the world caused him to develop an extreme right wing view. He originally was influenced and adopted the views of the right-wing Progress Party (FrP) which he was a former member of. However, due to his narcissism he believed that the party was not doing enough to change Norway and Europe for the better and thought he could do more for the cause. Breivik viewed himself as a protector of Norway's and

Europe's ideals and needed to fight against multiculturalism. What pushed Breivik to the breaking point was Norway's involvement in the NATO bombing of Serbia in 1999 in addition to Europe awarding the Nobel Peace prize to the Islamic Terrorist Yasser Arafat (Friedlander, 2011). He viewed the bombings as Europe attacking its own people and the awarding of Arafat as Europe's acceptance of Muslim integration and Breivik could no longer stand on the sideline.

Breivik stated in interviews after the mass murder that he began planning his attacks in 2002, even going on to write a manifesto stating his plans and reasoning prior to the attacks. He would acquire funding for his attacks by taking on various business ventures which included establishing a computer programming business and later a farming company. In 2005, he joined a firearms club in order to make it easier for him to purchase the weapons for the attack (BBC, 2012). He also dedicated his time to acquiring firearms and supplies for his attack, playing video games like Call of Duty to develop target acquisition, and experimenting with explosives. Breivik was able to obtain methods and instruction to construct a bomb through websites and postings online. While he was operating his farming company he set up other front companies in order to purchase the fertilizer that would be used to construct the bomb (BBC, 2012). In the summer of 2011, he moved to the farm where he ran his company to conduct the final preparations before he executed his plans (Keane & Looock, 2011; Messenger, 2011).

In Breivik's manifesto he wrote that his motivation behind the attacks was to prevent the occupation of Muslims in Norway and Europe (Leonard, Annas, Knoll, & Torrissen, 2014). He believed that left-wing politicians and the Norwegian Labour Party were conspiring to allow Muslims and other foreigners to take over Norway. Breivik believed that these individuals must be punished for promoting multiculturalism. His manifesto also laid out a clear operational plan for his terroristic attacks, anticipating that it would take several years before it could be executed.

Breivik's manifesto also identified the reason for the two attack location. The first attack was on the leaders of today with the bomb and the second on the future leaders of tomorrow with the shooting. Breivik believed that by doing this, the government would put a stop to multiculturalism and preserve Norway's traditions.

Tsarnaev Brothers

One of the most recent and devastating acts of lone wolf terrorism occurred on April 15, 2013, when the United States was held in a state of panic due to a terroristic attack that took place in the city of Boston, Massachusetts. Two homemade pressure cooker bombs planted near the finish line of the annual Boston Marathon. This attack resulted in the death of three individuals and injuries to 264 people. An immediate manhunt for the perpetrators of this attack was conducted, involving local, state, and federal law enforcement agencies. Immediately following the attack, law enforcement agencies, government officials and the general public all questioned who would commit such an attack and suspected that these attacks were committed by an Islamic terrorist organization. This came about because the attacks were similar to ones that occur frequently in the Middle East. However, a review of surveillance footage around the area of the incident would reveal two young male suspects as the ones who planted the homemade devices. On April 18, 2013, photos of the suspects were then released to the public in an effort to identify and apprehend the two individuals. A few hours after the photos were released a shooting occurred on the Massachusetts Institute of Technology (MIT) campus, leaving MIT police officer Sean A. Collier dead from multiple gunshot wounds. This shooting was committed by the same perpetrators of the bombing. The two individuals then carjacked an SUV and held the owner hostage until he was able to escape. Police bulletin was then sent out notifying law enforcement that the SUV was stolen by the Boston Marathon bombing suspects. Watertown police officers eventually made contact with the suspects and a gun fight ensued, resulting in the death of one of the suspects (BBC, 2013). The other perpetrator escaped in the SUV before abandoning it and fleeing on foot. The second bomber was eventually discovered hiding in a boat in a residence's backyard and after several hours of negotiation, the individual

was taken into custody. The perpetrators of the Boston Marathon bombing and murderers of Officer Collier were identified as Dzhokhar and Tamerlan Tsarnaev. After the arrest of Dzhokhar Tsarnaev, questions came about as to why these two brothers committed such a heinous attack and whether or not they were associated with Al Qaeda or another extremist group.

Dzhokhar and Tamerlan Tsarnaev were Chechen brothers who immigrated to America with their families seeking a better life. Tamerlan, who was the eldest child at age 26, and his brother Dzhokhar, at age 19 during the time of the attack, were born in the war torn area by the Caspian Sea which was constantly in conflict with the Soviet Union and after its fall, Russia (Reitman, 2013). They grew up in poverty and constantly saw violence on the streets. This type of living caused their family to flee to the United States, originally on tourist visas and later applying for political asylum, in hopes of a better life. Anzor and Zubeidat Tsarnaev (the father and mother of the brothers), along with Dzhokhar initially arrived in 2002 while Tamerlan and their two sisters (Ailina and Bella) arrived in 2003 and settled in the Boston area (BBC, 2013; Reitman, 2013). Though both brothers were from Dagestan, a Republic of Russia, Dzhokhar lived a majority of his life in the United States and thus was more Americanized than Tamerlan; even speaking fluent English within a few years with only a faint Chechen accent (Reitman, 2013).

From an outside appearance both brothers seemed to enjoy living in America and its culture. Tamerlan was an avid boxer in the Boston area winning multiple gold gloves in his weight class. He attended Cambridge Rindge and Latin School, a high school with such notable alumni as Matt Damon and Ben Affleck, and later attended Bunker Hill Community College before dropping out to focus on a career in boxing (Reitman, 2013). Tamerlan even had

aspirations of representing the United States in the Olympics for boxing and later become a professional fighter. However, this dream was cut short when he was disqualified from a nationwide boxing competition due to the fact that he was not an American citizen which prevented him from ever qualifying for the U.S. Olympic team (Reitman, 2013). This could be identified as a turning point in his life as a shift in Tamerlan's ethics and demeanor occurred. Tamerlan seemed to lose his sense of purpose in life as his dreams of becoming a professional boxer were quashed and not having completed his college education. Conversely, it was at this same time that Tamerlan began to discover his Islamic religion. Though he and his family were Muslim, they did not regularly practice their Islamic faith when they initially arrived in America. However, due to his recent demeanor, his mother believed that practicing Islam would calm Tamerlan's demons (Reitman, 2013). Tamerlan and his mother began to read regularly from the Koran and this provided a new sense of vigor to his life. The once avid partier and club goer now rejected any use of drugs or alcohol, stopped listening to music and even quit boxing as they were not permitted in the life of a practicing Muslim. Tamerlan would also spend hours on the computer reading Islamic websites and U.S. conspiracy sites, in particular with regards to the attacks on 9/11. This eventually led him to read online articles and books on Chechnya separatist movement and the struggles they faced against Russia. Tamerlan even desired to join the cause as it was part of his heritage and traveled back to his native Dagestan, seeking to take up the Chechen jihadist cause. He was eventually deterred and traveled back to America.

Dzhokhar on the other hand was more Americanized than Tamerlan. But, like his brother, attended Cambridge Rindge and Latin School where he became captain of the wrestling team and even adopted the nickname Jahar with friends, an Americanized version of his name. Dzhokhar was viewed by many of his peers as an easy going and relaxed individual who always

was willing to help a friend. He was an exceptional student and even earned a city scholarship which he used to go to UMass Dartmouth. However, during the same time that there was a shift in Tamerlan's outlook on life, Dzhokhar's view of the world began to change as well. In the Tsnarnaev house, and the Chechen culture, the eldest son is often viewed as one of the heads of the household (Reitman, 2013; Wines & Lovett, 2013). In a sense, what he says goes. Dzhokhar idolized his brother throughout his life, even learning to box because his brother did. It was also during the time that their parents had gotten a divorce and moved back to Dagestan, leaving Tamerlan to be the head of the family in America. Due to these factors, it is no surprise that Dzhokhar would adopt the same views as Tamerlan. Initially, the Islamic faith was forced upon him by his brother who made Dzhokhar engage in daily prayer, read from the Koran and the book *Islam 101*, and spend more time practicing their faith (Reitman, 2013). Eventually, Dzhokhar agreed with Tamerlan's view of the world and even expressed to his friends that he felt 9/11 and terrorism in general is justified. He told his friends that he did not agree with the killing of innocent civilians but accepts it due to the number of innocent civilians the United States has killed in the Middle East. Dzhokhar's posts and writings on social media sites shifted from sports and the latest trends to Islamic faith quotes, conspiracies about 9/11, and other anti-American culture quotes (Perlmutter, 2013; Reitman, 2013). Dzhokhar also surfed the Internet to view Islamic and Al Qaeda websites.

The brothers started to see the Chechen jihadist struggles as a cause that they needed to take up, but Tamerlan was talked out of it during his travels to Dagestan by relatives and Dzhokhar was unable to travel due to passport issues (Reitman, 2013). Instead of joining the resistance against Russia they shifted their target towards the United States. Investigations by law enforcement revealed that in the days and weeks before the Boston Marathon Bombings, the

brothers visited a gun range to practice shootings, purchased electronic components and a large quantity of firework mortars. It was also discovered that Dzhokhar conducted extensive research online regarding Islamic militant tracts and finding inspiration on how to make homemade bombs from the Al Qaeda magazine Inspire (Reitman, 2013). All this planning would lead to the devastation that occurred on April 15, 2014.

Analysis of the Lone Wolves

Analysis of the Four Lone Wolf Terrorist Case Studies

The four cases of lone wolf terrorism have shown similar consistencies with one another and past research on lone wolf terrorism.

Psychopathology

Acts of terrorism have changed over the years, becoming more heinous and involving innocent civilians, but the ideals behind them have not. The average criminal is impulsive, disorganized and opportunistic. They see crime as a way of acquiring money, goods, or desired stimulation. Terrorists, on the other hand, are well-organized and emotionally stable. Terrorists want to instill fear in order to change an outcome socially or politically. They are highly motivated and use symbolic attacks to make a statement. Though it is difficult to develop a profile of a terrorist, the one unanimous characteristic is the strong belief in a cause and the will to fight for it. Gibbs' (2010) utilization of the left realist perspective can aid law enforcement and the general public's understanding of a lone wolf terrorist's motivational drive.

The left realist theory believes that the root cause of crime is due to deprivation experienced by an individual or group. The theory focuses on the victim and the offender as well as actions and reactions in reference to the crime (Gibbs, 2010). Gibbs applies this theory to terrorism by focusing on the recruitment and subculture of the organization. Terrorists are not isolated to one set demographic; many different individuals become a part of terrorist organizations (Bartol & Bartol, 2011). Gibbs states that individuals who join terrorist organizations are deprived of a certain need. The same can be said for lone wolf individuals who have no direct connection to an organization or cause, but seek a sense of belonging or an agenda to strive towards. Terrorists do not just come from impoverished and repressed areas suffering

from economic hardship (Gibbs, 2010). Not all terrorists are poor and uneducated individuals. Many come from prominent families and are well educated whether through school, military service or both (Bartol & Bartol, 2011; Gibbs, 2010). These individuals are deprived of another need. They lack a sense of self and are socially alienated. (Gibbs, 2010; Hudson, 1999; Bartol & Bartol, 2011). These individuals want to gain a sense of purpose and social acceptance. Many Irish and European terrorists have admitted that they primarily became involved in political violence to seek a sense of self-worth (Bartol & Bartol, 2011). “Left realist theory argues that men who experience stress as a result of relative deprivation and do not have socially appropriate coping mechanisms turn to similarly situated peers, who provide support” (Gibbs, 2010, p. 177). Gibbs explains that terrorist organizations exploit the individual’s deprivation and lack of belonging to their advantage. In an effort to recruit new members, terrorist organizations provide a social setting to gradually integrate people into their organization. For example, Hamas has invested in social programs and online forums in order to build recruitment pools (Gibbs, 2010). Over time these individuals become sympathizers to the cause and start to show passive support by attending rallies, preparing items for upcoming protests or going to the same place of worship as the group. Potential terrorists begin to feel a sense of acceptance and want to gain more acknowledgement from the group. “It is a well-documented finding that terrorist groups provide an important source of identity and purpose for their members, and that this may well be part of what motivates people to join them” (Cottee & Hayward, 2011, p. 973). The recruited members receive positive reinforcement by directly or indirectly associating with the cause and gradually accept the ideals of the organization or an altered perspective of them in the case of lone wolves. In the case of Timothy McVeigh, he was considered very bright but a loner who dealt with being bullied and ridiculed. In a sense, McVeigh was deprived of a social atmosphere with other

individuals his age growing up. However, once he joined the army it seemed that he regained a bit of acceptance, even having army buddies who he stayed in touch with up until the attack. But once he left the army, he began to lose his sense of purpose again becoming a wanderer for a while. This void was fulfilled by the right-wing extremist view of the world. McVeigh became influenced by the writing of William Pierce and other right-wing individuals. He felt an acceptance with this movement, believing in their ideals. Their indirect influence would create a hatred for the rules and regulations of the U.S. Government, specifically the ones aimed towards gun control and firearms restrictions, which was one way McVeigh made money. McVeigh eventually became a sympathizer with other individuals like the Branch Davidians and felt that the Federal Agencies needed to pay for the atrocities they committed.

Eric Rudolph came from a similar background as McVeigh but was initially influenced towards the left-wing movement as his parents considered themselves pacifists and social activists. But unlike McVeigh, Rudolph was not a loner growing up and had a typical childhood. However, Rudolph did become deprived of his father's influence with his passing. In addition to Rudolph being deprived of his father, his family could no longer afford their standard of living and had to live a more secluded and self-reliant lifestyle in the mountains of North Carolina. As a result, Rudolph was first influenced by Branham, a sovereign citizen who rejected the laws of the U.S. government. Eric Rudolph denies that the "Church of Israel" had any influence on the attacks he committed but it is clear that they had an indirect influence on his motives. The Christian Identity church rejected both the normalization of homosexuality and abortion, both of which were the motivation for Rudolph's attacks. Rudolph was also influenced by the anti-abortion terrorist organization 'Army of God'. Though he had no direct ties to the organization,

Rudolph read many books and documents by them and the organization has been a proud and open supporter of Eric Rudolph, even posting his memoirs on their website.

Anders Breivik was deprived of a constant father figure in his life from a very young age due to the divorce of his parents when he was one year old. He also lacked an appropriate mother figure who resented having Breveik due to his uncontrollable attitude as a child. However, unlike the other mentioned lone wolf terrorists it did not seem that Breivik was initially drawn towards the right-wing movement in order to seek a sense of belonging. Rather, it was out of resentment for his parents and their liberal rationality. Breivik's narcissistic way of living would lead people to believe that he would be fine on his own without a care for anyone or any cause. Still, as Breivik joined the FrP, the ideology of the group became instilled into his lifestyle. Based on Gibbs' proposal of the left realist perspective, this is accomplished through the individual receiving peer support either directly or indirectly.

Gibbs' (2010) research states the following:

Members seek peer-support with like-minded people, forming subcultures supportive of these values or ideology Terror groups, then provide peer support that reinforces the ideology to which the member adheres, pressuring the member to conform to group norms and legitimizing violence. (p. 177-178)

Even though Breivik became fully enthralled in the FrP views on immigration and multiculturalism, his narcissism would get in the way. He believed that the party was not doing enough for the cause and asserted that he could do more for the cause on his own. In the years prior to the attacks, Breivik continued to show support and made contact with several far-right organizations including the English Defence League (EDL) and the Norwegian Defence League (NDL). Breivik became a member of the Norwegian Defence League, but was later removed for

being too extreme in his views. As Gibbs' (2010) left realist perspective stated, Breivik continued to seek interaction in the extremist movement even though he saw himself more as a leader in the right-wing movement and a savior to the cause.

As the individual is integrated with other group members and becomes committed to the same cause, the individual starts to depend on the terrorist organization. Eventually the need for social acceptance can only be provided by the organization or cause (White, 2002). However, according to Gibbs, "peer support" does not have to be through direct contact with others. Written communications and other forms of media can provide the same support structure to a terrorist (Gibbs, 2010). This explains how the phenomenon of lone wolf terrorism comes to fruition and how these leaderless individuals develop their ideology. Each of the above mentioned lone wolf terrorists were directly and indirectly drawn to their respective movements through interactions with political groups, published works, online forums and articles, etc. Bartol and Bartol's (2011) research on lone wolf terrorists found that "alternately, they adopt the ideological or philosophical leanings of an extremist or outside group, even when the group itself does not engage in terrorist activities" (p. 337). This was specifically seen with Anders Breivik, as the FrP and the NDL both fought against immigration and multiculturalism but rejected the violence and condemned the attacks committed by him. The inspiration to create a terroristic creed can be acquired through writings, published books, speeches, rallies and even the Internet. While terrorist organizations utilize these outlets for recruiting, lone wolf terrorists use it for inspiration. "Indeed, most terror groups have websites and the World Wide Web offers terror groups another platform on which to spread their message" (Gibbs, 2010, p. 178). Other studies have also found that the Internet is used to inspire and assemble terrorists and their networks in

Europe (Sciolino, 2008). Uniting individuals towards a common cause makes it that much easier for an organization to manipulate individuals to attack highly sought after targets.

Social Factors

A terrorist is not just affected by their psychological makeup alone; social (to include political, economic and theological) factors are also a part of the cause to bring an individual to the point of engaging in acts of terrorism (Hudson, 1999). As mentioned before, many different individuals become terrorists, however a majority of members are young men (Bartol & Bartol, 2011). These individuals lack a sense of self and are socially alienated. (Hudson, 1999; Bartol & Bartol, 2011). Potential terrorists have a desire to belong and want to gain a sense of purpose. Individuals start out by becoming sympathizers to the cause and showing passive support by attending an organization's outreach rally, actively or passively becoming involved in protests, reading and purchasing written books and documents by the organization or about the cause and/or practicing in their beliefs (i.e. attending meetings or religious venues). Timothy McVeigh actively protested government oppression outside the incident area during the ATF raid of the Branch Davidians in addition to being influenced by published works such as the "Turner Diaries". Tamerlan Tsarnaev began to visit the local mosque and practice the Islamic faith in addition to reading documents and participating in online forums on Al Qaeda websites. Anders Breivik remained in contact with right-wing extremists and supported right-wing political groups. Eric Rudolph read anti-homosexuality and anti-abortion literature and it is believed that he was influenced by the extremist organization Army of God (Monsky, 2000).

The social learning theory states that criminal behavior is learned and that external factors play a role in this. Therefore lone wolves learn to engage in acts of terrorism through observational learning, idolization and/or differential association. This can be explained through

Skinner's operant learning. The potential terrorist is receiving positive reinforcement by associating with the group. Just as the left realist theory demonstrated, they are gradually integrated into the ideals of the other members. They begin to feel accepted and aspire to gain more recognition from the group. A yearning to continue receiving the pleasant stimulus (sense of belonging or purpose in life) will motivate the once alienated individual to directly or indirectly conform to the extremist organization's beliefs. Potential terrorists seek to imitate the members of the group or specific individuals for the cause to continue the acceptance. Timothy McVeigh was indirectly influenced by William Luther Pierce as his attack was based on the attacks committed by the characters in the extremist novel "The Turner Diaries" written by Pierce. Both Eric Rudolph and Anders Breivik were influenced by McVeigh in their attacks. Breivik even constructed his bomb from an online recipe that was similar to what McVeigh used. In the case of the Tsarnaev brothers, Tamerlan was influenced by the Chechen rebel fighters whom he visited during trips back to his home country and attacks committed by Islamic militants like Al Qaeda. The reason Dzhokhar engaged in the attacks was because of his brother Tamerlan. Dzhokhar did not display as much resentment towards the United States and became well integrated into American culture. However, Dzhokhar began to have an extremist view of America through his brother's influence. Dzhokhar idolized and respected his brother as Tamerlan was viewed as the patriarch of the family. Building off of Skinner's operant learning, Dzhokhar displayed imitational learning towards criminal/terroristic behavior. Imitational learning (also known as observational learning) was introduced by Bandura (1973) and identifies that people mimic who they idolize. Because Tamerlan gradually became integrated into the Islamic jihadist movement and actively proclaimed support of his faith and disdain for an oppressive United States, Dzhokhar eventually followed suit. This was seen by Dzhokhar's

friends as he started to proclaim his support of terrorism and justification for the attacks on 9/11. He then began to distance himself from his friends, focus more on Islamic and Extremists beliefs instead of school and utilized the Internet to read jihadist literature. Eventually, Dzhokhar engaged in the planning and execution of the Boston Marathon bombings with his brother.

Reason Attacks Happened

Even though each of the lone wolf case studies identified motivated individuals who were committed to their belief and the cause they sought to fulfill, it was not the only reason for their successful attacks. Focusing on the act itself and not just the individual who committed the act can show a different perspective on lone wolf terrorism. The Routine Activity Theory was developed by Marcus Felson and Lawrence E. Cohen and demonstrates that criminal situations need to have three things present in order for them to occur. There needs to be a criminal/offender, a victim/target and a lack of protection/absence of a guardian (Clarke & Felson, 1993). In order to explain why the attacks committed by the lone wolves in the previously mentioned case studies were able to occur, the focus should be on the absence of a guardian. In all forms of terrorism it is easy to identify the offender (the individual terrorist or terrorist organization) and the target (those they are fighting against to fulfill their cause). However, the absence of a guardian is the one that stands out because in each attack there is reason to believe that guardians were present. It would stand to reason that each of the attacks committed by the lone wolves had some form of a guardian present. McVeigh's bombing was at a Federal Building which housed several law enforcement agencies and had federal security present. Rudolph's bombing at the Olympics had several law enforcement agencies and security agencies present conducting security checks. Breivik's bombing was at a Government Building which had security officers. The Boston Marathon bombing committed by the Tsarnaev brothers

had Boston PD and security personnel present. So why were they able to accomplish their attacks in spite of guardians being present. The answer is unfortunately pretty simple. Though deterrents were put into place to stop the general criminal from committing a crime, terrorists are more motivated in their cause and are willing to get caught or die to complete their task. Their commitment to the cause is a joint effort to achieve a winning outcome. The organization idolizes the true patrons of the cause by glorifying their deeds, actions, and commitments even when they are not directly connected with the collective such as with lone wolves. "Terrorists often experience considerable social and moral support...they are often regarded by their in-group as heroic freedom fighters and religious martyrs" (Bartol & Bartol, 2011, p. 345). Eric Rudolph was praised by the Army of God organization as a warrior for their cause and Timothy McVeigh is glorified by right-wing extremists as a defender against government oppression. The potential terrorist ultimately sees the desire for glory and a sense of meaning as the driving force for their actions. This can explain how a socially unaccepted individual can be molded into a suicide bomber, which is to obtain the greatest success within the organization. "The message that adolescents receive, extolling a utopian and transcendent immortality for the suicide bomber, may be particularly attractive" (Post et al., 2009). Each terrorist organization has a different set of goals. Not only is every individual terrorist unique, but each terrorist organization differs in their tactics and personality. This makes it impossible to develop a standard counterterrorism tactic to use against all terrorist groups. Each group must be handled differently.

Policy makers make use of the Routine Activities Theory in creating criminal prevention regulations and programs. Unfortunately many policies are also established after a severe incident occurs or mistake is made. After 9/11 airport security practices have increased tremendously. In an analysis of O'Hare International Airport, with this increase in security to

prevent future terroristic acts other crime activity, specifically larceny, has decreased at the airport. By applying the Routine Activities Theory, airport security focuses on the situational context and not the characteristics of the perpetrator thereby removing the criminal opportunity and reducing the vulnerability of the victim (Johnson, 2010).

Hactivism and the “Anonymous” Hacker Network

Hactivism is a recent phenomenon that first came about in the mid-1990s as another way for people to protest their perceived grievances to companies, government organizations and the world. The hactivism movement is focused on the freedom to share information and computer software in cyberspace. However, unlike normal protests that are conducted through a physical presence in the form of public speeches, sit-ins, parades, rallies, etc. this type of protest exists in cyberspace through the use of hacking techniques, computers technology and digital networks (Krapp, 2005; Penny, 2011; Taylor, 2005; Taylor, et. al, 2011; Vamosi, 2011).

Originally, this form of protest consisted of online graffiti of government or company web-pages and offered free digital information and data (Hampson, 2012; Krapp, 2005; Taylor, 2005; Vamosi, 2011). But as digital technology and the Internet has expanded, hactivists have become more aggressive and vicious in their tactics (Hampson, 2012; Vamosi, 2011).

Hactivists now engage in cyber-attacks in the form of Distributed Denial of Service (DDos) attacks, email bombings, diverting Internet traffic to false mirror sites, and writing or uploading computer viruses in an effort to accomplish their goals. There are a number of different collectives that are comprised of both hackers and supporters with no designated leader but are jointly unified in one cause. One of the most infamous hactivist groups that has declared war in cyberspace is the network of individuals known as “Anonymous”.

Originating in 2003, Anonymous is a leaderless network comprised of both activists and hactivists who are unified in their perceived social and political injustices they see throughout the world (Hampson, 2012; Penny, 2011; Taylor, 2005). The reason for their name is that it is used as a reference to the facelessness of their collective, being that the hactivists and activists associated with the network, share one identity and do not seek individuality (Hampson, 2012;

Penny, 2011; Reitman, 2012). This is further emphasized by the fact that when they are engaged in public protests or post online videos, those associated with the collective wear Guy Fawkes masks (which was made famous in the movie “V for Vendetta” to which the anarchist in the movie would wear such a mask) (Hampson, 2012). In recent years they have been involved in numerous cyber-attacks against both government organizations and private businesses. These include engaging in a DDos attack on the Scientology and Tunisian government websites, accessing user account information and shutting down Sony’s computer network, acquiring personal information of both military personnel and law enforcement officers and releasing it to the world on the Internet, and most recently posting personal information and photographs of members of the Ferguson Police Department after the shooting of Michael Brown (Hampson, 2012; Mills, 2011; Penny, 2011; Saporito, 2011; Taylor, 2005; Vamosi, 2005). Their victims range from large companies such as VISA, Mastercard and Paypal, law enforcement agencies and governments (Bever, 2014). Anonymous has collectively organized these attacks with such names as Project Chanology, Operation: Payback is a Bitch, Operation Tunisia and Operation Ferguson (Bever, 2014; Hampson, 2012). The Anonymous network has also shown its support for political protests such as the Occupy movement by attacking the website of the New York Stock Exchange and assisting the organization with protests around the world via the Internet (Hampson, 2012; Penny, 2011; Saporito, 2011).

Analysis of the Hacktivist Network

Though the computer capabilities of hacktivist networks like Anonymous are undeniable, they are viewed by many law enforcement agencies and government officials as a second rate threat to the world. They view cyber-attacks caused by nation-states, like the Stuxnet virus, as a more pressing issue that needs to be addressed (Penny, 2011). I would have to agree with this

security assessment due to the fact that no cyber-attack by a hacktivist has caused permanent damage or a loss to human life. But, what happens if the collective becomes motivated enough to commit an attack similar to the Stuxnet worm? What happens if they see no other way to get their point across and instill change than to create a realistic threat to the public? Several other extremist organizations started out as a collective group of individuals protesting what they viewed as a valid cause. The Animal Liberation Front wants to change U.S. policy on animal testing, Earth Liberation Front is against the destruction of the environment, and the Army of God is a Christian organization against abortion. Each group is seeking to change a perceived injustice through public protests and activist pursuits. Nevertheless, these as well as other organizations have become more violent over the years, participating in bombings, kidnapping and assaults, and destroying buildings and pieces of equipment. These same groups are now labeled as domestic terrorist organizations. It would stand to reason that a similar course of action could take place among the hacktivist collective. Based on recent events, this way of thinking may not be far from an actual reality. Barret Brown, who is associated with the Anonymous collective, made threats towards FBI agents through online video posts (Gallagher, 2013). Though an isolated incident, this could show that the hacktivist way of thinking is changing because it only takes one individual to influence others.

Felson and Cohen's Routine Activity Theory can also be used to explain how cyber criminals and cyber terrorists are able to commit their attacks. Not only is the number of potential targets in the billions due to the number of people, companies and organizations that utilize cyberspace on a daily basis, the lack of security measures in place is astonishing. Cyber criminals are less likely to be deterred from committing crimes in cyberspace because there is no certainty of arrest and punishment (Taylor, Fritsch, Liederbach, & Holt, 2011). This is due to the

current difficulty of locating and apprehending cyber criminals. There is no set domain in cyberspace, offenders can participate in cyber-activity by using a variety of computer networks and direct their attacks from an individual's or companies' computer server which is not their own (Haley, 2013). This makes it very difficult, but not impossible, for law enforcement agencies to pinpoint the origin of a cyber-attack. The New York Times identified that Chinese hackers were stealing passwords and conducting other illegal activity online (Haley, 2013; Perlroth, 2013). It was also determined that Russian hackers were responsible for attacks on Estonian and Georgian websites which caused significant damage to computer networks in 2007 and 2008 (Haley, 2013). Still, even though there has been some success in identifying and apprehending certain cyber criminals, the vast majority are still freely roaming cyberspace. Until the risk of getting caught increases, or is at least perceived to have increased, cyber criminals will continue to partake in criminal activity.

Analysis of a Potential Lone Wolf Cyber Terrorist Threat

Lone wolf terrorists generally have a different psychological makeup than those terrorists who belong to an extremist group or organized network (Bartol & Bartol, 2011). As mentioned before, in the case study analyses, they do not rely on an affiliation with a group for the justification of their cause. They normally operate alone or with a few select individuals who also have no affiliation with an organization. Lone wolves develop their own method of operation, targets and decision making. In a Q&A with Thompson (2013), Jeffrey D. Simon author of *Lone Wolf Terrorism: Understanding the Growing Threat* has related that because these terrorists think outside the box and are loners by nature with no one directing them, they pose the greatest threat. "Lone wolves have little or no constraints on their level of violence.

They are not concerned with alienating supporters (as would some terrorist groups), nor are they concerned with a potential government crackdown following an attack” (Thompson, 2013, p. 1). They only see the spread of the message towards their perceived cause as the ultimate goal. “Based on their unique interpretations of the world, they perceive injustices that they wish to bring to public attention” (Bartol & Bartol, 2011, p. 337). They tend to adopt the ideology of an extremist or outside group, whether or not that group engages in terroristic acts. Lone wolf terrorists believe they are acting on the group’s or causes’ behalf. With that, the most common ideologies followed by the lone wolves in America are white supremacy and anti-abortion. However, based on recent attacks and the rapid spread of Islamic extremist beliefs via the Internet, the threat of individual and leaderless Jihads is intensifying.

The danger and potential damage a leaderless terrorist is able to cause can be seen in the bombings committed by Timothy McVeigh, Eric Rudolph, Anders Breivik and the Tsarnaev brothers. Each viewed the United States (or in the case of Anders Breivik, Norway) as tyrannical against their beliefs and wanted to seek revenge for perceived past transgressions committed by the government. They initially sympathized or felt a connection with an extremist movement (right-wing, anti-abortion, and Jihad) and eventually took up the cause as part of their own lifestyle. However, they do not directly engage in the group’s activities or actions. They saw themselves as more of an outside medium and soldier for the cause. In the past, as seen with Timothy McVeigh and Eric Rudolph, potential lone wolves became inspired through readings, movies, speeches, political actions or by a number of other outside influences. However, as seen with Ander Breivik and the Tsarnaev Brothers, lone wolves no longer have to leave their home to become inspired. The Internet, along with social media, allows the terrorist to gain inspiration and verbal support to continue their terroristic activity instantly. Extremist organization leaders

and activists no longer have to be directly linked with the lone wolves they are promoting. Instead, they utilize webpages, web forums, videos and public speeches to call upon individuals to up arms and fight for their perceived beliefs. Al Qaeda members have dispersed manuals, training videos and their teachings on the Internet, promoting leaderless Jihad against perceived infidels, specifically the United States (Bakker & de Graaf, 2010; Weimann, 2012). Extremists see the potential acts a lone individual can accomplish with ease that a collective cannot.

As mentioned in the literature review, there are certain advantages that lone wolf terrorists have over an extremist group that causes them to be a greater threat to the world. One danger is that they have no one to restrain them from committing devastating acts of violence. Lone wolves utilize creative and resourceful ideas in their attacks without any consideration for the violence it will create and the innocent bystanders who will be victimized (Bakker & de Graaf, 2010; Simon, 2013; Thompson, 2013). Lone wolves only take into consideration how the attack will spread their perceived cause to the masses and display no remorse for the negative aspects of their attack. With no one to guide them or keep them in check, lone wolves become more dangerous and unpredictable than members of the extremist organizations they follow.

In addition, lone wolf terrorists predominantly work alone which makes them much harder to track or identify compared to a terrorist organization or cell that is outspoken and gathers in small or large groups (Bakker & de Graaf, 2010; Bates, 2012; Spaaij, 2010; Simon, 2013; Thompson, 2013; Woods & Spaulding, 2005). Compared to extremist groups, lone wolves are self-reliant and do not require the guidance, equipment or funding that members of an organizations need. Lone wolves tend to isolate themselves from the rest of society which allows their plans and intentions to go unnoticed to the world, making it harder for law enforcement to anticipate the threat (Bakker & de Graaf, 2010). These individuals require a

limited amount of resources, using material that is available to the general public to make home-made explosives and acquire firearms through legal purchases (Barnes, 2012; Bartol & Bartol, 2011; Spaaij, 2010). When these individuals are initially discovered by law enforcement agencies, specifically in the United States, it is difficult to determine who is using their freedom of speech and simply preaching radical beliefs versus those who actually intend to commit terrorist acts (Bakker & de Graat, 2010; Bates, 2012; Burton, 2007). “Knowing that all terrorists are radical but that most radicals are not terrorists, it is extremely difficult to single out potential lone wolves before they strike, even with the help of most sophisticated intelligence gathering tools” (Bakker & de Graaf, 2010, p. 5). Therefore, lone wolves have an easier time staying in the shadows and blending in before they finally strike.

One of the more significant and obvious reasons why America is vulnerable to a cyber-attack is due to the United States’ involvement in the Middle East. The United States has been a longtime ally and supporter of Israel, specifically with the Israeli–Palestinian conflict. The conflict is a result of both sides believing that they have a claim to Jerusalem, which they see as a location promised to them by God. The Israeli–Palestinian conflict has expanded to involve other Arab countries, creating an Arab-Israeli conflict in the Middle East (Rabinovich & Reinharz, 2008). Because of America’s demonstrated support towards Israel and their presence in the Middle East, Al Qaeda, Hezbollah and other Islamic extremist organizations view the U.S. as the enemy. These organizations seek to remove the United States’ and Israel’s control in the Middle East and believe that their struggles will end once both parties are obliterated (Post, Sprinzak, & Denny, 2003; Rabinovich & Reinharz, 2008; White, 2003). Initially, Islamic terrorist organizations took the approach of using guerilla warfare, propaganda, and violent scare tactics as a means of accomplishing their objectives. Later on, they expanded into more violent

strategies through the use of elaborate bombs, mass shootings with machine guns in public places and using vehicles in the destruction of buildings as seen in the attacks on 9/11. As improvements in technology change, so do the tactics used by terrorists. Islamic terrorist organizations have now shown an interest in cyberspace as another platform to achieve their goals.

Up until now, the Internet has been predominately used by Islamic terrorist organizations as a means of spreading their beliefs and perceived transgressions as well as recruiting members to their cause. Even though a majority of terroristic tactics in cyberspace has been used for propaganda, the threat for a more serious cyber-attack on the United States is imminent. "An al-Qaida safe house in Pakistan was reportedly used to train jihadists in computer hacking and to conduct reconnaissance on supervisory control and data acquisition systems, which manage critical infrastructures" (Wagner, 2007, p. 35). Other researchers have found similar evidence regarding terrorist organizations showing an interest in and training some of their members to use computer technology as a means of conducting coordinated attacks on the United States and their supporters (Jain, 2005; Weimann, 2011; 2004; White, 2003). "Radical Muslims as well as terrorists worldwide use the Internet to build up effective communication networks and to spread information and propaganda" (Brauchler, 2004, p. 267). Websites and online forums have also been generated by Islamic extremists who depict their organization's history, beliefs, and the attacks/incidents for which they have taken credit (Tsfati & Weimann, 2011). These webpages allow access to a much larger audience and offer a way for organizations to influence others in a way that media outlets and public protests cannot. They are used to rally potential supporters of the organization's cause, as well as instill fear and sway their adversaries from continuing their efforts (Brauchler, 2004; Tsfati & Weimann, 2011; Weimann, 2011; 2004). These same

websites have the potential to create and call upon lone individuals to engage in leaderless terroristic activity in the name of the organization's cause. This was seen most recently with the lone wolf terrorists Anders Breivik and the Tsarnaev brothers, who were both influenced in their extremists beliefs and how to create/commit their attacks through the Internet. Despite the fact that terrorist organizations present a clear and present danger to America's infrastructure and their citizens, they are not the only threat in cyberspace.

A lone computer hacker or cyber-terrorist has the same ability to cripple the United States that a terrorist organization does. Previous incidents have shown the potential damage that a hacker who is against the U.S. government can present. The power outages that took place in New Orleans back in 2008 were confirmed by the CIA to be the result of cyber-attacks conducted by unidentified hackers. A Chinese hacking group was also linked to the creation of a "slammer" computer worm which disabled 911 emergency systems and ATM machines in January of 2003 (Piggin, 2010). Hackers have developed other computer programs which have been turned into cyber weapons.

Thaanum's (2013) research found the following:

The Rabbit Virus (1974), Elk Cloner (1981), Pakistani Flu (1986), The Morris Worm (1988), Michelangelo (1992), and so forth. These digital weapons, these cyber weapons, slowly evolved from the 1970s to the end of the 20th century. Since 2000, the amount of weaponized code has grown exponentially and has shown no signs of slowing down. One of the latest pieces of weaponized code is StuxNet; a highly sophisticated computer worm that targeted Iran's nuclear program and caused its centrifuges to essentially melt down. (p.491)

Still, one of the most significant attacks in cyberspace was accomplished by two computer hackers in 2001. Hackers Reonel Ramones and Onel de Guzman constructed the computer virus known as the “Love Bug”. The virus was designed to infect computers through email accounts and steal the user’s internet password (Brenner & Goodman, 2002). The end result caused millions of computers across the world, including in the United States, to be infected and resulted in billions of dollars in damages. Although this virus did not cripple or incapacitate the United States government’s infrastructure, the devastation it caused over a decade ago shows the potential that a computer virus is capable of doing. In spite of everything that was mentioned, there is one less obvious factor that allows a country like the United States to become vulnerable to a cyber-attack, which is the unintentional threat from within.

Cyber security breaches and the infiltration of computer systems could be the result of the hacker’s or cyber-terrorist’s level of proficiency, an unforeseen cyber weapon program, a lack of government funding or a number of other possible scenarios. However, a more likely yet less obvious reason can explain America’s vulnerability. “[S]temming to its source, the principle issue for threats to cyber security and how they happen are mainly due to human error. A massive contributor to programming flaws and glitches are from the programmers themselves” (Thaanum, 2013, p. 492). Human error is an often overlooked dilemma, yet a just as equally threatening factor, in identifying America’s susceptibility to an attack in cyberspace. The result of these errors can be seen on a daily basis. From the number of glitches left on computer software and electronic devices so that companies can get the products to the consumer faster and turn a profit, to the acceptance of malicious malware from websites and emails by the general public. Researchers have identified that computer programmers are developing insufficient cyber security systems with backdoors and alternate access points which cyber

criminals have used to their advantage (McGraw, 2013; Moss, 2013; Preimesberger, 2008; Thaanum, 2013). Then again, programmers are not the only ones at fault. Government employees and the general public have also contributed to the reason why America is so vulnerable. People accept emails, files and applications to download onto their smartphones and computers, even when pop-up notifications appear on the screen warning them of the potential danger or threat to their system (Thaanum, 2013). A majority of people keep classified and personal information stored on these devices and it is not out of the realm of possibility that a malicious virus could be imbedded on the downloaded file, infecting the system and retrieving the confidential information. The computer virus could then spread onto other computer systems that are on the same network as the originally contaminated gadget and result in a massive system shut down or theft of digital funds and confidential information. Human error is a vulnerability that can be easily remedied through a series of computer program/system checks along with training and education. Nevertheless, the human element is often overlooked but always present in every situation and should be taken into consideration when addressing the issue of the United States' vulnerability in cyberspace.

Many researchers have determined that because most countries' infrastructures are run by computers, cyber-terrorism is an imminent if not immediate threat to national security. These cyber-attacks could even come without initial warning. Developing computer viruses, breaking computer firewalls and creating backdoor programs in order to implement a terrorist attack could take years to plan, but once all the computer data needed is acquired, it can be implemented instantly. A letter was discovered by the United States government from Osama bin Laden addressing the use of modern technology to destroy capitalist states' economies (Weimann, 2004). Other researchers have identified the possibility of terrorists planting "logic bombs"

viruses that would lie dormant in computer systems for years until a code instructs it to overwhelm a computer's system (White, 2003). Due to the fact that most banking systems, financial records and the stock market are all conducted and stored on computer software and hardware, crippling and destroying a country's economic structure is possible. Jain (2005) identifies that businesses, specifically those that operate globally are significantly vulnerable to these cyber-attacks. Leon Panetta, former Secretary of Defense, stated that "A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11....such a destructive cyber terrorist attack could virtually paralyze the nation" (Williams, 2012). Other possible areas that could be attacked virtually in the future are utilities and services, since most of these systems are now run solely through computer software. Water supplies could be shut off or contaminated, power grids could be shutdown, and air traffic control systems could be hacked all with one key stroke (Jain, 2005; Prasad, 2012; Tafoya, 2011; Williams, 2012). Train systems also have the potential to become targets. The tracking control systems could be hacked which would result in derailments and crashes of passenger trains or even more dangerous trains that contain lethal chemicals as their cargo (Jain, 2005; Williams, 2012). The combination of a physical attack on a country in addition to multiple services being attacked or shutdown through cyberspace would cause the most destruction and widespread panic (Weimann, 2004; Williams, 2012). Weimann anticipates the possibility that terrorist groups could combine the physical with the virtual; an attack might include a bombing with the launching of a cyber-attack that disrupts the communication infrastructure (Weimann, 2004). The same potential threat could be said for a lone individual hacker or small group of leaderless hackers. A lone wolf cyber terrorist or a collective of lone wolf cyber terrorists has the potential to commit a devastating cyber-attack or combine that attack with a physical attack in the form of

a bomb or coordinated shooting. However, the evaluated case studies of the four lone wolf terrorists establishes that unlike most members of extremist organizations, they were able to remain hidden from the world until they finally committed their attacks. This demonstrates that lone wolf cyber terrorists present an even greater threat to the world as their activity will remain unnoticed until it is too late.

Chapter Summary

Since the turn of the century, terrorism has become a major area of concern among law enforcement agencies. Most people associate terrorism with international terrorist organizations like Al Qaeda and Hezbollah. However, in recent years most attacks have been perpetrated by “lone wolf” terrorists (Thompson, 2013). A lone wolf terrorist is an individual or small group of individuals who use terroristic tactics to achieve their ideological goals but act without any membership to a terrorist organization (Weimann, 2012). “The lone wolf operators do not rely on group or organization affiliations to validate their missions” (Bartol & Bartol, 2011, p. 337). One of the most well-known lone wolf terrorists is Timothy McVeigh. McVeigh committed one of the most devastating forms of domestic terrorism the world has ever seen and showed the destruction a lone actor can truly cause. Other lone wolf terrorists include Eric Rudolph, Anders Breivik and most recently with Dzhokhar and Tamerlan Tsarnaev in the Boston Marathon bombing. Though terrorist attacks have existed throughout history, the attacks committed by lone wolf terrorists have radically increased in recent years with the potential to continue to rise and branch out into new areas in years to come.

In addition, cyber-terrorism presents a new threat to both national security and the world. In light of the fact that society has become so dependent upon technology, the infrastructures of both businesses and countries are potential targets for attacks by cyber-terrorists. The best way to combat the threat of cyber-terrorism is to understand the behavior of the individuals who commit these attacks. Identifying a cyber-terrorist’s criminal psychopathology is no different than describing any other individual who has extremist ideals. Cyber-terrorists are just as politically motivated in their actions as those who are involved in the use of terrorism. A cyber-terrorist’s goal is to change the political or social policy, position, or control with their attacks

being focused on social, political, economic, geographic, and/or religious structures. One of the main goals behind their cyber-attacks is to cause fear and panic, believing that this in turn will influence political change and alter the course of history. Terrorism is in the “eye of the beholder” and unfortunately what we perceive to be heinous and despicable attacks, such as the Oklahoma City bombings and attacks on 9/11, other individuals see as justified in the fight against their perceived struggle (Bartol & Bartol, 2011; Hudson, 1999; White, 2003). The lone wolf cyber terrorist is an even greater threat when committing these acts because they do not take into account or care about the collateral damage to supporters of their cause in addition to their intended targets. The lone wolf only sees the spread of their message and the punishment of perceived moral transgressors as the ultimate goal, no matter the cost. Lone wolves are innovative and think outside the box with no restrictions on what they can do (Thompson, 2013). The lone wolf terrorist does not have the constraints that members of a terrorist organization do. They are not concerned with alienating their supporters and are only interested in carrying out their beliefs and actions that support the cause (Thompson, 2013). This way of thinking makes a lone wolf terrorist more dangerous in cyberspace. Terrorist organizations carefully plan and take every measure into account when engaging in cyber terrorism; seeing that only certain systems or countries are infected by the cyber-attack, so not to lose their supporters. Unlike these organizations, the lone wolves do not concern themselves with collateral damage or upsetting their supporters, just that their message is received. “Based on their unique interpretations of the world, they perceive injustices that they wish to bring to public attention” (Bartol & Bartol, 2011, p. 337). Thus, in the eyes of the lone wolf, the creation of a virus or the hacking of computer programs, no matter who is affected by it, is valuable for their alleged cause.

This shows that a dedicated lone wolf hacker or a group of lone wolves can develop a malicious piece of software, similar to the Stuxnet Virus, which has the capability to cause a significant amount of damage and loss of life. The devastation one piece of malware program can cause further establishes the potential threat a lone wolf cyber terrorist could be capable of doing. This new form of terrorism is ideal for a lone wolf to seek out and utilize in the fulfillment of their cause. Certain lone wolf terrorists can now develop into computer hackers instead of bomb makers. This is why activist organizations comprised of hackers, also known as hacktivists, present a growing threat to the United States and the world. A lone wolf, who may also be an experienced hacker, may end up believing in the hacktivist ideology and willing to support their cause through direct or indirect interaction. Timothy McVeigh grew to support the right-wing movement through reading anarchist literature, specifically the Turner Diaries, and witnessing the incidents of Ruby Ridge and Waco Texas. Tamerlan Tsarnaev was persuaded to go against American society after he was denied his dream and began to read anti-American propaganda on Islamic Internet sites and chat rooms. Lone wolves are capable of adopting the perceived transgression of a hacktivist network, like Anonymous, and begin to engage in terroristic activity in the name of that cause. If hackers become motivated by a real world “offline” issue and resort to terroristic tactics then there may be no end to the degree of damage they could inflict in cyberspace and to the world (Hampson, 2012). Despite the fact that most attacks committed by lone wolf cyber terrorists have only affected certain areas or systems, the potential for domestic and international attacks on critical infrastructures in cyberspace is present.

However, looking a little deeper into the behavior of a cyber terrorist or a lone wolf cyber terrorist, one will see that they were not born to be a terrorist. The ideals and principles held by

an individual who engages in cyber-terrorism are gradually learned over time through positive reinforcement and differentially associating with other extremists. Individuals were originally isolated and felt shunned by the rest of society and ended up seeking a sense of purpose and yearning for acceptance. Through online and personal interaction with members of an extremist organization they start to acknowledge the group as a way to receive both. The individual eventually becomes totally committed to the cause which will lead to them committing attacks in cyberspace. Thus, the behavior of a possible lone wolf cyber-terrorist cannot simply be explained through the use of the political theory. Even though lone wolves and hackers are motivated towards a political agenda, there is still a much deeper element which explains their commitment to the extremist organization.

Chapter 5

Discussion

This capstone research project focuses on analyzing characteristics of lone wolf terrorism and cyber terrorism in order to determine the likelihood that a lone wolf cyber terrorist could emerge. Several conclusions can be made based on this research. From the collected data it is clear that lone wolf terrorism can be very destructive and it could be difficult to apprehend the suspect or prevent the attack by the lone individual from occurring. The four case studies show that a majority of their planning and preparations for the attacks remained hidden from the world until it was too late. They utilized items that were easily accessible to the general public, obtained firearms through legal means and acquired the plans to construct their explosive devices through available reading material or past training.

Similar to Spaaij's (2010) research study this research project establishes that lone wolf terrorists develop their own ideology because they seek a sense of purpose due to their own deprivations and vexations and cling to a political cause. Based on the findings, terrorism is an ideal that attracts individuals who are isolated and seeking a sense of purpose. These types of individuals yearn for acceptance and see the extremist cause as a means of receiving both. By integrating with the organization's or group's belief they lose their individuality and are gradually swayed towards an extremist view of the world. As a result, they see terrorism as the only means of fulfilling the cause and spreading their perceived grievances to the world. However, despite the fact that the lone wolf's principles are dictated by the organizations they follow, their own personal frustrations and deprivations augment them into a more volatile and leaderless form of terrorism.

In addition to them being loners and difficult to track, there is also no set profile for a lone wolf terrorist. “[I]one wolf terrorists comprise a wide variety of violent extremists. Among them are religious zealots, environmental and animal right extremists, white supremacists and jihadists” (Bakker & de Graaf, 2010, p. 2). A terrorist, including the lone wolf, is not just affected by their psychological makeup. Social (to include political, economic and theological) factors are also a part of the cause to bring an individual to the point of perpetrating terrorism (Hudson, 1999). Eric Rudolph was motivated by an anti-abortionist and anti-homosexuality perception; Timothy McVeigh and Anders Breivik both had far right militant ideologies; and most recently the Tsarnaev brothers were motivated by extremist Islamic beliefs (Bakker & de Graaf, 2010; Spaaij, 2010; Thompson, 2013). A variety of individuals can view certain aspects in society differently than others. What one person sees as justice or routine, another interprets as political or religious dissension. Though it is difficult to develop a profile of a lone wolf terrorist, the one common characteristic is the strong belief in a cause and the will to fight for it. Lone wolves want to instill fear and create chaos in order to change an outcome socially or politically. They are highly motivated and use symbolic attacks to make a statement. With their vision to think outside of the box a new wave of terrorism is approaching and becoming an imminent threat through the use of modern technology.

The introduction of cyber terrorism has become an apparent and imminent threat to national and international security that could potentially be committed by lone wolf terrorists. “Cyber terrorism is aimed primarily at disrupting or destroying a crucial infrastructure, using the Internet to facilitate traditional terrorism, and information attacks, which are aimed at destroying important electronic data” (Jain, 2005, p. 7). Past computer viruses created by hackers, such as the Love Bug virus created by Reonel Ramones and Onel de Guzman and the Stuxnet Virus

which almost caused a nuclear meltdown in Iran, have the potential to be catastrophic to a country's social and economic system. Simon believes that these attacks are tailored for the lone wolf terrorist because they have no need to leave their home to create the program and launch the computer driven attack (Thompson, 2013). Lone-wolf hackers have disrupted computer systems in the past and continue to show a presence in cyberspace. It is possible, in the not so distant future, for an individual to become motivated enough over a perceived strife to succeed in the first major cyber-attack on a country's infrastructure.

An increase in cyber-attacks carried out by black hat hackers, as well as politically and socially motivated hacktivists from collective networks, is anticipated by law enforcement professional in the near future (Hampson, 2012; Taylor, 2005; Taylor et. al, 2011). Some researchers suggest that the recent pursuits of online website WikiLeaks is just a foundation for future types of avant-garde activities that America and the world will be faced with (Hampson, 2012; Krapp, 2005; Taylor, 2005). Attack campaigns by hacktivist organizations, such as those initiated by the Anonymous group and Operation Payback, who utilize virus programs, DDos attacks, email bombings, and Internet spam campaigns will continue to grow. Cybercrime has become the wave of the future and is being pushed to the forefront as an issue that must be dealt with (Hampson, 2012; Taylor, 2005; Taylor et. al, 2011). Based on the recent wave of weaponized computer viruses, as seen with the Stuxnet Worm, law enforcement agencies and government officials can no longer view cybercrime and attacks in cyberspace as a minimal hazard. The analysis on the Anonymous hacktivist network identified that the type of activity the members associated with the network has progressively shifted to a more aggressive approach in order to air their grievances to the world. Originally these hacktivists voiced their opinion on the Internet and committed minor website graffiti. However, their members have

shifted to more disruptive and destructive cyber-attacks in the name of their cause and protest their perceived injustices. Based on the findings, with no evidence showing that these hacktivists have regressed back to a more peaceful form of protesting, these cyber-attacks will only continue to become more aggressive and damaging. It is also likely that a single hacktivist with or without a connection to the collective will take a cyber-attack to the extreme, resulting in the loss of human life. The fact that society has become so reliant upon technology to maintain and control critical infrastructures, the potential danger to both the real world and cyberspace that a lone hacker presents to the world is more threatening now than it has ever been before.

Lone wolf terrorists have also utilized whatever means are at their disposal in the fight for their cause. In each of the four case studies, the lone wolf terrorists used tactics and material that were easily acquired and readily available to them. The bombs were easily constructed from material and instructions that anyone could obtain. Based on these findings it would stand to reason that lone wolves seek the easiest yet most effective way to create panic and cause destruction. The acts of terrorism are always changing and evolving with society. The tactics utilized in the past may not work or be as effective in the present. Cyber terrorism has emerged as a new means of engagement in the names of the terrorist's beliefs. Cyber terrorism is a terrorist attack in cyberspace, with cyberspace itself being the place where computer programs function and computer data is moved (Conway, 2002). In order for cyber terrorism to be successful it simply has to significantly hamper an organizations or countries infrastructure and does not have to create physical harm or economic devastation (Hardy, 2011). Because everything is connected through computers, terroristic attacks in cyberspace can have an effect on the financial market, services, and data files and networks, which would likely create widespread panic among citizens and businesses. It is then only natural for many lone wolf

terrorists to engage in this new form of terrorism as a means to display their frustration or support their cause. The lone wolf terrorist's threat is no longer a simple shooter or bomb maker but a sophisticated computer hacker.

Clearly, law enforcement agencies and government officials understand that terrorism tactics are always changing and expanding into new areas which includes cyberspace. Governments have therefore established policies and penalties to prosecute cyber terrorists. "The USA Patriot Act of 2001 and the Cyber Security Enhancement Act of 2002 finely calibrate the penalties for cyber-attacks against infrastructure according to the level of harm caused" (Hardy, 2011, p. 159). In the United States, any offense under these acts is considered a federal crime although the maximum penalty, which is life imprisonment, is only justified if the cyber-attack causes or attempts to cause loss of human life. Nevertheless, in order to minimize the impact of the imminent threat of cyber-attacks and apprehend the cyber terrorists who initiated them, government agencies as well as businesses must understand their own vulnerabilities and establish cyber-specific preventative measures. The FBI has established the InfraGard program and the National Infrastructure Protection Center so that individuals in law enforcement, government and private sectors can work together and share information in an attempt to protect critical infrastructures (Jain, 2005; Mueller, 2012). The CIA has created websites for the purpose of attracting existing and potential jihadists who are seeking online forums to discuss terrorism-related activities (International Debates, 2011). Agencies are also constantly monitoring fundamental computer systems in order to detect intrusions. These cyber intruders are then identified and investigations are launched in order to prosecute. Government agencies have been aggressively tackling terrorist threats to the United States, including the threat in cyberspace. However, some citizens believe that because of these tactics and acts, certain ethical

violations have been committed by government agencies. A current assessment of these potential violations is needed in order to effectively police cyber terrorists without violating a person's rights.

Based on the current acts implemented by the United States government, many citizens believe that certain rights are being violated, specifically the right to privacy and unlawful search and seizure. This fear of government spying was recently brought about due to leaked information from former NSA computer specialist Edward Snowden. Snowden revealed classified data about surveillance programs that government agencies were using to gather information on individuals in other countries as well as citizens of the United States. The NSA developed the computer program Prism in 2007, which allows the agency to collect data from an individual's search history, email content, computer file transfers and live chat sessions (Greenwald & MacAskill, 2013). Snowden also revealed other similar computer programs, which includes XKeyscore and Tempora, implemented in the U.S. as well as the U.K. Snowden was driven to inform the general public what the government was doing against them, stating that "the government has granted itself power it is not entitled to" (Greenwald, MacAskill, & Poitras, 2013). Government officials have condemned Snowden's actions and are attempting to locate his whereabouts in order to prosecute him for treason and stealing intelligence information. Still, this discovery has fueled numerous debates over what is justified for the sake of national security and a person's right to privacy on the Internet. It also brings into question what other government programs are secretly implementing in the name of national security. It is known that certain freedoms must be given up for the sake of security: baggage and body inspections at airports and public events, background checks when applying for certain jobs, being monitored by surveillance systems at government facilities and places of businesses, and

even on traffic stops citizens are being recording with audio and visual equipment. Then again, how many freedoms are people willing to give up and how much power are we willing to give to law enforcement agencies for the sake of combating lone wolf cyber terrorists and the threat of terrorism itself?

Conclusion

This research study attempted to assess the possible threat a leaderless individual could present in the real world and cyberspace. A review of the literature found that there is a recent increase in both lone wolf terrorism and cyber terrorism and present an apparent and imminent threat to national and international security. Government agencies and organizations have identified that the infrastructures of both businesses and countries are potential targets for cyber-attacks due to the dependency upon technology. Based on previous attacks committed by leaderless individuals and cyber-attacks in the form of computer viruses, the potential damage from one or both can be catastrophic to a country's social and economic system. A lone wolf terrorists or hacktivist has the potential to cause even more destruction and harm to innocent bystanders because they are less likely to be swayed from committing the terroristic attack due to collateral damage. Their focus is only on punishing those who are inhibiting their cause and spreading their beliefs to the world.

In view of the fact that society has become so dependent upon technology, the infrastructures of both businesses and countries are potential targets for attacks by cyber-terrorists. The best way to fight the threat of cyber-terrorism is to understand the behavior of the individuals who commit these attacks. Identifying a lone wolf cyber-terrorist's criminal psychopathology is no different than describing any other individual who has extremist ideals. Cyber-terrorists are just as politically motivated in their actions as those who are involved in the

use of terrorism. A lone wolf cyber-terrorist's goal is to change the political or social policy, position, or control with their attacks being focused on social, political, economic, geographic, and/or religious structures. One of the main goals behind their cyber-attacks is to cause fear and panic, believing that this in turn will influence political change and alter the course of history. Terrorism is in the "eye of the beholder" and unfortunately what we perceive to be heinous and despicable attacks, such as the Oklahoma City bombings and attacks on 9/11, other individuals see as justified in the fight against their perceived struggle (Bartol & Bartol, 2011; Hudson, 1999; White, 2003). However, looking a little deeper into the behavior of a lone wolf terrorist, one will see that they were not born to be a terrorist. This research study found that the ideals and principles held by an individual who engages in lone wolf terrorism are gradually learned over time through positive reinforcement and differentially associating with other extremists. Individuals were originally isolated and shunned from the rest of society and ended up seeking a sense of purpose and yearning for acceptance. Through direct or indirect online and personal interaction with members of an extremist organization they start to acknowledge the group as a way to receive both. The individual eventually becomes totally committed to the cause which will lead to them committing attacks. Thus, the behavior of a lone wolf terrorist or cyber-terrorist cannot simply be explained through the use of the political theory. Even though they are motivated towards a political agenda, there is still a much deeper element which explains their devoted commitment to the extremist organization.

Though this research study was unable to come to a definitive conclusion as to whether or not the next significant terroristic attack against the United States and/or the world will come from a lone wolf cyber terrorist, it was able to bring to the forefront the significant threat that a lone wolf cyber terrorist presents. Based on the case study analyses, there is a strong possibility

that a lone hacker/hacktivist could support and fulfill the cause of a hacktivist movement through the use of terroristic activity. This individual would most likely be a loner trying to find a sense of purpose in his life or a hacktivist that disassociated from a hacktivist collective believing that the network was not doing enough for the cause. As most lone wolf terrorist use the weapons and tactics that are at their disposal, the lone hacker/hacktivist is comfortable in cyberspace and proficient with computers and would utilize cyber-attacks or combine it with a physical attack (i.e. a bomb). This lone hacker has the ability to do this because of the lack of guardians that exist in cyberspace. Despite the amount of cyber security available to the world, it is still playing catch up to the rapid advancements in digital technology (Thaanum, 2013). Video games like "Watch Dogs" portraying a hacker that can control and hack an entire city's digital network (traffic lights, surveillance system, power grids, etc.) through the use of a smart phone seemed like science fiction 10 years ago, but it is now a possible reality. Today's smart phones and thumb drives allow for more digital memory storage compared to the giant government computers of the 70s and 80s. Rotary phones and pay phones that could only be used in a set location are now replaced with hand held cellphones that have the capability to hold a video conference with a person while on the go. Digital information systems now control power grids and transportation systems as well as crucial financial services (McGraw, 2013). Facilities which initially needed to be operated and maintained by hundreds of workers are now monitored and stabilized predominately by a computer program. Messages and information exchanges that used to take days or weeks to receive are now received instantly because of the Internet. The current smart phones are just another computer that hackers and cyber terrorists can use to their advantage with both law enforcement and cyber security lacking the technology to stop them (Thaanum, 2013).

Due to the limited amount of research on both lone wolves and cyber terrorists, future studies need to focus on the various forms of terrorism that lone wolf individuals and hackers/hacktivists are willing to engage in. It is important to conduct other case studies on lone wolf terrorists in order to determine if this research study's findings hold any weight when compared with other leaderless individuals. It would also be ideal to compare case studies on known lone wolf terrorists with known criminal (black hat) hackers in order to identify a possible merging of the two. One other significant finding that was not originally anticipated while conducting the case study analysis of the four lone wolves was that each one dealt with significant family trauma (death or divorce) of their parents at a young age. Future research studies should identify if this is a similar developmental characteristic among other lone wolf terrorists.

The development of cyber terrorists along with the increase in lone wolf terrorist attacks is a cause for major concern to the already existing threat of terrorism and an area that needs to be addressed by law enforcement agencies. The threat could come from either terrorist organizations or lone wolf cyber terrorists and would be a multi-tier attack causing damage to many systems at once or a combination of both a physical and virtual assault. The potential damage of an attack that combines the devastation that occurred on 9/11 or at Oklahoma City with the 2003 power outage which blacked out the entire northeastern part of the country would be catastrophic. This type of terroristic attack could occur instantly and would cause widespread panic with no way for law enforcement and emergency personnel to coordinate and respond. Unless systems are reevaluated for potential flaws and improvements are made to cyber security networks, along with training and educating law enforcement personnel, computer programmers and the general public, this theoretical scenario could become a reality in the near future.

References

- Appleton, C. (2014). Lone wolf terrorism in Norway. *The International Journal of Human Rights*, 18 (2), 127-142.
- Babbie, E. (2010). *The practice of social research*, (12th ed.). Belmont, CA: Wadsworth.
- Bakker, E. & de Graaf, B. (2010). Lone wolves: How to prevent this phenomenon? *International Centre for Counter-Terrorism*, retrieved from <https://openaccess.leidenuniv.nl/bitstream/handle/1887/16557/ICCT%2520EM%2520Lone%2520Wolves%2520Paper.pdf?sequence=2>.
- Bakker, E. & de Graaf, B. (2011). Preventing lone wolf terrorism: Some CT approaches addressed. *Perspectives on Terrorism*, 5 (5-6), 43-50.
- Bandura, A. (1973). Social learning theory of aggression. In J.F. Knutson (Ed.), *The control of aggression*. Chicago: Aldine.
- Barnes, B. D. (2012). Confronting the one-man wolf pack: Adapting law enforcement and prosecution responses to the threat of lone wolf terrorism. *Boston University Law Review*, 92 (5), p. 1613-1662.
- Bartol, C. R., & Bartol, A. M. (2011). *Criminal behavior: A psychological approach* (9th ed.). Upper Saddle River, NJ: Prentice Hall.
- Bates, R. A. (2012). Dancing with wolves: Today's lone wolf terrorists. *The Journal of Public and Professional Sociology*, 4 (1), p. 1-14.
- BBC. (2001, May 11). Profile: Timothy McVeigh. *BBC News*, retrieved from <http://news.bbc.co.uk/2/hi/1321244.stm>.
- BBC. (2013, April 22). Profile: Dzhokhar and Tamerlan Tsarnaev. *BBC News US & Canada*, retrieved from <http://www.bbc.com/news/world-us-canada-22219116>.
- Bever, L. (2014, August 13). Amid Ferguson protests, hack collective Anonymous wages cyberwar. *The Washington Post*, retrieved from <http://www.washingtonpost.com/news/morning-mix/wp/2014/08/13/amid-ferguson-protests-anonymous-hacktivists-wage-cyberwar/>.
- Brauchler, B. (2004). Islamic radicalism online; The moluccan mission of laskar jihad in cyberspace. *The Australian Journal of Anthropology*, 15 (3), p. 267-285.
- Brenner, S. W. & Goodman, M. D. (2002). Cybercrime: The need to harmonize national penal and procedural laws. *Technology and Its Effects on Criminal Responsibility, Security and Criminal Justice*, retrieved from <http://www.isrcl.org/Papers/Brenner.pdf>
- Burton, F. (2007, May 30). The Challenge of the Lone Wolf. *Security Weekly*, retrieved from

http://www.stratfor.com/challenge_lone_wolf .

Cassim, F. (2012). Addressing the spectre of cyber terrorism: A comparative perspective. *Potchefstroom Electronic Law Journal*, 15 (2), 380-415.

Chermak, S. M., Freilich, J. D., & Simone, J. (2010). Surveying American state police agencies about lone wolves, far-right criminality, and far-right and Islamic jihadist criminal collaboration. *Studies in Conflict & Terrorism*, 33 (11), 1019-1041.

Clarke, R. V. & Felson, M. (1993). *Routine Activity and Rational Choice: Advances in Criminological Theory* (Volume 5). Piscataway, NJ: Transaction Publishers.

Congressional Digest Corp. (2011). Cyber-terrorism. *International Debates*, 9 (9), p. 10-13.

Conway, M. (2002). What is cyberterrorism? *Current History*, 101(659), p. 436-442.

Cottee, S. & Hayward, K. (2011). Terrorist (E)motives: The Existential Attractions of Terrorism. *Studies in Conflict & Terrorism*, 34 (12), 963-986.

CNN. (1999, May 10). Hackers attack U.S. government Web sites in protest of Chinese embassy bombing. *Cable News Network*, retrieved from <http://www.cnn.com/TECH/computing/9905/10/hack.attack/>.

CNN. (2003, December 11). Eric Robert Rudolph: Loner and survivalist. *Cable News Network*, retrieved from http://www.cnn.com/2003/US/05/31/rudolph.profile/index.html?_s=PM:US

CNN. (n.d.). Timothy McVeigh profile: from decorated veteran to mass murderer. *Cable News Network*, retrieved from <http://www.cnn.com/CNN/Programs/people/shows/mcveigh/profile.html>

Cooper, M., Schmidt, M. S., & Schmitt, E. (2013, April 23). Boston Suspects are Seen as Self-Taught and Fueled by Web. *The New York Times*, retrieved from http://www.nytimes.com/2013/04/24/us/boston-marathon-bombing-developments.html?hp&pagewanted=all&_r=0&pagewanted=print

Farwell, J. P. & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival: Global Politics and Strategy*, 53 (1), 23-40.

Fields, G. & Perez, E. (2009, June 15). U.S. news: FBI hunts lone wolves before they act. *Wall Street Journal: Eastern Edition*, pp. A3.

Fildes, J. (Technology Reporter), (2010, September 23). Stuxnet worm 'targeted high-value Iranian assets. *BBC News*, Retrieved from <http://www.bbc.co.uk/news/technology-11388018>.

Friedlander, B. (2011, July 24). An Interview with a Madman: Breivik Asks and Answers His Own Questions. *Time*, retrieved from <http://content.time.com/time/world/article/0,8599,2084895,00.html>

- Gallagher, R. (2013). How Barret Brown went from Anonymous's PR to federal target. *The Guardian*, retrieved from <http://www.theguardian.com/technology/2013/mar/20/barrett-brown-anonymous-pr-federal-target>
- Gettleman, J. & Halbfinger, D. M. (2003, June 1). Suspect in '96 Olympic bombing And 3 other attacks Is caught. *The New York Times*, retrieved from <http://www.nytimes.com/2003/06/01/us/suspect-in-96-olympic-bombing-and-3-other-attacks-is-caught.html>
- Gibbs, J. C. (2010). Looking at Terrorism Through Left Realist Lenses. *Crime, Law and Social Change*, 54 (2), 171-182.
- Gold, S. (2014). Get your head around hacker psychology. *Engineering & Technology*, 9 (1), 76-80.
- Greenwald, G., & MacAskill, E. (2013, June 6). NSA Prism Program Taps in to User Data of Apple, Google and Others. *The Guardian*, retrieved from <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>
- Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 9). Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations. *The Guardian*, retrieved from <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>
- Gruenewald, J., Chermak, S., & Freilich, J. D. (2013). Far-right lone wolf homicides in the United States. *Studies in Conflict & Terrorism*, 36(12), 1005-1024.
- Haley, C. (2013, February 6). A theory of cyber deterrence. *Georgetown Journal of International Affairs*, retrieved from <http://journal.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence-christopher-haley/>
- Hampson, N. C. N. (2012). Hacktivism: A new breed of protest in a networked world. *Boston College International and Comparative Law Review*, 35 (2), 511-542.
- Hardy, K. (2011). WWWMDs: Cyber-attacks against infrastructure in domestic anti-terror laws. *Computer Law & Security Review*, 27 (2), p. 152-161.
- Hewitt, C. (2003). *Understanding terrorism in America: From the klan to al qaeda*. New York, NY: Routledge, 2003.
- Hudson, R. A. (1999). *The sociology and psychology of terrorism: Who becomes a terrorist and why?* Washington D.C., MD: Library of Congress.
- International Debates. (2011). Cyber-Terrorism. *International Debates*, 9 (9), p. 10-13.
- Jain, G. (2005). Cyber Terrorism: A clear and present danger to civilized society? *Information Systems Education Journal*, 3 (44), p. 3-8.

- Johnson, B. R. (2010). Property Crime at O'Hare International Airport: An Examination of the Routine Activities Approach. *Journal of Applied Security Research*, 5(1), 42-59.
- Keane, L. & Loock, V. V. (2011, August). *Norway massacre: The killers mind*. United States: Discovery Channel.
- Krapp, P. (2005). Terror and play, or what was hacktivism? *Grey Room*, 21, 70-93.
- Kurtz, G. (2010, January 13). Google attack is tip of iceberg. *McAfee* retrieved from <http://blogs.mcafee.com/archive/google-attack-is-tip-of-iceberg>.
- Leonard, C. H., Annas, G. D., Knoll, J. L., & Torrissen, T. (2014). The case of Anders Behring Breivik: Language of a lone terrorist. *Behavioral Sciences and the Law*, 32 (3), 408-422.
- Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22 (3), 365-404.
- Madhani, A. (2011, August 16). Obama: 'Lone Wolf' attack is biggest concern. *National Journal*, retrieved from <http://www.nationaljournal.com/whitehouse/obama-lone-wolf-attack-is-biggest-concern-20110816>.
- Marsella, A. J. (2004). Reflections on international terrorism: Issues, concepts, and directions. In F.M. Moghaddam & A.J. Marsella (Eds.), *Understanding terrorism: Psychosocial Roots, Consequences, and Interventions*. Washington DC: American Psychological Association.
- Mass, H. (2013, May 23). London's gruesome attack and the rising threat of lone-wolf terrorism: Does the world have to worry about a new wave of Muslim extremists who are inspired by Al Qaeda but working alone? *The Week*, retrieved from <http://theweek.com/article/index/244633/londons-gruesome-attack-and-the-rising-threat-of-lone-wolf-terrorism>.
- McCauley, C., Moskaleiko, S., & Van Son, B. (2013). Characteristics of lone-wolf violent offenders: A comparison of assassins and school attackers. *Perspectives on Terrorism*, 7(1), 4-24.
- McGraw, G. (2013). Cyber war is inevitable (Unless we build security in). *The Journal of Strategic Studies*, 36 (1), 109-119.
- Messenger, C. (2011). *Anders Breivik: His life and mission*. Raleigh, NC: Lulu Press.
- Michael, G. (2012). Leaderless resistance: The new face of terrorism. *Defense Studies*, 12 (2), p. 257-282.
- Michel, L. & Herbeck, D. (2001). *American terrorist: Timothy McVeigh and the Oklahoma City bombing*. New York, NY: HarperCollins Publishers.
- Mills, E. (2011). AntiSec hackers post stolen police data as revenge for arrests. *CBS interactive*, retrieved from <http://www.webcitation.org/60jwqabgh>
- Monsky, A. (2000). *Mugshots: Eric Rudolph*. United States: TruTV

- Moskalenko, S., & McCauley, C. (2011). The psychology of lone-wolf terrorism. *Counseling Psychology Quarterly*, 24 (2), p. 115-126.
- Moss, J. A. (2013). Enhancing the brave new world of cyber liabilities and insurance coverage. *Brief*, 42 (3), 28-35.
- Mueller, R. S. (2012). Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies. *Federal Bureau of Investigation Speeches*, retrieved from <http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>
- Nijboer, M. (2012). A review of lone wolf terrorism: The need for a different approach. *Social Cosmos*, 3 (1), p. 33-39.
- Nikitina, S. (2012). Hackers as tricksters of the digital age: Creativity in hacker culture. *Journal of Popular Culture*, 45 (1), 133-152.
- Orange, R. (2012, October 7). Anders Behring Breivik's mother 'sexualised' him when he was four. *The Telegraph*, retrieved from <http://www.telegraph.co.uk/news/worldnews/europe/norway/9592433/Anders-Behring-Breiviks-mother-sexualised-him-when-he-was-four.html>
- Penny, L. (2011). Rise of the digital natives. *Nation*, 293 (18), 20-22.
- Perlmutter, D. (2013). Prelude to the Boston Bombings. *Middle East Quarterly*, 20 (4), 67-77.
- Perlroth, N. (2013, January 30). Hackers in China attacked the times for last 4 months. *The New York Times*, retrieved from http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0
- Pidd, H. (2012, August 24). Anders Behring Breivik spent years training and plotting for massacre. *The Guardian*, retrieved from <http://www.theguardian.com/world/2012/aug/24/anders-behring-breivik-profile-oslo>
- Piggin, R. (2010). The reality of cyber terrorism. *Engineering and Technology*, 5 (17), p. 36-38.
- Post, J. M., Ali, F., Henderson, S. W., Shanfield, S., Victoroff, J., & Weine, S. (2009). The Psychology of Suicide Terrorism. *Psychiatry: Interpersonal & Biological Processes*, 72 (1), 13-31.
- Post, J. M., McGinnis, C., & Moody, M. (2014). The changing face of terrorism in the 21st century: The communications revolution and the virtual community of hatred. *Behavioral Sciences and the Law*, 32, 306-334.
- Post, J. M., Sprinzak, E. & Denny, L. M. (2003). The Terrorists in Their Own Words: Interviews with 35 Incarcerated Middle Eastern Terrorists. *Terrorism and Political Violence*, 15 (1), 171-184.

Prasad, K. (2012). Cyberterrorism: Addressing the Challenges for Establishing an International

Legal Framework. *Edith Cowan University Research Online*, retrieved from <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act&sei-redir=1&referer=http%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3Dcyberterrorism%253A%2520addressing%2520the%2520challenges%26source%3Dweb%26cd%3D1%26ved%3D0CC8QFjAA%26url%3Dhttp%253A%252F%252Fro.ecu.edu.au%252Fcgi%252Fviewcontent.cgi%253Farticle%253D1016%2526context%253Dact%26ei%3DwaT8UZGIGMPmyQHj94GoDA%26usg%3DAFQjCNEa1cq5O4qiCXKBd0xqKDvgYLC00g%26bvm%3Dbv.50165853%2Cd.aWc#search=%22cyberterrorism%3A%20addressing%20challenges%22>

Preimesberger, C. (2008). Innovation drives security. *eWeek*, 25(8), 22-24.

Pressman, J. (2003). Leaderless Resistance: The Next Threat? *Current History*, 102 (668), p. 422-425.

Rabinovich, I. & Reinharz, J. (2008). *Israel in the Middle East: Documents and readings on society, politics and foreign relations, pre-1948 to the present*. Lebanon, NH: University Press of New England.

Reitman, J. (2012, August 11). Enemy of the state. *Rollingstone*, 1169, 52-62.

Reitman, J. (2013, August 1). Jahar's world. *Rolling Stone*, 1188, 46-57.

Rothman, P. (2012, September 28). Cyber terror rages in the banking sector. *Security Info Watch*, retrieved from <http://www.securityinfowatch.com/blog/10796084/cyber-terror-rages-in-the-banking-sector>.

Saporito, B. (2011, July 4). Hack Attack. *Time*, 178 (1), 50-55.

Simon, J. D. (2013). *Lone wolf terrorism: Understanding the growing threat*. Amherst, NY: Prometheus Books.

Smith, B. L. & Damphousse, K. R. (2002). American terrorism study: Patterns of behavior, investigation and prosecution of American terrorists, final report. *National Institute of Justice*, retrieved from <https://www.ncjrs.gov/pdffiles1/nij/grants/193420.pdf>.

Spaaij, R. (2010). The enigma of lone wolf terrorism: An assessment. *Studies in Conflict & Terrorism*, 33 (9), p. 854-870.

Tafoya, W. I. (2011). Cyber terror. *FBI Law Enforcement Bulletin*, 80 (11), p. 1-7.

Taylor, P. A. (2005). From hackers to hacktivists: Speed bumps on the global superhighway? *New Media Society*, 7 (5), 625-646.

Taylor, R., Fritsch, E., Liederbach, J., & Holt, T., (2011). *Digital crime and digital terrorism* (2nd ed). Upper Saddle River, N.J.: Prentice Hall.

- Thaanum, J. D. (2013). Threats to cyber security: The dangers of malicious mobile code, users, and the iphone. *Journal of Applied Security Research*, 8 (4), 490-509.
- Thompson, M. (2013, February, 27). The danger of the lone-wolf terrorist. *Time Magazine*, retrieved from <http://nation.time.com/2013/02/27/the-danger-of-the-lone-wolf-terrorist/>.
- Tsfati, Y., & Weimann, G. (2011). www.terrorism.com: Terror on the Internet. *Studies in Conflict & Terrorism*, 25 (5), p. 317-332.
- Vamosi, R. (2011). How hacktivism affects us all. *PCWorld*, 29 (11), 37-38.
- Vollers, M. (2007). *Lone wolf: Eric Rudolph and the legacy of American terror*. New York, NY: Harper Perennial.
- Wagner, B. (2007). Electronic jihad: Experts downplay imminent threat of cyberterrorism. *National Defense*, 92 (644), p. 34-36.
- Weimann, G. (2012). Lone wolves in cyberspace. *Journal of Terrorism Research*, 3 (2), retrieved from <http://ois.st-andrews.ac.uk/index.php/jtr/article/view/405/431>.
- Weimann, G. (2011). Cyber-fatwas and terrorism. *Studies in Conflict & Terrorism*, 34 (10), p. 765-781.
- Weimann, G. (2004). Cyberterrorism: How real is the threat? *United States Institute of Peace*, retrieved from <http://www.usip.org/sites/default/files/sr119.pdf>.
- Welner, M. (2001). The cult of Al Qaeda? *Forensic Panel Letter*, 5 (10), p. 1-2.
- White, J. R. (2003). *Terrorism: An introduction*. (4th ed.). Belmont, CA: Wadsworth Thomson Learning.
- Williams, M (2012, October 12). Future Cyber Attacks Could Rival 9-11, Cripple US, Warns Panetta. *Computerworld*, retrieved from http://www.computerworld.com/s/article/9232317/Future_cyber_attacks_could_rival_9_11_cripple_US_warns_Panetta
- Wines, M. & Lovett, I. (2013, May 4). The dark side, carefully masked. *The New York Times*, retrieved from http://www.nytimes.com/2013/05/05/us/dzhokhar-tsarnaevs-dark-side-carefully-masked.html?pagewanted=all&_r=0
- Woods, M. J. & Spaulding, S. (2005). Part one provisions expiring in 2005: Intercepting lone wolf terrorists. *Patriot Debates: Experts Debate the USA Patriot Act*, p. 81-92.
- Wyatt, K. (2005, April 14). Eric Rudolph, proud killer. *The Decatur Daily News*, retrieved from <http://legacy.decaturdaily.com/decaturdaily/news/050414/rudolph.shtml>
- Zeff, L. (1997, July 8). *Timothy McVeigh: Soldier of terror*. United States: Biography Channel.