ABSTRACT

The Internet as a Tool for Terrorism

Shawn Douglas Miller

Director: Timothy Kayworth

This paper analysis the usage of the internet for terrorist campaigns. It begins with an analysis of the ways that terrorists are – and potentially could – use the internet such as cyber warfare, information warfare, and social media-spread propaganda. It then looks at the reasons that explain why terrorists would want to use the internet. It shows that there is more value than risk for terrorist groups that choose to use the internet for various reasons. The paper then analyzes the response to this threat by looking at legal response from the United States as well as various non-governmental response. Finally the paper concludes with policy recommendations that include further research and education as well as privatizing cyber security.

APPROVED BY DIRECTOR OF HONORS THESIS:

_____

Dr. Timothy Kayworth, Department Chair of Information Systems

APPROVED BY THE HONORS PROGRAM

_____

Dr. Elizabeth Corey, Director

DATE: Fall 2015

THE INTERNET AS A TOOL FOR TERRORISM

A Thesis Submitted to the Faculty of

Baylor University

In Partial Fulfillment of the Requirements for the

Honors Program

By

Shawn Douglas Miller

Waco, Texas

December 2015

TABLE OF CONTENTS

Chapter One: How Terrorists are using the Internet 1

1.1 General introduction 1

1.2 Introduction to theories and models 3

1.3 Introduction to the ways internet is used by terrorists . . 9

Chapter Two: Benefits of the Internet for Terrorist Insurgency . . 19

2.1 Denial of service 21

2.2 Information gathering 26

2.3 Using the internet to command, control, and convert . . 30

2.4 Directly using the internet as a weapon 38

Chapter Three: Responses to the Emerging Cyber Threat . . . 45

3.1 Net neutrality and internet regulation 46

3.2 Legality of mass surveillance 52

3.3 Cybersecurity initiatives 56

3.4 Non-governmental responses 60

Chapter Four: Conclusion and Policy Recommendations . . . 65

4.1 Increase cybersecurity education initiatives . . . 66

4.2 Focus on private industry 67

4.3 Multilateral discussion and establishing international norms . 69

4.4 Conclusion 71

Bibliography 73

CHAPTER ONE

How Terrorist are using the Internet

1.1 *General introduction*

The purpose of this paper is to analyze the ways in which the internet can be used as a tool for terrorism and the responses available to this emerging threat. Terrorism is a global threat that shows no sign of abating. Terrorists have historically adapted to technological advancements in order to maximize their effectiveness in cases of asymmetrical warfare. The internet has become nearly synonymous with the modern world. As the internet spreads to even the most remote areas terrorists may begin experimenting with ways of using the internet to further their own goals. This has already begun to some degree as terrorists are turning towards social media to spread propaganda and recruitment but this is only the beginning. There are countless ways the internet can be used as a valuable tool for terrorists and this paper aims to analyze a few of them in order to get a better understanding of the threat the internet poses. Various responses to

current cyber security threats will be analyzed in order to provide context to how the terrorist threat may be dealt with.

Chapter 1 will introduce some models used to understand terrorist insurgency operating within the cyber domain. This chapter will also delve into the various ways terrorists can use the internet and the related threats these actions cause. Next chapter 2 will discuss the reasons why terrorists are attracted to the internet. A focus on cost-benefit analysis are used to determine how attractive the internet is as a tool for terrorist groups. Chapter 3 introduces some of the responses of the US government to the growing cyber threat. This chapter will also discuss private cyber security initiatives and the responses of other non-state groups to the growing threat of malicious actors in cyberspace. When US policy is not clearly stated the information will be extrapolated based on previous actions taken by the US military and counter-terrorism agencies. International and non-state responses will also be used to show solutions other than the ones chosen by the United States. Finally, chapter 4 will conclude with policy recommendations based on the findings in the preceding sections. A focus on using early-education to teach cyber security, allowing private industry to self-regulate the internet, and using multilateral engagement to build cyber security infrastructure will be the focus of these recommendations.

The overarching goal of this paper is to establish a shallow but broad understanding of how modern terrorists groups are integrating the internet into their actions. To do this, a cross-disciplinary approach to analysis will be used that unites theories from political science, information systems, and computer science to help explain why and how the internet is such an attractive tool for terrorists. The terrorist

groups that will be referenced are primarily Islamic State (ISIS/ISIL) and Al Qaeda and its affiliates. The United States of America will be the primary target for analysis of counter-terrorism strategies that affect the issues presented here. As often as possible real-world examples will be used to illustrate points but this may not be possible for every example. The paper will culminate into policy recommendations based on what is discovered about terrorists using the internet. Potential areas of future research will also be highlighted throughout the paper.

1.2 *Introduction to theories and models*

There is no universally accepted definition for terrorism. For any paper dealing with terrorism it is necessary to first establish what exactly terrorism is in the context of the paper and with this paper cyber terrorism must also be defined. Terrorism, as it will be referred to here, is the use of violence by non-state actors in order to intimidate or coerce and further sociopolitical goals. This definition is functionally similar to the US State Department officially recognized definition of terrorism.[1] Cyber terrorism, then, is the use of networked devices in order to intimidate or coerce and further sociopolitical goals. Cyber terrorists have the advantage of using traditional terrorist strategies without much change in the cyber domain. Terrorism typically involves asymmetrical warfare

[1] U.S. Department of State. "Foreign Terrorist Organizations." Bureau of Counterterrorism.Last modified September 30, 2015. Accessed November 16, 2015.http://www.state.gov/j/ct/rls/other/des/123085.htm

that often employs guerilla tactics to disrupt an enemy. Especially for weak terrorist groups, there is often a focus on a war of attrition rather than outright victories of overt displays of might. This translate perfectly to the cyber domain because it is very difficult to do lasting damage. Most cyber-attacks involve disruption rather than destruction so attrition is an integral part of a cyber campaign.

A common understanding of terrorism is that it comes in waves. David Rapoport created a model to explain that terrorism has always been around but it occurs in waves so people tend to overlook it until it resurges.[2] The current wave of religious terrorism is the fourth wave in this model and is a fairly recent development. Many see this latest wave of terrorism as unpredictable but according to Rapoport this isn't true. He says you cannot truly eliminate terrorism but instead a wave will naturally die out and another one will take its place sometime in the future. Waves are related in their usage of violence to pursue political goals but in many other ways they are different. They have different goals, different geographical locations, and different tools. The first wave, for example, occurred at the end of the 19th century and the beginning of the 20th century. This wave of terrorism was anarchic and relied on targeted assassination of political leaders to destabilize governments. Modern Islamic extremist rarely engage in leadership targeting and instead engage in attacks on military and civilian targets that allow them to gain popular support. Modern day terrorist also have access to many new techniques of terrorism like suicide bombing and guerilla warfare. These tactics did not exist for earlier terrorists but today they are an inherent part of any terrorist insurgency.

[2] Rapoport, David C. "The four waves of modern terrorism." *Attacking terrorism: Elements of a grand strategy*, edited by Audrey Kurth Cronlin. 47-73. Washington D.C.: Georgetown University Press, 2004.

The point to be made is that even if the United States' war of terror is successful and ends the current trend of Islamic extremist terrorism, there will be a future wave with differing political ambitions, according to the Waves of Terrorism Model.. This new group will naturally use the most up-to-date technology and tactics available just as modern day terrorists do. This means that as the internet's function expands so too does the risk of supplying future terrorists with new tools to engage in violence. This is all purely hypothetical but it is important to identify threats early so if they do come to pass there is already a plan in place. One of the reasons the September 11 attack was so devastating was because the United States government did not expect something like that to occur. Even the current wave of terrorist groups are turning towards the internet and new technologies to facilitate their plans so this is not a purely hypothetical exercise but rather one of current circumstance.

Another important model that is useful in understanding this topic is the security dilemma and the offense-defense balance. The security dilemma is an international relations theory that describes the international system as being in anarchy.[3] Because there is no ruling power, each state feels that it is on its own and all other states are threats to its existence. This understanding of the international system explains why multilateral cooperation is so difficult to achieve: there is no power that can enforce nations to follow agreements. There needs to be trust for the international system to operate and trust is difficult to achieve when the opposing side potentially has the capability to destroy you and you have nothing to stop them but your own defenses. This

[3] Jervis, Robert. "Cooperation under the security dilemma." *World Politics* 30, no. 02 (1978): 167-214

idea extends to the cyber domain because there is no regulatory body or supreme power that has oversight over the internet. The security dilemma is even more apt in terms of cyberspace because states cannot exert their sovereignty onto the internet because it is multinational and largely owned by private corporations. This leads to states not wanting to cooperate on cyber issues and makes it difficult to deal with terrorist who can effectively operate in conditions of anarchy with little effect on their actions.

The offense-defense balance is an analysis of whether technology is better suited for attacking or defending. Glaser and Kaufman define the offense-defense balance as a ratio of cost to defend vs. cost to take territory.[4] This theory can be understood in terms of physically capturing land and defending land but in the case of the cyber domain the concept is a little different. For the cyber offense-defense balance it is best to understand offense as the ability to breach cyber defenses and gain access to private information or services. Cyber security is already well defined as protecting a database or internet service from intrusion so that is the cost of defense in the theory. Anyone with any experience with cyber security can tell you that it is a lot more difficult and expensive, both in terms of time and money, to defend a system. There are a myriad of ways to gain access to an electronic system from brute force attacks to phishing scams to social engineering. If the goal is merely to disrupt the system there are even more ways like Distributed Denial of Service (DDoS) attacks which are easy to use and almost impossible to trace. Under this theory, a state will only attack if the system is strongly in favor of offense, so much so that it would be irreparably costly not to attack.

[4] Glaser, Charles L, and Chaim Kaufmann. "What is the offense-defense balance and how can we measure it?." *International Security* 22, no. 4 (1998): 44-82

Because many modern states are so reliant on the internet for communication and infrastructure, it is very expensive to openly engage in cyber-attacks. If the United States, for example, were to launch a cyber-attack on China out of fear that China is growing too powerful they must completely destroy China's ability to counterattack or risk getting attacked themselves. Cyber-attacks, as already mentioned, are more denial than destruction so this idea prevents states from openly engaging in largescale cyber-attacks against each other. The internet is very much an offense-dominant technology in terms of the offense-defense balance but states are still restricted from attacking because of the nature of the cyber domain. To use cyber warfare a state would have to also use a physical force to destroy the opponent's infrastructure which increases the cost of offense in this case and causes the offense-defense balance to favor defense more so than is readily apparent in terms of the cyber domain. This pushes states to prefer cyber espionage over more open aggression in cyber space. Terrorists themselves do not have as much risk of being counterattacked so they can utilize the internet offensively without much risk of repercussion.

Many policy makers, particularly in the US, have seen the international system in terms of the security dilemma and the offense-defense balance for so long that they have difficulty analyzing the cyber domain. Since the Cold War the prevailing idea of security has been based around deterrence and defense but the offense-dominant cyberwar does not seem suited to this type of thinking. States also have difficulty establishing global norms for operation in cyberspace because of the security dilemma preventing collaboration. The lack of cyberspace norms make it even more difficult to fully understand the role of states in cyberspace. Policy makers rely on inefficient, Cold War

era deterrence strategy in cyberspace because they are unable to completely understand their role in cyber space. Relying on deterrence leaves states vulnerable to terrorist who are not being affected by this state-focused deterrence and instead merely want to cause destruction at any cost.

The increasing reliance on the internet for infrastructure and planning as well as new weapons – like drones – shows that the internet has been increasingly integrated into the military at a very high level. Being offense dominant means that these new tools are best used in aggressive campaigns but since the Cold War the international system has been very defense focused. The defense-dominant system is possibly one reason for the seemingly slow adoption rate of new cyber warfare technologies and strategies by the military. This norm of not making the first move lowers the effectiveness of these new tools as they are best suited for first-strikes and other aggressive tactics. Terrorists have access to many of the same tools due to the open source nature of the internet. Terrorists are also typically much more aggressive with their use of violence. Terrorist groups can use the internet for preemptive strikes against enemies without fear of reprisal because of the difficulty that arises from tracking cyber-attacks. Terrorists don't have a real presence in the cyber domain because they don't host servers, large databases of information or complex services for their operatives like a traditional state does. Terrorist piggy-back off of other services to use the internet so they don't have to worry about defense. This allows terrorists to have all of the power of cyber capability without any of its weaknesses. The offense-defense balance for the cyber domain only applies to states because terrorists don't have to balance defense. The way terrorists use the internet as a defensive resource is very reminiscent of the classical guerrilla warfare technique of

hiding among the populace. It is difficult to discover the individuals who plan to engage in violence and taking action against them often results in collateral damage that may damage the regime's legitimacy.

1.3 *Introduction to the ways internet is used by terrorists*

1.3.1 *Cyber warfare*

The most obvious use of the internet by terrorist is to launch cyber-attacks. Cyber warfare is a rapidly expanding field of study because many fear its dangers as the modern world grows increasingly dependent on technology. Cyber warfare is valuable in asymmetrical situations like terrorist insurgencies because it has a fairly low barrier to entry and doesn't require a lot of manpower to operate effectively. A defending force has to protect themselves against every possible method of intrusion, of which there could be hundreds. An attacker only needs to find one entrance into the system. This means that a single individual could potentially access a system that is being defended by an entire security team. In cyber conflicts the number of members is less relevant than the technical ability of each force. Another aspect of cyber warfare is that has already been mentioned is that it is disruptive rather than destructive. The nature of the internet and technology in general is that it is easy to repair so effective cyber warfare campaigns are

typically hybrid attacks that include a physical element as well.[5] An example of this in practice is the military action of Israel to shut down the Syrian air defense network so that Israeli bombers could destroy Syrian nuclear facilities without fear of reprisal. An example of a cyber-attack accomplishing physical damage by itself is the Stuxnet virus that infected Iran's nuclear centrifuges and caused them to spin out of control and damage themselves.[6] The Stuxnet virus seems to be more of an anomaly than a prediction of future cyber campaigns so this paper will work under the assumption that cyber warfare does not require physical destruction or violence in order to be considered effective.

The largest targets of cyber-attacks are the most technologically advanced countries like the United States. This causes an inherent problem because the nations that are most vulnerable in the cyber domain typically have the strongest physical force to defend themselves which negates some of their cyber weakness. Terrorist groups cannot typically engage in open warfare against an opposing power so they have to engage in asymmetrical war like guerrilla warfare. Using the internet to abuse IT infrastructure and cause disruptions is another potential way terrorists could use to engage a larger and well-equipped force. An insurgency typically starts by disrupting those in power while strengthening themselves until they can engage in more traditional warfare. In this case, cyber-attacks become a valuable weapon for newly formed groups trying to disrupt the government from prematurely destroying the terrorist insurgency. Cyber warfare can be

[5] Gartzke, Erik. "The myth of cyberwar: bringing war in cyberspace back down to Earth." *International Security* 38, no. 2 (2013): 41-73

[6] Collins, Sean, and Stephen McCombie. "Stuxnet: the emergence of a new cyber weapon and its implications." *Journal of Policing, Intelligence and Counter Terrorism* 7, no. 1 (2012): 80-91.

used to harm the legitimacy of a state by interrupting infrastructure and causing the local people to lose faith in the government's ability to properly control the area. This is a classic way to gain recruits for an insurgency and cyber-attacks are ideally suited for this as they have a low cost and are difficult to trace. Perhaps in the future the definition of cyber warfare will expand to include this type of aggression that does not lead to physical destruction. For now it seems the prevailing opinion among scholars is that cyber warfare must cause long-term destruction which currently means a physical force to complement a cyber-attack is necessary.

1.3.2 *Cyberplanning*

Another way terrorists can use the internet is to engage in "cyberplanning."[7] Cyberplanning refers to using the internet as a command and control tool by terrorist leaders. The internet provides an easily accessible way to disseminate operation plans, training manuals, and ideological propaganda with very little risk. Access to the internet is so widespread that it is easy for a terrorist operative to get materials by simply logging in to a specialized web service that allows them to communicate with their leadership. A leader can monitor and control many terrorist cells at the same time and engage in more complicated schemes. Another possibility is a number of smaller cells staying in loose communication via the internet but operating in relative isolation. Leaders can exchange advice and general plans so that the group stays cohesive without being overly hierarchical. A hierarchical terrorist group is much more susceptible to traditional

[7] Thomas, Timothy L. *Al Qaeda and the Internet: The Danger of 'Cyberplanning'*. Fort Leavenworth: Foreign Military Studies Office (ARMY) (2003).

counter-terrorism techniques like decapitation. Decentralized terrorist cells are difficult to completely destroy because even if one cell is eliminated there are many others that are unaffected. The internet supports this because cells don't have to be in physical communication to work together. This makes it difficult for law enforcement to track and link terrorist cells. Relying on the internet for communication also makes it more difficult for law enforcement to track decentralized terrorist cells because the internet has so many tools to ensure that a message is not intercepted. There are built in tools for encryption, anonymous services like the Tor networks that make IP address tracking irrelevant, and ways to quickly wipe hard drives of information if necessary. All of these protections build trust in internet as a form of communication among terrorist cells and make it more attractive as a tool that can be adopted with little cost associated with it.

Cyberplanning is difficult to prevent because the internet is being increasingly seen as a fundamental right among developed nations.[8] Furthermore the internet is difficult to regulate because it is trans-national and largely free of government control. A very large social movement in the United States and the European Union is opposing any government regulation that attempts to limit what users can do on the internet. An example of a proposed internet censorship bill that has already failed in the US is the Stop Online Piracy Act (SOPA). Although the bill attempts to primarily prevent illegal activities there was a very negative backlash among US citizens who saw this as the first step in the government taking away their freedom to use the internet. Terrorists are able

[8] La Rue, Frank. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" Paper presented at the United Nations General Assembly Human Rights Council, 17th session. London, United Kingdom. May 16, 2011. (Document A/HRC/17/27)

to use the internet to make their plans because there is no real regulatory body that can monitor, catch, or prevent them from doing so. Internet Service Providers (ISPs) have even been found to unknowingly host pro-terrorist websites that facilitate cyberplanning.[9] When discovered, the ISP would suspend the website but the group would just create another website with the same function by hosting it from a different physical location. Because physical location is completely irrelevant to cyberplanning the terrorist groups can chose a host that is either ineffective at monitoring how their service is being used or a host that does not care how their service is being used. Then members of the terrorist group, or anyone else for that matter, can log on to that website from anywhere in the world. Even if hosting a pro-terrorism website in the US is difficult it does not stop people in the US from accessing such a website.

1.3.3 *Information Warfare*

Yet another way terrorist can use the internet is to spread propaganda and increase recruitment. This is the way that modern terrorist groups like Al-Qaeda and ISIS have become so successful. They rely on social media to spread the word of their deeds so that everyone can see any success they have. They can spread their message to every corner of the world with the internet and gain recruits from widespread areas without having to physically go there. Al-Qaeda publishes a magazine called Inspire online to keep members caught up with recent developments as well as encourage people to join.[10] In

[9] Thomas *Al Qaeda and the Internet: the Danger of Cyberplanning*

[10] Zelin, Aaron Y. "al-Malāḥim Media presents a new issue of al-Qā'idah in the Arabian Peninsula's magazine: 'Inspire #14'." *Jihadology*. Last modified September 9, 2015. Accessed November 16, 2015. http://jihadology.net/category/inspire-magazine/

issue #14 of Inspire magazine there is an article called "Open Source Jihad" which describes a manual distributed electronically that allows Muslims to "train at home rather than risking a dangerous travel abroad."[11] This is the exact danger that internet-savvy terrorist pose: widespread dissemination of dangerous information with malicious purpose. ISIS uses Twitter to spread ideological messages that reach far and wide through retweeting and other built-in social media sharing features. ISIS also posts videos online to spread their message, including several graphic videos of executions. Social media is designed to link people together and make it easy to use and terrorist groups are abusing these factors to spread propaganda and create loose networks of individuals interested in terrorism.

It is very difficult to prevent terrorist from using social media because of the nature of the social media itself. First, many social media websites are very pro-freedom and speech and do no engage in censorship unless absolutely necessary. Terrorists can use this to their benefit by keeping their message broad enough that it does not directly violate any end user agreements on the given form of social media. Furthermore, even if an account is suspended by the administrators of a social media website, it only takes a few short minutes for a terrorist to make a new account and repost the same material. In fact, a very simple script can be written to make tens and hundreds of account from which to post the terrorist group-approved messages without any user input necessary. Another inherent aspect of social media tools that make them such valuable propaganda tools is that they support information and articles going "viral". Going viral refers to a

---

[11] al-A'siri, Ibrahim ibn Hassan. "Charlie Hebdo: Military Analysis." *Inspire Magazine: Assassination Operations*, issue 14: 38-42. Summer 2015.

piece of information – a video, a news article, a picture, or anything else – being spread quickly across social media websites via crowdsource distribution. By using Twitter a terrorist can post an ideological message from the leader of that group. Then everyone who follows that twitter account can retweet the message, then follows or those accounts retweet the message also. The message is spread very quickly due to the willing participation of hundreds of individuals linked to this terrorist group via social media. The message reaches a much larger audience than it would have without social media and there was not a particularly noticeable increase in manpower required to accomplish this.

Terrorists can also use the internet to obtain intelligence on enemies via social media and personal websites. Social media can occasionally lead to lapses in judgments that an intelligent data miner can turn into actionable intelligence. An example of this happen, albeit against terrorist and not for, is in mid-2015 when the US Air Force reportedly found an ISIS stronghold because of an ISIS member posting a 'selfie' online.[12] The picture allowed USAF officials to identify the location of the stronghold and promptly destroyed the structure with a drone strike. Terrorists can do similar things if they patrol social media and find dissidents within the geographical areas upon which they operate. This allows terrorists to use targeted violence against people they know are enemies and reduces the risk of turning the local population against them because they have the social media as evidence of wrongdoing. Actions like this considers only the lawful application of social media to obtain information and locations. Terrorists can also

[12] Ernst, Douglas. "Terrorist 'moron' reveals ISIS HQ in online selfie; U.S. Air Force promptly destroys compound." *The Washington Times*, June 4, 2015. Accessed November 16, 2015.

use widely available software to listen in on unsecured Wi-Fi signals and use others means of getting information that people may not plan to make public.

1.3.4 *Funding and Support*

The final way terrorists can use the internet is to secure funding. Attacking funding is a very traditional and effective counter-terrorism measure as many groups have difficulty getting money. Traditionally the most successful groups have either very wealthy benefactors that donate money for their causes or access to a valuable natural resource like oil or narcotics. In fact, many terrorist insurgencies are started because of the perception that they can gain funding by capturing local areas with the natural resources. ISIS, for example, captured oil fields within Syria very early on in its campaign to establish a physical state that it controls.[13] Since being captured, the oil from these fields has been sold on the black market to fund ISIS's violence in the region. By using the internet, a widely available commodity, terrorist groups can reduce their reliance on natural resources as a necessary precursor for insurgency.

Besides the usage of natural resources, many terrorist groups are financed by charities and fund raisers.[14] Some of these charities are hoaxes intended to scam money out of innocent people and others are open about their intention and aimed at potential supporters of the insurgency. The internet allows these kinds of charities to be spread

---

[13] Mroue, Bassem. "Here's A Breakdown Of The Oil Assets ISIS Now Controls." *Business Insider: Military & Defense*, September 25, 2015. Accessed November 16, 2015.

[14] Kaplan, Eben. "Tracking Down Terrorist Financing." *Council on Foreign Relations*, April 4, 2006. Accessed November 16, 2015. http://www.cfr.org/terrorist-financing/tracking-down-terrorist-financing/p10356

globally very easily and allows crowdsourcing of financing. The internet's role in the financial world is growing with the advent of electronic currency like bitcoin so it is natural for terrorist groups to turn towards the internet for their financial needs. Those who wish to support terrorist groups can do so anonymously through a resource like bitcoin or via another online payment service that hides identity. Besides crowdsourcing, the internet also allows terrorist groups to research the interests of wealthy individuals and then contact them. Armed with information obtained from the internet, a terrorist operative is much more likely to convince wealthy individuals to help fund their operations.

The internet can also be used to obtain information via hacking or other online scams that can be sold on the black market for high prices. US businesses are victims of stolen data via internet intrusions thousands a times a year, showing that a vulnerability has already been established. Terrorists groups can research these vulnerabilities, which are well reported within the news, to find likely targets to focus on. They can steal valuable information on products to sell or even potentially gain direct access to financial information of the company and its employees. The internet adds many robust options for terrorists to potentially gain funding which has previously not been possible. This lowers the cost of engaging in terrorist activities and makes violence a more appealing option for groups who want to change the political system.

These are a few of the ways that terrorists can use the internet to improve their operational efficiency. Whether it's disrupting an enemy government or spreading propaganda far and wide the internet is a resource that is perfectly positioned for terrorists to take advantage of. As computer literacy grows and internet coverage both

spreads and improves, it becomes easier and easier for individuals with malicious intent to discover effective ways to leverage this technology. There is also the danger of new technology emerging that opens up new vulnerabilities for society that we aren't even capable of considering at this point. Technology advances forwards in leaps and bounds but governments are often too constricted by bureaucracy to respond quickly enough. Terrorist groups tend to be relatively small and have simpler structures so they are well-positioned to integrate new technology into their organization. There needs to be a concentrated effort to both predict the dangers of technology and invent ways of find ways to eliminate this threat. While improving cybersecurity infrastructure we must also consider the balance between security and personal liberties. There needs to be a reasonable trade-off between security and liberty and the sooner this trade-off is decided upon and implemented the sooner developed governments can begin properly protecting their people against the next wave of terrorism.

CHAPTER TWO:

Benefits of the Internet for Terrorist Insurgency

Having described how modern terrorists are using the internet the paper will now attempt to discern why terrorists are using the internet. Various weaknesses and strengths of the internet as a tool for insurgency will be considered and compared to more traditional tools. This should provide an understanding of why terrorists are using the internet which is important if we are to predict not only the ways terrorists can use the internet but the extent to which they may come to rely on it. It may also allow an educated guess as to whether terroristic activity will continue in cyberspace or whether it is merely a short trend based on how beneficial cyber terrorist activity is when compared to the ways terrorists have historically engaged in insurgency. This evaluation is based on the cost-benefit relationship of cyber terrorism and assumes terrorist organizations are rational actors.

The purpose of this chapter is to help answer the question of why terrorists would want to use the internet as a tool for their actions. The first chapter demonstrated that there is a lot of potential for terrorist groups to utilize the internet but this does not

necessarily mean that they will. What determines the likelihood of terrorist usage of the internet is how valuable cyber activity is as opposed to alternative physical action. If a terrorist group feels that the internet provides more value than risk for their operations then naturally they will be more likely to use it. It is presumed that terrorist organizations considered here have internet access and technical knowledge or the ability to gain technical knowledge of how the internet can be used for their purposes. There is also an assumption that terrorists will most likely use a hybrid of traditional tactics as well as new cyber tactics to organize and engage in terrorism. There is no way to know how integrated the internet will be in any terrorist group but there should be some level of technology usage among most groups. Terrorist groups may adapt any number of cyber activities mention in the first section or they may use the internet in completely unexpected ways. The goal of this section is not to definitively predict how terrorists will – or will not – use the internet but rather predict some of the arguments that they might consider when deciding whether or not to use the internet in general.

Each section will be focused on a main idea that is pertinent to whether or not terrorists would want to adopt the usage of the internet into their organization. The sections involve internet access, information gathering, internet communication, and finally cyber-attacks. This analysis is not an exhaustive analysis of all the reasons terrorist may or may not want to rely on the internet. Instead these section hit some key ideas that all terrorist insurgencies must consider when they are operating. These ideas will also hopefully shed some light on further research topics that may be undertaken to get a better understanding of the interest among terrorist groups in entering the cyber domain.

2.1 *Denial of service*

The internet has been increasingly seen as a fundamental human right that all people should have access to in order to properly ensure freedom of expression in the modern age. There have been a number of states as well as large international organizations that have declared internet access a human right. The most notable of these groups is the UN who declared the internet as a basic human right in 2011[1] There is also been a number of grassroots movement whose goals are to spread internet to everyone and help establish internet access as a fundamental right in the modern age. One of these movements, known as A Human Right (ahumanright.org), has engaged in a number of advocacy projects including successfully petitioned to move the South Atlantic Express Cable in order to connect previously isolated islands to the modern world via the internet.[2] Facebook and Google have also both outline plans to provide proprietary internet connections to developing nations by using autonomous drones as an intermediary between internet-providing satellites and end users.[3] This would allow much more reliable internet connections in developing nations with poor infrastructure that may not support overland cables. The areas without strong infrastructure are often hotbeds for violence and terrorism so this shows there are initiatives that could supply even remote

[1] La Rue, Frank. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" Paper presented at the United Nations General Assembly Human Rights Council, 17th session. London, United Kingdom. May 16, 2011. (Document A/HRC/17/27)

[2] A Human Right. "Projects." *A Human Right*, last modified 2015. Accessed November 16, 2015. http://ahumanright.org/projects.php

[3] Zuckerberg, Mark. Facebook post. March 27, 2014, accessed November 16, 2015. https://www.facebook.com/zuck/posts/10101322049893211

terrorist groups with internet access. The availability of internet may currently be the biggest barrier of entry into the cyber domain for some groups. This issue is already being addressed by in various ways so it is unlikely to continue being a barrier in the near future.

Many modern terrorists groups have been turning increasingly towards the internet as a tool to engage in a variety of acts from recruitment to information gathering. As has been previously discussed there are numerous ways for terrorists to use the internet to support its actions. The internet also gives terrorist insurgencies new weaknesses that they would not have to account for otherwise. One of these weaknesses is the most obvious: a reliance on internet access. If a terrorist group tries to occupy a particular physical location, like in the case of ISIS, it is possible to remove their ability to access the internet. If the group is very reliant on the internet for day-to-day operations then this opens new possibilities for counter terrorism options like denial of service. Terrorist organization typically don't have to consider the danger of cyber-attacks because they are hidden in the shadows of the cyber world and don't have any easily visible internet services that can be either identified or attacked whereas states do have all of these weaknesses. There are some cases – like ISIS for example – that can be targeted because they occupy a relatively large and very well defined geographical area. Groups that hold physical territory like in this way can have their internet access disrupted by simple removing internet access for the entire area. This can be accomplished with DDoS attacks that disrupt internet connections with the area. Internet access can also be removed by working with local ISPs but there are no laws in place to enforce cooperation so actually turning off the internet would be up to the individual ISPs. This is a danger for

terrorist groups that have a high level of reliance on technology and also expect to exert control over physical areas.

The tactic of entirely removing internet access in an area may backfire as it prevents people within the disputed area from being able to contact anyone outside. It makes the people of that area more reliant on the terrorist groups because they have no alternative and it may actually increase a terrorist group's legitimacy to not have internet. The internet may also be a valuable source of intel for opposition forces looking for weaknesses in the terrorist group controlling the area. This intel can come in the form of internet snooping and interception of communication from the area or even direct information gathering from the populace by engaging in communications via the internet. Another risk of simply removing internet access is that it may be in the best interest of that terrorist group. ISIS, for example, has personally cut internet access in its capital Raqqa in order to extend greater control over the populace.[4] One way of de-radicalizing individuals is by letting them stay in contact with friends and family who are not willing to support their extremism. ISIS has had issues in the past of foreign fighters becoming disillusioned with the leaders of ISIS and contacting friends and family through social media or e-mail. These friend and family members then convince the individual that they should stop assisting ISIS and returning to their home. It is for this reason – to increase control over its current members – that ISIS cut internet access in Raqqa.

Internet access in these high conflict areas typically arise from satellites that provide the internet to a large area. These ISPs are privately owned and have not been

[4] Tasch, Barbara. "ISIS wants to shut down private internet access in the capital of its 'Caliphate'." Business Insider: Military & Defense. July 20, 2015. Accessed November 16, 2015.

shy about providing internet to areas with known terrorist groups. One way of possible addressing this issue would be to work closer with ISPs to determine what ways in which the internet in that area is being used. By identifying websites and services that are possible related to terrorism the ISP could then block access to these areas and prevent terrorists in the area from accessing them. This will not completely stop terrorists from using the internet since information gathering and recruitment are done via popular websites and social media that are more difficult to block. These are all factors to take into consideration when looking at these types of terrorism in cyberspace but in reality a terrorist groups that control large, geographically distinct areas are rare so the importance of continued analysis into these groups may not be very useful.

The more likely situation is attempting to deny internet access to a widely dispersed terrorist network. This is understandably much more difficult as the terrorist must be identified and then tracked. Unfortunately terrorist have access to software designed to increase internet security and ensure anonymity. One example of this is the TOR network that hides the source connection by bouncing a signal over many servers across many countries. It is then difficult to trace the original signal so authorities monitoring suspicious traffic cannot discover exactly where the information originated from without significant investments of time and resources. Another popular choice for increasing security is the usage of an IP VPN service that hides your true location. This is only a single VPN - whereas TOR is several connected nodes - so it is less secure but still difficult for any law enforcement to track individuals hiding behind this layer of cyber defense. The next step for counter-terrorism groups would be to profile internet users hiding behind extra encryption and IP VPNs in order to narrow down a list of potential

terrorists. This strategy will not work either because many internet users are becoming increasingly conscious of their security in the cyber domain.

Arguably precipitated by the Snowden revelations of widespread NSA wiretapping, consumption of specialized cyber security software has been rapidly increasing. The consulting firm ICP has published a report in which it expects the number of IP VPNs users to continue growing through the next decade.[5] This ruins any hope of using software and VPN usage to help in identifying potential cyber terrorists. The difficulty of targeting cyber terrorists for denial of service attacks becomes the difficulty of identifying the terrorists. Terrorists are difficult enough to identify in physical combat situations because they can blend in with average citizens. In cyber space it becomes increasingly difficult to identify individuals so removing a terrorist's ability to access the internet doesn't seem to be a viable strategy to combat terrorism in the cyber domain. Terrorists can use the internet relatively free from worry of being targeted for their actions. At the same time terrorists can use denial of service attacks on states themselves. Denial of service ends up being an advantage for terrorist and a reason to use the internet as a tool for terrorism.

[5] Nav, Chander. "Advanced IP Services and Cloud Connectivity with AT&T's MPLS-Enable Virtual Private Network Solution." White Paper *by International Data Corporation*, sponsored by AT&T. January 2014.

2.2 *Information gathering*

One of the internet's primarily roles since its creation has been to compile and share information. In modern warfare information is absolutely necessary to engage in any large scale conflict and expect success. The US military has a concept of Information Warfare (IW) that involves the use of information technology to gain advantages over an enemy.[6] Information Warfare can take many forms such as collection of tactical data, fact-checking your own military intelligence, or spreading propaganda. For advanced states the internet is merely one source of information. Countries like the United States have vast resources and have the ability to get military intelligence without relying on the internet. Terrorists groups have fewer resources and the internet can be a low cost way for them to gain information. Terrorists are encouraged to engage in Information Warfare because of how important it is to modern military engagements. The US Navy has an officer whose title is "Information Warfare Officer" and a group dedicated to IW known as the Information Dominance Corps.[7] If IW is going to be a tactic so important it has this amount of manpower devoted to it then terrorists would naturally wish to have their own force to oppose enemy IW combatants.

The information collection aspect of IW in particular is valuable to terrorists because they are often engaged in asymmetrical warfare and have to carefully plan

[6] Cebrowski, Arthur K. and John J. Garska. "Network-centric warfare: Its origin and future." US Naval Institute Proceedings Vol. 124 No. 1 (1998): 28-35

[7] "Information Warfare Officer." *United States Navy*. Accessed November 16, 2015. http://www.navy.com/careers/information-and-technology/information-warfare.html

attacks to avoid outright confrontation. The information gathered from the internet can be anything from military intelligence to locations of political rivals. News sources and academic papers often include detailed accounts of military operations, profiles of political leaders, and other information that can be combined with other sources in intelligence to gain a deep understanding of a relevant issue. Terrorists seek information to be able to exert better control over an area and to give them the ability to resist government intervention. The internet is a cheap source of information that terrorists can utilize to gain a variety of different types of information. Terrorists can use the internet to engage in targeted attacks on corporations and government entities, stealing sensitive information. If a terrorist group does not have the capability itself it can use the internet to find and hire professional hackers who are more than willing to get this information for a large sum of money. An example of a website where cybercriminals can be hired to breach a specific system is the now defunct online forum "Enigma."[8] As cyber-security expert Brian Krebs states "crime forums almost universally help lower the barrier to entry for would-be cybercriminals."[9] Terrorists can get in contact with these cybercriminals to bolster their own IW capabilities without having to recruit or train anyone.

One type of information terrorists can gather using the internet is public opinion in an area. Terrorists can use social media and popular news sites to see how people are talking about them and which areas these people are located. This allows terrorists to capitalize on situations in which the local population would be supportive of the terrorist

[8] Krebs, Brian. "Bidding for Breaches, Redefining Targeted Attacks." Krebs on Security. September 23, 2015. Accessed November 16, 2015. http://krebsonsecurity.com/2015/09/bidding-for-breaches-redefining-targeted-attacks/

[9] Krebs, Brian. Spam Nation: The Inside Story of Organized Cybercrime – from Global Epidemic to Your Front Door. Naperville IL, Sourcebooks, 2014.

group's cause. It also allows the terrorist group to find the areas in which the people are resisting. The group can then use physical violence, or the threat of physical violence, to coerce this area to side with them and monitor the effectiveness of the violence by what people are saying online. A terrorists group can spread propaganda via the internet to further strengthen their public image in relevant places. In an area that is already under the terrorist group's control, terrorists engaging in IW can eavesdrop on local internet traffic to find individuals who are opposed to the terrorist group. Gaining information on the civilians is important for a terrorist insurgency because they often rely on the goodwill of the people to help them from being targeted by the incumbent government. Beyond just seeing what a general population thinks, the terrorist group can also gather information on political leaders.

Political speeches are often posted online, in summary if not in their entirety. Political campaigns are also increasingly reliant on internet advertising to spread their message. If this trend of political reliance on the internet grows it gives terrorists much more information on these leaders. Terrorist groups can find political leaders with sympathy for the group and support them. They can also find political leaders who are openly opposed to the mission of the terrorist group and eliminate this leader via direct violence against the leader or by coercing the population and controlling election with violence. These are all secondary uses of the internet that support actions terrorists are already doing. This means that terrorist don't need to alter their current operations much in order to utilize the internet. The internet is merely a weapon for terrorism and like any other weapon is can and will be used in conjunction with many other weapons.

There are a few reasons that terrorists would want to use the internet for information gathering. Firstly and most importantly, the internet is low cost and high benefit. The risk of using the internet is being backtracked to the source and inadvertently allowing enemies to gain information on the terrorist group. Another risk is the inability to ensure the accuracy of information. People can post false information to mislead terrorists knowingly or not. The speed at which information propagates on the internet is very fast so false information or rumors can look credible even without real verification. This can lead to terrorists being used by the populace to attack people or this can also be used by counter-terrorist forces. Terrorists should be aware that they do not completely control the internet and thus cannot ensure the information they receive is accurate.

Although the cost of using the internet is low the benefits are dubious and difficult to understand. It seems that terrorists will certainly use the internet as a source of information but will probably not ever come to completely rely on. Terrorist groups are looking to exert control over a physical area. Cyber space is not physical but it is also a part of any area where citizens can connect to the internet. It is also something that cannot be controlled by any real use of violence because cyber citizens are insulated from physical violence the same way terrorists are. Terrorist should always be wary of the internet because unlike territory it is not something they can exert control over. Citizens can use the internet to inform on the terrorists to the legitimate government. Terrorist recruits can use the internet to reconnect to friends and family and be disillusioned by the terrorist group's mission. Improper use of the internet may also lead to member of the terrorist group leaking sensitive information unknowingly. All of these concerns are things that a capable terrorist leader will consider when choosing how to handle using the

internet. Terrorists can either allow the use of internet or prevent it like in the case of ISIS, regulation is typically too resource intensive for a terrorist group to engage in.

2.3 *Using the internet to command, control and convert*

The internet may look attractive to terrorists because of its ability to increase ease of communication. Communication is the key to any organization and it is particularly important for terrorists that may lack a clear, centralized authority. The internet provides communication between different terrorist cells and other groups within the insurgency. This allows leaders to disseminate information and orders to any number of subordinates without the danger of meeting with these individuals personally. The internet allows a leader to exercise control over a terrorist group without revealing their physical location.

Typically a terrorist group with a strong central leader is vulnerable to decapitation. That is to say, eliminating the leader of one of these groups drastically weakens the group because of their extreme reliance on that leader. A leader in this position might see the internet as an attractive way to communicate with their subordinate because it can make it more difficult for enemies to locate this person through surveillance. There is a danger of the leader actually being traced over the internet and having their physical location discovered but with the proper software this risk can be minimized. To utilize the internet in this way requires an individual with a strong understanding of cyber security. For some modern terrorists this may prove difficult

because of how relatively recent the reliance on the internet has become. Younger generations – like millennials – who have been surrounded by the internet from a young age may have a better natural understanding of internet anonymity. Assuming this is true then it should be expected that the next generation of terrorists will be naturally be more suited to using the internet with a higher proficiency.

Ignoring what capability and desires potential terrorists may have, let's discuss some of the reasons why terrorist groups would see the internet as an important communication tool. The first thing to consider is the internal structure of terrorist groups. There are groups that are very hierarchical and have a central authority which keeps a firm control on the rest of the group. This terrorist structure requires constant contact between the leadership and the individuals so that the leaders can ensure that their instructions are followed exactly. Leaders in religious extremist groups need robust communication systems because they are often responsible for spreading religious doctrine in order to unite the group. Internet communication can be used in this group structure to create and strengthen vertical ties within the group as well as insure unity among members. Other terrorist groups have a decentralized structure that is composed of numerous independent cells loosely related by a shared goal or ideology. Within decentralized terrorist groups communication is often difficult because the different cells operate independently and do not know much about members of the terrorist group outside of their cell. Communication between the cells is often limited to disseminating relevant intelligence, sharing resources, and occasionally planning joint attacks. The internet is an efficient medium to do all of these due to a number of reasons. Decentralized terrorists groups are often more difficult to combat because of the lack of

connection between cells. These groups can use the internet to send anonymous and encoded messages that make it much more difficult to link different cells together than alternative means of communications that leave evidence behind. The internet also allows different cells to set up prearranged cyber drop-offs so that they can spread information without ever actually interacting with other cells. This is helpful because once again it makes it difficult for law enforcement to intercept these exchanges and makes it nearly impossible to link different cells together without having more information. The internet offers a number of valuable advantages for communicating that are tailored for the type of terrorist group. Terrorists often don't have resources to acquire exactly what they need so many of their tools are adapted and imperfect. Internet communication stands out as a dynamic and easily customized tool that may attract terrorist groups who are looking for specialized services to fit their unique group structure.

Terrorists can protect their internet anonymity by using previously discussed technologies like VPNs in order to strengthen the security internet-based communication networks. Terrorist can also use traditional communication espionage techniques – like ciphers – to hide their communications from easily being intercepted. Any successful terrorist group should also know better than to give away any physical location or personal details within communication in order to minimize the damage resulting from intercepted communications. With a bit of online research lots of information can be found that can be used by a terrorist to minimize costs of using internet communication. Law enforcement may intercept these messages but depending on the sophistication of the network and the tools employed by the terrorist group the messages might not contain any real actionable intelligence. A cost of internet communication is that it does create a

semi-permanent backlog of communication if records are not properly erased. This may allow a law enforcement agency to build a case against suspected terrorists and bring them to justice via the legal system if they get access to these logs but it is unlikely to help in proactively identifying terrorists.

One of the most widely reported usages of the internet by terrorism is the usage of social media for recruitment. ISIS in particular is known to post ideological messages to Twitter in an attempt to spread their message to a global audience. A key component of social media is the ease of connecting to other individuals so it is a very powerful platform for spreading a message quickly. USC's Ali Fisher has said that the widespread adoption of social media software has allowed terrorists to "create a persistent as well as ideologically cohesive presence for jihadi propaganda online."[10] In his article Fisher also describes the existence of terrorist groups, primarily ISIS, on Twitter as a "Swarmcast" based on their similarity with a swarm of bees. Even if one connection is terminated or the swarm is interrupted it quickly reforms into a cohesive group. This metaphor helps to explain the difficulty of dealing with terrorists on social media but also within the context of cyber space in general. All nodes of the terrorist network are connected via the internet so even if one node is removed it does not cause any major communication issues.

Consider a centralized network with a central figure or group organizing everything. If this control element is eliminated then the entire network falls apart because they no longer have a means of communicating. Another possible model is a chain model in which a terrorist cell has 2 communication points so that the nodes form a

[10] Fisher, Ali. "How Jihadist Networks Maintain a Persistent Online Presence." Perspectives on Terrorism 9, no. 3 (2015).

linked list and there is no central cell. Removing any cell of a terrorist group organized like this will fracture the group and limit communication and effectiveness even if the group is not completely interrupted. Terrorists that use the internet for communication are insulated from targeted attacks because even if a key figure is removed then there is not necessarily any loss of communication as each cell can communicate with any other group. This makes the classic counterterrorist strategy of decapitation ineffective if not entirely useless as the Swarm will merely reform from the leftover nodes. Terrorist command structures with close reliance on internet communication will be more resistant to targeted attacks which are the US government's most commonly used tool under the Obama administration. Anderson argues for the usage of targeted attacks saying that they are particularly effective at dealing with non-state actors and groups not protected under Security Council resolutions.[11] While it is true that these groups will undoubtedly continue to emerge if they continue the trend of internet organization structures then Anderson's insistence on the important of targeted killings seems moot. This built-in reliance does not necessary ensure more terrorists will use the internet but those groups who use the internet will likely survive longer and become larger threats.

Continuing on with the analysis of ISIS's use of social media under Fisher's Swarmcast model, the usage of social media is key. ISIS is waging a very modern information warfare campaign with a very heavy reliance on propaganda. Think tank VOX-Pol has done an in-depth analysis of ISIS's propaganda messages and has found 7 major targets of propaganda: opponents, international audiences, active members,

[11] Anderson, Kenneth. "Targeted Killing in US counterterrorism strategy and law." *Available at SSRN 1415070* (2009).

potential recruits, disseminators, proselytizer, and recruiters.[12] Some of these targets are straightforward, like targeting opponents with propaganda meant to intimidate. Three of these categories in particular are interesting as they are uniquely possible due to the internet. The first of these is international audiences. Without the internet ISIS's message would be limited to its region of operation and the nearby areas. This would limit its overall effectiveness as that would cause a much more limited pool for potential recruitment and support. By using social media to put out the message terrorist organizations can reach an international audience that it would not able to reach otherwise and may actually prolong its own lifespan as an active insurgency by increasing support and recruitment.

The second key category is active members. The core of ISIS is geographically concentrated and so communication with its members does not seem like it would be relevant. In fact, as mentioned before, ISIS has even removed internet access to its members in its capital Raqqa. The important of using the internet to spread messages to its members shows that ideological weakness within ISIS. Members may gain access to the internet and see ISIS in a negative light due to information they receive. They may also get in contact with family and friends who convince them to defect from ISIS. Internet within the structure of ISIS can end up being a weakness and so ISIS makes great efforts to consistently put out messages to encourage its members to stay loyal to the group and constantly reinforce core ideology. The usage of the internet in this case actually shows a potential weakness that could be exploited by counterterrorist groups.

[12] Winter, Charlie. "Documenting the Virtual 'Caliphate'." *Quilliam Foundation* (2015).

Members of ISIS are already known to be susceptible to internet propaganda so one counterterrorist strategy could be to abuse this known weakness by targeting members of ISIS for anti-ISIS propaganda that could influence these individuals to defect.

The third key target with particular relevance to the internet as a medium is the disseminators. In Fisher's analysis of ISIS on Twitter he found that a majority of ISIS propaganda did not come directly from members of ISIS but rather from retweets of their original message on Twitter.[13] The members that do spread these messages use a constantly shifting swarm of accounts in order to resist being blocked from posting messages. By using social media that has built in sharing features, like Twitter's retweet feature, terrorists are able to utilize a dispersed network of disseminators that may not directly support their cause but are more than willing to help spread the message. Although Fisher is specifically analyzing Twitter, terrorists can use most forms of social media to effectively spread their message over a wide audience. The success of the terrorist group is based on the social features built in to social media networks as well as the adaptability of the terrorist propaganda operators. Some social media networks may be more effective than others and so it may be valuable to see which social media platform is most commonly used by terrorists and attempt to discover what aspects of this platform make it particularly attractive to terrorists groups. As long as there are social media platforms, and for all intents and purposes it appears that there always will be, terrorists have access to free, rapid, and dispersed networks of disseminators that helps spread their message throughout the world.

[13] Fisher "How Jihadist Networks Maintain a Persistent Online Presence"

Using the internet does require some amount of manpower because groups wanting to operate in cyberspace must maintain a constant online presence. Online presence is important because a terrorist group should be able to respond to any criticism quickly and also have the ability to consistently put out ideological messages for supporters and potential recruits. The problem of manpower can be alleviated by automated scripts and bots that release pre-written messages without requiring human intervention. Problems of manpower can also be mitigated capitalizing on public support and relying on voluntary sharing of messages on social media. It is important to keep any audience engaged and so the most effective usage of the internet for communicating is to have a group whose sole purpose is to ensure this happens. It is also important to have individuals in charge of storing and spreading operational information within the organization. This threat has been known by the US government for years with an early example being "Irhabi 007", a 22-year old from the UK who coordinated information online for Al Qaeda cells in several countries.[14] Terrorists cannot simply rely on plaintext e-mails to disseminate sensitive intraorganizational information. There must be trained IT professionals able to set up secure, and anonymous, online repositories of information. This is a barrier to entry for some terrorist groups but not a particularly high one.

The benefits of using the internet for communication are numerous for any terrorist group with the capacity to do so. The usage of the internet makes terrorist groups more resistant to targeted campaigns meant to cause confusion and the disruption of communication by encouraging a decentralized network of communication nodes. The

[14] O'Brien, Lauren B. "The Evolution of Terrorism Since 9/11." *FBI Law Enforcement Bulletin*. Last modified September 2011. Accessed November 16, 2015.

usage of social media also provides a cheap source of manpower in the voluntary spreading official doctrine via built-in sharing options of most social media services. The internet also allows the terrorist group to keep up a constant presence for anyone to reach out to which may build legitimacy. Finally the internet can be used to communicate a terrorist's goals to a much larger audience than more traditional means. There is some potential for counterterrorism based on this information, namely the spread of counter-propaganda by opponents of the terrorist organization, but the benefits of using the internet for communication are outweighed by any risks or costs.

2.4 *Directly using the internet as a weapon*

One of the most important questions to answer in regards to cyberterrorism is how effectively it can be used as a weapon. Many of the ways terrorist use the internet are non-violent and revolve around communication and intelligence. Traditional concepts of terrorism have violence as one of the key denominators of what makes a terrorist group. Whether or not cyberterrorism has to involve violence, physical or digital, is one of the founding question that should be answered in order to properly classify cyber-attacks. It seems that while cyber violence is not necessary for terrorists to utilize the internet as a tool for terrorism the threat of that violence is definitely present. It is important to distinguish cyber-violence and violence in the real world. Violence typically involved physical destruction of property and persons. In cyberspace it is nearly impossible to

destroy anything as there are countless redundant backup systems and very little that affects the real world. Cyber-violence is better classified as interrupting – for any noticeable length of time – an internet service that causes difficulty for many individuals. Cyber terrorism involves disruption, rather than destruction, which means that terrorists may not be as interesting in utilizing it due to its temporary nature. Terrorists traditionally want to seriously disrupt the day-to-day life of as many individuals as possible and cause fear in order to coerce them into compliance. The internet is designed to quickly be fixed and restored to working condition so cyber terrorism may end up inspiring annoyance than fear.

There are a few ways terrorists can utilize internet services to engage in violence in order to coerce a group. One example that has been mentioned previously is the usage of DDoS attacks in order to cripple and extort groups. DDoS attacks can range from targeting individuals in order to remove their ability to access cyberspace all the way up to DDoS transnational organizations and entire states. One of the key examples of state-targeted cyber violence is the case of Estonia in 2007. Estonia is sometimes called E-stonia because of its emergence as one of the most technologically integrated nations. In 2007 Estonia was the victim of a large scale Distributed Denial of Service (DDoS) attack that crippled the entire country's day-to-day operations in additional to physical riots of protest over the removal of a WW2 memorial statue. The director of Estonia's Computer Emergency Response Team, Hillar Aarelaid, had expected this attack and had said "if there are fights on the street, there are going to be fights on the Internet."[15] Despite the

[15] Landler, Mark. "Digital Fears Emerge After Data Siege in Estonia." *New York Times*. May 29, 2015. Accessed November 16, 2015.

warnings and preparedness of the Estonian government the scale of the attack was still able to overwhelm websites relating to government officials, agencies, banking, and many other important services. As this was one of the first example of a true cyber war between a state and non-state actors this is a valuable case study on what to expect if terrorists utilize the internet for attacks.

In DDoS attacks an individual or group takes control of numerous machines connected to the internet and uses them to send numerous requests to certain webpages or internet services.[16] This causes a very large strain on the webhost and ultimately makes it difficult or impossible for legitimate users to access these websites. There are numerous ways to perpetrate DDoS attacks but one thing they all have in common is the relative low manpower required as well as the difficulty of discovering the perpetrator. Usage of specialized Trojan viruses are used to take control of a number of machines at one time. A group of controlled machines are called botnets.[17] This type of attack is self-perpetuating because each infected machine can then continue spreading the Trojan virus to others. Botnets can then be controlled as a whole by the originator of the Trojan who is given access to all infected systems. A single person can create a large botnet due to the rapid peer-to-peer sharing technology abundant on the internet and so the manpower required to engage in this type of attack is incredibly low. Because the attacks hinges on an aggressor taking control of numerous machines connected to the internet the original source of the attack is difficult to trace back to the source. Botnets can be from several

[16] Chang, Rocky KD. "Defending against flooding-based distributed denial-of-service attacks: a tutorial." Communication Magazine, IEEE 40, no. 10 (2002): 42-51

[17] Abu Rajab, Moheeb, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. "A multifaceted approach to understanding the botnet phenomenon." In Proceedings of the 6th ACM SIGCOMM conference on internet measurement, ACM (2006): 41-52

geographical locations, connected to the internet via numerous ISPs, and include an incredibly large amount of data that obscures the originator of the attack. Attacks that are anonymous and not resource intensive are incredibly valuable in asymmetrical warfare. Terrorists looking for a low-cost way of projecting power and disrupting an incumbent government may see a form of DDoS as one of the most efficient ways to do so.

When considering the offensive capabilities of the internet, terrorists groups will also consider conceived vulnerabilities when determining whether or not to use the internet to engage in violence. Actually vulnerabilities are not as important as perceived vulnerabilities because of the fact that terrorists will have imperfect information and within the cyber space there is less cost for failure. An example of a perceived vulnerability is within the US power grid. The electricity grid within the US is incredibly reliant on IT systems and network and this reliance exposes the electrical grid to vulnerabilities within these systems. If a hacker can gain access to the systems that run the US power grid then they can turn off electricity for millions of people and get the attention of an entire nation. Several entities within the US have taken steps to establish cybersecurity standards to help protect key systems – like those that run the power grid – but there has been several challenges to this initiative.[18] These challenges include lack of built-in security features, lack of a coordinated approach to monitor compliance, and a focus on regulatory compliance rather than comprehensive security. So many vulnerabilities in such a key system surely makes an attack on the US power grid incredibly attractive for any terrorist group looking to strike on American soil.

[18] Gaffney, Frank J. *Guilty Knowledge: What the US Government Knows about the Vulnerability of the Electric Grid, But Refuses to Fix.* Center for Security Policy Archival Series (January 26, 2014).

The United States has many perceived cyber vulnerabilities besides weaknesses in the power grid. In 2014 the US Postal Service was hacked and details including names, date of birth, social security numbers, and financial information of over 800 000 people were accessed by an unknown party.[19] The perpetrator of this attack is unconfirmed but some sources blame China so it is unclear if an organization as small and underfunded as a terrorist organization would actually be able to engage in actions like this. Another similar hack, blamed on Russians, involved an unknown number of attackers gaining access to President Obama's personal emails in April of 2015.[20] Neither of the hacks managed to accomplish much real damage or gain any classified information but they were able to show vulnerabilities in US cyber defense. In this case, the actual threat of an attack is not as important at the potential threat. It may be the case that terrorists cannot realistically attack the US via the internet for a variety of reasons. There is already a precedent of the US being vulnerable to cyberattacks due to these previously reported hacks so terrorists may be more willing to try. It seems that if more and more people begin testing US cyber defense then someone is bound to get into an area that is particularly sensitive or dangerous. At that point it is merely a game of statistics and there is no cyber defense strategy currently being employed that is foolproof. One of the core tenants of the American military post-WW2 has been security via deterrence. The US is not successfully deterring enemies in the cyber space because it is allowing constant attacks to occur without publicly doing anything about it. It is doubtful that the US

[19] Weisse, Elizabeth. "U.S. Postal Service hacked, told Congress Oct. 22." *USAToday*, November 10, 2014. Accessed November 16, 2015.

[20] Gibson, Zach. "Russian Hackers Read Obama's Unclassified Emails, Officials Say." New York Times. April 25, 2015. Accessed November 16, 2015.

military is merely ignoring this matter but there needs to be some tradeoff between public discourse and secret actions done to improve defense.

All of this discussion on direct attacks via the internet has been considering the weaknesses of the US in particular. Based on information compiled by ABI Research on cybersecurity preparedness the US ranks as the country most prepared to deal with a cyber-attack.[21] If the country most prepared for cyberattack is still facing these difficulties then other countries are even more at risk. Terrorist groups typically operate in failed states or states with weak infrastructure so it seems that cyberterrorism would be particularly effective in these areas as long as there is a strong enough internet presence. As mentioned before the internet is constantly expanding into all corners of the world so it is possibly – if not likely – that even the weakest states will still have internet access for their citizens at some future date. The current threat of cyberterrorist exists but it is relatively small due to the limitations of the modern internet in the areas that terrorist are typically known to exist in: failed states, rural or undeveloped areas, war-torn areas with little or no infrastructure. Just because the threat is low now does not mean it will stay like this. There should be steps taken to begin preparing for potential cyberterrorism and these steps should be taken now while there is not an immediate danger.

Through this chapter various reasons for terrorists to use the internet have been presented. The internet looks to be an attractive tool in the arsenal of terrorist, both current and future. The internet not only allows terrorists to engage in activities like widespread propaganda, direct attacks on previously difficult targets, and efficient

[21] "Global Cybersecurity Index" By *ABI Research* at the request of *International Telecommunication Union*. December 9, 2014.

internal communications but it also encourages terrorist to operate in ways that make counterterrorism difficult. The internet works best for those groups who are dispersed and resistant to typical terrorist strategy like decapitation. It also facilitates larger terrorist groups because the internet can be successfully used in recruitment, as seen in the case of ISIS, and makes communication between many people and groups much easier than it has ever been before. The danger of terrorists in cyberspace is a real danger and the most important part for states to acknowledge is that everyone is at risk. The next section will discuss some of the steps taken by states, particularly the US, in response to cyber threats and how effect these steps seem to be.

CHAPTER THREE:

Responses to the Emerging Cyber Threat

The internet is a relatively new invention that poses many problems for policy makers and groups in charge of national security. This section will analyze the responses to the cyber threats that have occurred recently. Few, if any, of the responses were designed to specifically respond to terrorists using the internet but are rather meant to increase security of the cyber domain from all malicious users. For the purpose of this paper the effect on terrorist groups in cyber space will be emphasized and brought to the forefront of discussion. The focus will be on legal constraints added to internet users as well as the responses of private individuals. It is likely that militaries around the world, in particular American and Chinese, have made significant progress in establishing cyber-security guidelines and operating procedures but these are not widely available. In order to avoid pure speculation and focus on observable actions military responses will not be considered. This section will analyze responses to cyber threats that include proposed legal restrictions on cyber space, the usage of mass surveillance, and various initiatives to foster more concern for cyber vulnerabilities.

3.1 *Net neutrality and internet regulation*

A key issue for global policy makers that is also important for understanding the role of cyberspace is the idea of "net neutrality." Net neutrality refers the idea that the internet should not be regulated and all individuals and companies should have equal access to the internet. The alternative to net neutrality is blocking certain service providers or giving preferential treatment to certain groups on the internet.[1] The debate on net neutrality is, at its core, the debate on the role of government and regulation on the internet. The current focus of net neutrality tends to be on economic effects of internet regulation and the threat of internet monopolies but these ideas are more far-reaching than this.[2] Besides potential economic abuses there is also a fear of fragmenting the internet so that certain services are only available to certain individuals. Keeping the internet universally accessible and equal to any person is an important aspect of net neutrality defenders. Without the idea of net neutrality it would be the governments' right, if not their duty, to much more carefully monitor internet traffic. Currently internet traffic is monitored at its source and destination. This means that services like VPNs are effective because they scramble the connection between the two points. Without internet neutrality governments could remove the effectiveness of services like this and have much more power to gather intelligence on the internet.

---

[1]Cheng, Hsing Kenneth, Subhajyoti Bandyopadhay, and Hong Guo. "The debate on net neutrality: a policy perspective." Information Systems Research 22, no. 1 (2011): 60-82.

[2] Lee, Robin S. and Tim Wu. "Subsidizing creativity through network design: Zero-pricing and net neutrality." The Journal of Economic Perspectives (2009): 61-76

Proponents of net neutrality wish for the internet to remain open for peer-to-peer communication and completely unregulated. Net neutrality has often been called the "First amendment of our time" in regards to its relationship to freedom of speech and fostering the flow of ideas.[3] The large public pressure to keep the internet neutral is actually very important in determining whether or not terrorists can effectively use the internet. A closely regulated internet that is built to support organizations that pay additional fees in order to improve their internet experience would be worst-case scenario for terrorists group looking to enter into the cyber domain for malicious reasons. It is much more likely to be caught engaging in terrorist acts if things are closely regulated by government entities, ISPs, and private corporations which would be the case if the net neutrality movement failed. Alternatively, with net neutrality in place and minimum regulation on the internet, terrorists don't have very many barriers to enter into cyber-terrorism or other uses of the internet. True net neutrality might even raise the issue of removing terrorist's propaganda from the internet for fear that it would be an attack on free speech.

The United States government seems to have reservations about true net neutrality but there has been no real announcement of their plans for internet regulation. In February of 2015 the Federal Communications Commissions decided to treat the internet like a utility and took control of its regulation.[4] The FCC has promised to promote free expression and innovation on the internet in a series of rules called the "Open Internet."

---

[3] May, Randolph J. "New Neutrality Mandates: Neutering the First Amendment in the Digital Age." ISJLP 3 (2007): 197.

[4] "Open Internet." Federal Communication Commision. Accessed November 16, 2015. https://www.fcc.gov/openinternet

Despite the fact that the FCC has seemingly been promoting Net Neutrality there have been a number of proposed bills that seem to completely contrast Net Neutrality in the US Congress. The first bill that attempted to exert US power into cyberspace was the Protect IP Act (PIPA) in 2011.[5] This bill is actually a rewrite of an even earlier bill – Combating Online Infringement and Counterfeits Act (COICA) – and demonstrates how the government sees the internet. The US government, at least the judicial branch, wants to create legislation to control aspects of the internet they see as illegal or immoral and are willing to push bills forward to do so until it passes. Both PIPA and COICA were created by the House of Representatives and neither of them had much support.

The next example of a bill to regulate online interaction was the House of Representatives' Stop Online Piracy Act (SOPA) also in 2011. This bill attempted restrict websites and ISPs from allowing access to websites streaming pirated media.[6] Although seemingly innocent this bill would have greatly expanded the US government's ability to prosecute individuals based on their internet usage and also potentially limited freedom of speech on the internet. The bill was eventually voted down after an enormous public outcry but it shows Congress's interest in attempting to regulate the internet. Both the House of Representatives and Congress attempted to pass bills restricting internet piracy in the same year but neither passed. It seems that the government support for internet regulation is present but large public outcries and well-supported petitions led to the

[5] "S.968 – Protect IP Act of 2011" U.S. 112th Congress. Sponsored by Sen. Leahy, Patrick J. May 12, 2011.

[6] "H.R.3261 – Stop Online Piracy Act" 112th Congress. Sponsored by Rep. Smith, Lamar. December 16, 2011.

dismissal of both potential bills. A SOPA petition on the White House website, for example, reached over 100 000 signatures.[7]

The most recent potential bill attempting to place restrictions on the internet is the Cybersecurity Information Sharing Act (CISA) of 2015.[8] Whereas PIPA and SOPA were both focused on economic interests relating to piracy in cyberspace, CISA is supposed to address cyber security concerns. The proposed law allows the US government to get information about internet users from privates companies in order to identify and assess potential threats. The bill had initially passed the Senate Intelligence Committee but it has not yet been voted on in a full Senate session. There are a number of concerns from both private citizens and internet-related companies over the fact that the bill gives several governmental organizations access to private information with little oversight. Net neutrality activists see CISA as a violation of the right to privacy and as actually lowering security for individuals. CISA effectively takes responsibility for securing user information away from private companies and puts it in the hands of the government. In terms of cyber capability private companies are actually much more secure than governmental agencies due to the fact that each company may have different cybersecurity protocols whereas government agencies tend to be built upon the same cyber security infrastructure. CISA would open US internet infrastructure to potential information leaks that could be used by terrorists looking to gather information on potential recruits or allies.

[7] "Stop SOPA 2014." We the People Petition (web). Feb 17, 2014. Accessed November 16, 2015.

[8] "S.754 – Cybersecurity Information Sharing Act of 2015." 114th Congress. Sponsored by Sen. Burr, Richard. Introduced 3/17/2015. Passed Senate 10/27/2015.

All of these regulations show that the US government is beginning to consider internet regulations but none of these regulations do much to address the actions that might be carried out by terrorists in cyberspace. These regulations are attempting to apply US laws to cyberspace which is inherently stateless. In order to do this, policy makers are specifically attempting to focus on domestic issues that have precedents in the real world. For examples PIPA and SOPA are both attempting to outlaw the cyber version of theft and piracy. The thinking of US policy makers is flawed because they are trying to apply legal logic based on physical concepts on cyberspace, something that is non-physical and has different rules. There is also the issue of who, if anyone, truly owns cyberspace. Is cyberspace owned by individuals, private groups, states, or someone else entirely? Is there is a single owner of cyberspace or are there several owners? What power do states have over cyberspace if private corporations are in charge of developing, operating, and maintaining it? All of these questions are things that should be considered by policy makers before they begin to impose legal constraints on internet users. Currently the internet is best classified as an independent "territory" in which there is no real governing body. This means that internet is in anarchy and individuals and groups connected to the internet have no support if they are attacked. This is important for terrorist groups because they thrive in anarchy. The fact that there are no real internet-wide regulatory bodies mean that there is no unified and concentrated effort to defeat malicious groups like cyber criminals and internet terrorists.

The US's cybersecurity strategy, based on the ideas found in CISA, seem to be focused on intelligence gathering in order to deter potential internet attacks and discover those that have already occurred. This is not a particularly proactive strategy as the sheer

volume of internet traffic, coupled with the mass consumption of encryption software, means that intelligence gathering is limited in its application. Looking at every internet user's history is impossible so bills like CISA and its younger cousins will likely be ineffective. They may yield some results and may prevent some crimes but there is no guarantee and the odds are that they will miss even more. US policy makers are stuck thinking in terms of the Cold War in which deterrence and technological superiority are the best tools for the situation. Cyber space is so robust and has so much traffic that deterrence is very limited in its application and not effective in preventing malicious activity on a large scale. Technological superiority is also unlikely as the internet is largely based on the principles of sharing and open source development so it becomes increasingly difficult to maintain technological superiority on any related field before someone either makes a similar breakthrough or the technology itself was acquired by competitors via some alternative means.

The rapid pace of technological advancement also makes it difficult for any one group to maintain a monopoly as improvements in all areas of computing are being done by countless independent groups every day. It should also be mentioned that legacy software compatibility is important for new technologies to work well with old technologies. The internet is an amalgamation of technologies developed by countless people and to work together they may share some foundation. This advancement makes it doubly difficult for policy makers to account for as they have cannot react at a very fast pace. There tends to be a decade long gap between technology and global laws created to

regulate these technologies.[9] Terrorists groups are much smaller and less bureaucratic than states so it may be easier for them to integrate new technologies into their strategies before states can properly establish regulations that may prevent this. The current legal and political response to emerging technological threats seems to be particularly lacking and is unlikely to prevent cyber terrorism without a serious reevaluation of priorities and a more efficient way of implementing policy.

3.2 *Legality of mass surveillance*

Another way the US government has responded to emerging threats in cyberspace is to institute mass surveillance campaigns via the National Security Agency (NSA). Edward Snowden, an NSA contractor, leaked sensitive documents detailing a widespread mass surveillance program called PRISM by the US government that involved secretly spying on US citizens, foreign citizens, and foreign political leaders.[10] Shortly after information about the PRISM program leaked James R. Clapper, director of National Intelligence, released a factsheet that included reference to the fact that PRISM had

[9] Vasilescu, Cezar. “"Kybernetické útoky: nové hrozby pro kritickou informační infrastrukturu ve 21. století Cyber Attacks: Emerging Threats to the 21st Century Critical Information Infrastructures." Defense and Strategy EU. June 15, 2012.

[10] Greenwald, Glenn. No Place to hide: Edward Snowden, the NSA, and the US surveillance state. Macmillian, 2014.

successfully helped in counterterrorism activities.[11] It is difficult to judge how effective PRISM actually was in identifying terrorists and stopping potential attacks without specific details and statistics but counter-terrorism was not the only target of PRISM. There is evidence of PRISM being used to listen in on political leaders of nations – including allies of the US – as well as listening to an unknown number of civilians. CISA could be seen as a new version of PRISM, albeit one that has been legalized and limited to only work within American borders.

There are two main issues with mass surveillance as a tool to combat internet terrorism: effectiveness and legality. The effectiveness is dubious as it seems incredibly ambitious to monitor the majority of the internet, bypassing encryption and other defense methods in some cases, and be able to effectively compile this data into a usable format. What the NSA is likely doing is compiling transcripts of the data into massive repositories and then using Big Data analysis techniques in order to mine the raw data for valuable intelligence. Big Data is a quickly growing field that uses specially designed algorithms to analyze enormous data sets that would be impossible to analyze with traditional techniques.[12] Assuming the NSA was using these types of algorithms to analyze the data – which is necessary if they expect to use all of the collected data – then it seems that it would be incredibly easy to hide your intentions in codes that fool these algorithms. For example, if these algorithms are designed to seek out any conversations that sound like terrorists planning an attack, how would they deal with conversations that

[11] Ovide, Shira. "US Official Releases Details of Prism Program." The Wall Street Journal, June 8, 2013. Accessed November 16, 2015.

[12] Manyika, James, Michael Chui, Brad Brown, Jacquest Bughin, Richard Dobbs, Charles Roxburgh, and Angela H. Byers. "Big data: The next frontier for innovation, competition, and productivity." Report for McKinsey Global Institute. May 2011.

don't directly mention attacks? It is well reported that jihadists are known to refer to attacks as "weddings" when they are communicating in order to conceal their intentions. Would these NSA algorithms pull up every conversation involving the words like "wedding" and other commonplace words that may have an alternative meaning?

Identifying terrorists is not a process that can be automated due to the nature of terrorist communication. Terrorists may use different codes, languages, and technology to hide their meaning and modern computers are not at the level in which they can distinguish these hidden meanings. That means that counterterrorism must have human eyes on the situation. Mass surveillance programs like NSA's PRISM would have to be highly automated in order to process such inhumanly large amounts of data. The only way that these kind of operations would be effective is if the sheer volume of data lead to a large number of terrorists being identified despite flaws within the system. The opposite of this would be humans looking over a smaller data set but doing so much more efficiently and in a way that makes it much difficult for terrorists to avoid detection. The question of mass surveillance becomes one of quantity or quality and it is impossible to know at this point which is better for dealing with terrorists.

The other issue of mass surveillance is the issue of its legality. This issue is then broken up into two subsets of issues: domestic and international. The domestic issue of mass surveillance is fairly straight forward. In the United States – and almost all other democratic nations – citizens are guaranteed some measure of privacy. Opponents of mass surveillance argue that the US government, by spying on its own citizens, is actually exceeding its power and failing to ensure the rights of its citizens. One of the arguments for mass surveillance is that personal rights must be suspended in times of

duress in order to increase national security. For mass surveillance programs to continue to be used in combating terrorism the domestic issues that prevent their use should be solved. Legal constraints that outline exactly when surveillance can and cannot be used are necessary. CISA seems like it was trying to solve this issue by outlining one of the ways government agencies could legally obtain information from private corporations.

The other issue of surveillance is the issue of international legality. This issue plagues internet regulation as a whole due to the fact that the internet transcends the idea of states. There is no real state sovereignty in cyberspace currently. The US government using the internet to obtain information on citizens of other states seems like it infringes upon that state's sovereignty but if this infringement was done over the internet, where there are no borders, is it still a violation? How do international laws on non-aggression and basic human rights apply to cyberspace if they were written without the internet in mind? Does international law need to be adapted in order to compensate for modern technology or can the technology be adapted to the law? These issues are things that need to be addressed even before the issue of mass surveillance and its legality are considered at the international level. Cyberspace truly is an anarchical dimension in which the laws of the land are none exist and the rights of the users are constantly changing. There needs to be multilateral discussion on establishing democratic norms for cyberspace so that consistent regulations can be developed. Until the legal issues can be solved both domestically and internationally, the effectiveness of mass surveillance cannot be truly considered. The US's seeming reliance on mass surveillance is actually hurting its global image and creating negative norms associated with aggressive cyber policy that operates outside of the international legal system. These norms set a precedent for cyberspace

being a frontier without laws that may actually attract terrorists towards its use. These norms may also encourage other states to increase their own cyber surveillance capability, leading to even more unwillingness to impose regulations on these types of actions. This can be seen in the fact that several European Union member states have been found to also engage in mass surveillance programs similar to the US's PRISM program despite the fact that these programs violate EU law.[13]

3.3 *Cybersecurity initiatives*

Attempting to change the legal system is not the only way states have been responding to cyber threats. There have been numerous advances in cybersecurity in recent years, both in terms of theory and practice. One of the most successful examples of improved cybersecurity is Estonia after being the first victim of a major cyber-attack in 2007. After 2007 Estonia began using a new cybersecurity system on all key internet services that has made it much more resilient to cyber-attack and has prevented it from being successfully targeted since 2007. The system Estonia uses is known as Keyless Signatures' Infrastructure (KSI).[14] KSI provides a layer of security that includes a digital signature that verifies the authenticity of an attempted connection to a network as well as

[13] Bigo, Didier, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Rossi Ragazzi, and Amandine Scherrer. "Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law." Liberty and Security Papers 61 (2013).

[14] "Keyless Signature Infrastructure." E-stonia Digital Society (web). Accessed November 16, 2015. https://e-estonia.com/component/keyless-signature-infrastructure/

a timestamp. KSI, as the name implies, has no keys that can be compromised and instead assigns unique identifiers to each file that can be independently verified via the use of hashes.[15] This offers two benefits over earlier technologies: it makes it more difficult for non-authorized users to access data or forms and it also provides information on who accessed what information when. This, coupled with anti-flooding technology built into their key systems, prevents DDoS attacks like what occurred in 2007. KSI also provides increased transparency and accountability for the government in order to reassure the citizens that the internet services are being used responsibly by the government. Due to the fact that all internet traffic is stored with users and dates and under KSI cannot be erased means that the government always has evidence to show its actions are entirely legal. A state-wide cybersecurity initiative is incredibly difficult and expensive but Estonia is a case that shows that it is possible and effective.

It is not only individual states that are looking to improve their cybersecurity but collective cybersecurity is also increasingly seen as a valuable way to increase cyber capacity. In November of 2010 NATO leaders agreed to a new cyberdefense policy at a summit in Lisbon.[16] This response was in part due to the experiences of Estonia, a NATO member state, in 2007. NATO relies on cyber networks in order to facilitate communication and cooperation among its members. Due to how closely related the member states of NATO are, a weakness in the systems of one state is a weakness for all states. This encourages not only collective defense but collective initiatives for improving cybersecurity in each NATO member state. NATO faces a few challenges in its

[15] Buldas, Ahto, Andrew Kroonmaa, and Risto Laanoja. "Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees." Secure IT Systems. Springer Berlin Hedelberg (2013): 313-320

[16] Abrial, Stephanie. "NATO Builds Its Cyberdefenses." New York Times, February 27, 2011.

establishment of a joint cybersecurity force. First, how much power does it truly have in terms of cyber security when a majority of the internet is held by private hands? Second, what exactly constitutes an attack on a nation and would a cyberattack be enough for a NATO response under Article V of the Washington treatment (an attack on one is an attack on all)? There are also questions of how much of its budget and forces should be allocated to cyberdefense as opposed to operations in the physical world.

Despite the weaknesses of collective security it may have the best chance of being successful. Creating a multinational cyber defense organization mitigates some of the issues of state sovereignty in cyber space and cyber threats that originate from multiple states. NATO's focus on cyber security also show that it recognizes its growing importance. Whether cyberwar is a real threat for the future is irrelevant now as NATO's growing cyber capability will force its rivals, primarily China and Russia, to respond by improving their own cyber infrastructure. The focus of NATO's cybersecurity policy is to protect communication systems and ensure that each member state is able to defend themselves against cyber-attack.[17] NATO's Computer Incident Response Capability (NCIRC) allows NATO to supply centralized and constant cyber defense support to member states.[18] Having a single central authority responsible for cyber defense is also valuable in that is helps establish definitions and acceptable response for cyber-attacks and standardizes cyber security training.

[17] "Cyber Security." NATO Official Website. Last updated September 1, 2015. Accessed November 16, 2015.

[18] Anil, Suleyman. "NCIRC (NATO Computer Incident Response Capability)" 11th TF-CSIRT Meeting at Madrid, Spain. Jan 15, 2004.

Having a centralized authority may be valuable to facilitate cooperation among so many groups but it also has its own weaknesses. It provides a single, high priority target for any groups looking to engage in cyberwar against NATO (as unlikely as that may be). A central command also puts certain member states at advantage over others in getting assistance due to physical proximity. The internet is often seen as instantaneous communication but this is not the case. It takes time for messages to travel across the internet and is particularly noticeable when the source and destination are far removed from each other. Signals between states on opposite side of the Atlantic Ocean in particular may detect noticeable lag that may negatively affect operational efficiency. It is also dangerous for NATO to try to force cyber security to fit into traditional molds of collective security. The cyber domain is different than physical domains and should be considered independently of traditional ideas of strategy in order to create a dynamic and effective cyber policy that is not over reliant on outdated concepts.

NATO member states are not the only ones attempting to revamp their cyber security measures. The People's Republic of China has recently made grade strides in standardizing and improving its cyber defense capability. President Xi Jinping has made cyber security a key issue for the Chinese government and created a concerted cyber security strategy for the first time.[19] One of the unique aspects of Chinese cyber policy is that it considers foreign software a threat and thus encourages the use of proprietary software. This has made China increasingly independent from the foreign IT industry and is a stark contrast to the collective security of NATO. China's method for cyber security

[19] Gierow, Hauke Johannes. "Cyber Security in China: New Political Leadership Focuses on Boosting National Security." China Monitor no. 20. December 9. 2014.

revolves around a uniform and comprehensive response to cyber threats that does not adjust to the dynamic needs of the average internet user. This leaves China open to potential system-wide vulnerabilities that can be exploited by hackers, terrorists, or foreign governments looking to compromise Chinese IT systems. China's independence means that it does not have to account for vulnerabilities in the IT infrastructure of its allies but its approach to cyber security is flawed and needs to be revamped. The issue of cyber security in China is currently a very political issue that is more about internal power struggle than real infrastructure development. It is impossible to tell if China will resolve its political issues to improve cyber defense but if it does it has the potential to be an incredibly powerful cyber nation in terms of cyber security.

3.4 *Non-governmental responses*

Cyber security and the dangers of internet terrorism are not only issues for states to deal with. Individuals, private corporations, and NGOs all have to contend with the dangers of cyberspace. Private firms specializing in various aspects of cyber security are numerous all over the world. As an example of how large the cybersecurity industry has become, Cybersecurity Ventures posts a list of the top 500 cybersecurity firms within the US each year.[20] The top-ranked firm of 2015 is FireEye which offers personalized

[20] "Cybersecurity 500" Cybersecurity Ventures. July 31, 2015. Accessed November 16, 2015. http://cybersecurityventures.com/cybersecurity-500/

consulting and cyber security to individuals and businesses and also provides information and training on current security threats.[21] The firm is really focused on assessing the weakness of a security system through penetration testing and then going through several steps to help solve these security issues. Because it works on a much smaller scale than a government it can personalize cyber security measures that best suit each of its clients. It also publishes reports on security vulnerabilities and provides lots of free information on cyber security and potential threats on its websites. The focus of many firms are specifically corporate cyber security so it is unknown how they might respond to the threat of cyber terrorism.

Many private organizations also have their own specialized cybersecurity teams such as Hewlett-Packard Co. which publishes a Cyber Security Risk Report each year detailing various dangers of the internet.[22] This report only mentions the dangers of terrorism operating on the internet in passing by citing a report that claims terrorists receiving training in cyberwar from supporters in the Middle East. The majority of the report mentions specific cyberattacks that could be employed by terrorist so while cyber terrorism is not directly addressed this report does acknowledge the issue and inadvertently includes ways of thwarting potential cyberterrorist attacks. Terrorists are largely the concern of states and not private corporations by cyber security is something that needs to be done at all levels of society in order to be effective.

[21] "Current Threats" FireEye. Accessed November 16, 2015. https://www.fireeye.com/current-threats.html

[22] "HP Cyber Risk Report 2015." HP Security Research. 2015. Accessed November 16, 2015.

Any computer connected to a network can be the target of a cyber terrorist attack so all citizens must have some level of defense in place to defend themselves. Oftentimes this defense is built into systems intuitively so users do not need to operate or even understand the security measures in place. This is a dangerous approach to security as it opens the network to vulnerability caused by user ignorance. An example of this would be social engineering in which a hacker speaks with an individuals and convinces the individual to divulge sensitive information that would allow the hacker to access a private network. Another attack that may be effective on individuals not familiar with cyber security are phishing attacking. Phishing attacks involve a fake website pretending to be a real website in order to convince a user to input their username and password. The false website then saves this information and forwards the victim to the real website so that they stay unaware that they just compromised their own account. It is important to increase education and raise the overall level of internet literacy in order to insulate networks from cyber-attacks based on exploiting ignorance of users. The National Initiative for Cybersecurity Education is an example of a proposed way to foster cybersecurity education and is supported by IEEE.[23] There is danger in widespread education about cyber security as it gives future terrorists the ability to gain deeper understanding of cyber security and may allow them to find ways to bypass this security. Terrorists are the minority group of cyber security consumers, however, and thus the benefits of educating the masses on cyber security would outweigh the costs.

[23] Paulsen, Celia, Ernest McDuffle, William Newhouse, and Patricia Toth. "NICE: Creating a cybersecurity workforce and aware public." IEEE Security & Privacy 3 (2012): 76-79

A final example of non-governmental cyber security initiatives is the increasingly popular topic "Cyber Threat Analysis." Cyber Threat Analysis (CTA) is a way to use Big Data to analyze large portions of corporate data in order to analyze weaknesses in the cyber network that can be strengthen for improved defense.[24] It is a constant process that fosters a fast and dynamic response to emerging threats. Algorithms run that analyze risks and feed this data directly to security programs that can then respond in real time as threats are identified. This form of cybersecurity is dynamic and efficient but also automated so it does not need a lot of manpower. This type of threat analysis is supposed to be much faster than typical responses so a group that employs CTA can respond to events as they occur and minimize damage rather than trying to repair things after the attack has already occurred. CTA is also focused on processing and sorting information by relevance so the largest risks are dealt with first as opposed to dealing with risks in chronological order.

This approach to cyber security is much different than previously discussed ideas like collective security and deterrence. CTA is built to respond to the unique aspects of the internet that make it so resilient to applying other, previously established security techniques. CTA can also be applied on top of existing infrastructure and does not necessitate a complete system-wide renovation to support the security. CTA is what future cybersecurity should strike to be: fast, efficient, dynamic, and actionable. Cyber Threat Analysis is a method pioneered by independent cyber security firms and shows the potential of private industry in the cyber domain. Traditional warfare is done exclusively

[24] "What is Cyber Threat Intelligence and why do I need it?" iSightPartners Inc. 2014. Accessed November 16, 2015.

by states because they have a monopoly on violence and are the institutions most able to effectively organize large armies. This does not hold true for the cyber domain as states do not have a monopoly on much of anything on the internet. States cannot exert control over the internet so it might be necessary to pass the buck of cyber security to private corporations that have a more vested interest in the cyber world.

If the internet is controlled primarily by private groups then perhaps these groups should be the one responsible for defending it. Governments could support these private groups by allowing them to exercise more freedom in the cyber domain rather than trying to use laws like CISA to force the private entities to assist the government. If laws are needed then they could be laws to ensure private corporations are acting in the best interests of their clients and maximizing cybersecurity rather than profits. An example of a law that could be used to impose stricter security standards on privately owned IT corporations could be a fine for software found to have a serious security flaw. This would lead corporations to implement more rigorous testing standards in order to put out software that they are sure is completely secure. This would effectively reduce a lot of the ways terrorist could abuse internet services for their own malicious purposes.

CHAPTER FOUR:

Conclusion and Policy Recommendations

Terrorism has a variety of ways to use the internet to accomplish its own goals such as using social media for recruitment, engaging in targeted disruption of incumbent governments, and using internet services for robust communication options. The internet also offers numerous benefits for terrorists like offering new offensive techniques and encouraging dispersed networks of terrorist cells that are more resistant to counterterrorism strategies. The response to this emerging threat has been underwhelming and there are very few places in which the threat of cyber terrorism specifically is addressed. Although cyber security is a concern for many nations they do not frame it in terms of how terrorists can use the internet and this is a mistake. Terrorists can use the internet in new ways to promote their own goals and governments will be unable to effectively respond because they have not properly considered all of the implications of terrorists using the internet. This is a field that should be researched further in order to ensure preparedness. Without further research there are also a few general policies that would help better prepare states and their citizens for the unique threat of internet terrorism.

4.1 *Policy Recommendation: Increase cybersecurity education initiatives*

The first recommendation I would like to offer is for government to make an effort to offer early-education classes on cyber security and exercising responsibility on the internet. Even the best designed cyber security strategy can crumble if the average citizens do not know how to properly implement it. In cyber security you are only as strong as your weakest link and that means the government is only as strong as its most inept employee. Complicated security systems will not insulate governments from attacks if an employee allows their password to get stolen via a phishing scam or a keylogger or some other easily identifiable method. It is possible to design a system to prevent these types of scams from occurring at all; a web browser can know to alert the user when a website is suspicious or detect when a keylogger is being installed. It is unnecessarily resource intensive to design system to account for every possibility when it is much more efficient and a more long-term solution to merely educate people about security concerns when they are using the internet.

It is safe to say that within a couple of decades nearly everyone in the world will be connected to the internet if they wish. This means there will be an incredible volume of traffic on websites and it may be impossible to monitor it all and provide security to every individual. Just because we have police officers in the real world does not mean people shouldn't know how to protect themselves. This same principle should be true for the internet. Early-education seems like the best time to begin education on cyber security so that it will be ingrained on children and they will grow up with norms of safe internet usage. This would greatly strengthen internet infrastructure without actually investing in

the infrastructure itself. Education should be offered that includes topics such as potential internet scams, password security, and basic cryptography. This deeper understanding of the way the internet works would help people remain safe on the internet.

This increased security would then take away some of the tools that terrorists may exercise on the internet. Terrorists would lose access to some sensitive information as people learn to properly protect themselves and their employer from individuals looking to obtain sensitive information. Terrorists would also have a more difficult time engaging in direct cyberattacks because there will be fewer vulnerabilities to exploit in order to carry out the attack. There is a threat that terrorists themselves will receive this education and thus become more difficult to target by counterterrorist groups. This is a risk that is worth taking because if both sides have stronger defenses then the internet becomes a much less attractive option to terrorists looking for cheap methods of engaging in violence and coercion.

4.2 *Policy Recommendation: Focus on private industry*

Private industry is uniquely suited to deal with cyber threats for a number of reasons. The private industry is the majority owner of the internet and are also by-and-large the innovators of IT technology. This means private firms, more so than governments, are at the cutting edge of technology and in a position to impose changed to vast portions of the internet for the sake of improved security. Private industry has

already shown initiative with many leading internet technologies including robust security options without any government regulations forcing them to do so. Internet users expect their information to be secure so private industry also has a large stake in insuring that there are high security standards or else they will lose customers and revenue. The norms of capitalism can be the driving force of technological innovation for increased cyber security.

The counter argument is that terrorists will most likely target governments and so it should be the government's response to deal with this threat. It is also in the best interest of the citizens for the government to take an active role in internet regulation because the government's job is to ensure that its citizens' rights are not being violated. Without the government's backing there is no guarantee that private corporations will find a way to maximize profits at the expense of security. The government is needed to provide oversight and ensure that a situation like this can never occur.

It seems unlikely that government regulation is necessary for the private development of cyber security technologies. There are numerous private firms whose sole purpose is to provide cyber security consulting and assistance. These groups are better suited to dealing with issues in cyber security because they are smaller and more agile, able to react quickly and dynamically to a problem. Governments, on the other hand, are tied down by red tape and cannot quickly react to cyber threats as they emerge. That is one reason this paper is so important: governments should begin planning for cyber terrorism now so that they don't have to desperately respond to a future act of aggression without a plan like the US government did after 9/11.

It is not advisable for governments to completely rely on private industry for the purposes of cyber defense but instead there should be joint action taken between government agencies and private industries. Let the private corporations deal with innovation and new security methods while the government supplies funding and legal support for these new defense strategies. As I have mentioned numerous times before now, in cyber security you are only as strong as your weakest link. This implies that there should be no one left behind in the push to secure internet infrastructure from malicious attacks from terrorists or any other group. Cyber security is a group effort that must be engaged with at every level in order to be completely successful.

4.3 *Policy Recommendation: Multilateral discussion and establishing international norms*

Cyberspace is an international domain without state borders so the issue of terrorists operating within cyberspace cannot be addressed by a single state. There needs to be discourse within the United Nations and other international bodies so that a clear understanding can be established among the world's governments. The current issue is that no major power really wants to address the issue of cyber security because they have become reliant on cyber espionage. Creating laws to limit actions a legitimate actor can take in cyberspace would most likely limit – if not completely outlaw – mass surveillance programs that many states use. By publicly discussing the issue states may potentially

weaken themselves by taking away one of their tools for self-defense: intelligence gathering. Because of the security dilemma states are unlikely to do this so international regulation on actions within cyberspace are unlikely to progress until a major power steps forward and really pushes a pro-cyber security agenda.

Someone needs to step forward and take responsibility in establishing norms of good faith relationships in cyberspace. Until this happens there will be few international laws placed on the internet and few international restrictions placed on terrorists looking to operate within cyberspace. States need to make a choice between sacrificing their ability to operate freely in cyberspace and allowing terrorist free reign to engage in propaganda campaigns and cyber-attacks. As it is now, the internet is a very attractive option for terrorists because they do not need to fear international pressures. If a terrorist uses the internet to attack a state it is the responsibility of that state to respond and no one else. This limits the amount of resistance terrorists face by using the internet as a tool for insurgency. It is much easier for the terrorist to then make a cost-benefit analysis on whether or not to use the internet due to a lack of external influence.

If states do engage in multilateral discussions and eventually agreements that regulate cyberspace then it only hurts potential internet terrorists. The first step in this discussion is to establish norms of peaceful cohabitation in cyberspace. States need to stop covertly hacking each other for information and instead rely on other means to obtain intelligence. Private citizens are so used to hearing about major hacks that they are becoming desensitized to cyber violence and norms established against these kinds of action would do a good job of reminding citizens of the dangers present on the internet. Cyberwar is at its heart information warfare and governments need to realize that they are

not enemies in information warfare. The real enemies are terrorist and cybercriminals who will use tensions between different states in cyberspace to exploit the system and strengthen their own insurgency while delegitimizing real governments.

4.4 *Conclusion*

Terrorists are currently beginning to use the internet as a key part of their insurgent strategy and trends seem to show that this will continue to occur unless something is done to stop it. Terrorists currently have lots of incentives to use the internet and engage in cyber and information warfare. Terrorists are also uniquely positioned to take advantages of flaws in the system due to the anarchy of cyberspace and the lack of laws regulating internet usage. Policy makers are stuck trying to use Cold War logic to deter terrorists from using the internet in ways that do not make sense with in terms of cyberspace. Furthermore, policy makers are hesitant to put forth more cybersecurity-focused agendas for fear of weakening themselves by outlawing mass surveillance programs and other abusive actions currently done by states in cyberspace.

In order to combat the threat of terrorism in cyberspace, more research needs to be done to better understand the ways and reasons terrorists are using the internet. This is an under-researched that field that has numerous opportunities for increased academic exposure. More analysis on how terrorists are using social media, threat analysis of key US infrastructures' subjected to cyber-attacks, and the effect of internet on a population

controlled by terrorists are just a few potential research topics that could lead to a better understanding of the relationship between terrorism and the internet. A few preliminary policy recommendations to combat this threat are to increase early-childhood education to improve cyber security literacy, support private industry in building robust cyber security infrastructure, and for states to engage in multilateral discussion on establishing international laws over cyberspace. These would be good steps to combatting the threat of terrorism on the internet but the lack of understanding of this topic really limits what can be done. Once more research is done more specialized recommendations can be made to properly address different aspects of the cyberterrorist threat.

BIBLIOGRAPHY

CHAPTER 1

1. U.S. Department of State. “Foreign Terrorist Organizations.” Bureau of Counterterrorism. Last modified September 30, 2015. Accessed November 16, 2015. http://www.state.gov/j/ct/rls/other/des/123085.htm

2. Rapoport, David C. "The four waves of modern terrorism." *Attacking terrorism: Elements of a grand strategy*, edited by Audrey Kurth Cronlin. 47-73. Washington D.C.: Georgetown University Press, 2004.

3. Jervis, Robert. “Cooperation under the security dilemma.” *World Politics* 30, no. 02 (1978): 167-214

4. Glaser, Charles L, and Chaim Kaufmann. “What is the offense-defense balance and how can we measure it?.” *International Security* 22, no. 4 (1998): 44-82

5. Gartzke, Erik. “The myth of cyberwar: bringing war in cyberspace back down to Earth.” *International Security* 38, no. 2 (2013): 41-73

6. Collins, Sean and McCombie, Stephen. “Stuxnet: the emergence of a new cyber weapon and its implications.” *Journal of Policing: Intelligence and Counter Terrorism* 7, no. 1 (2012): 80-91

7. Thomas, Timothy L. *Al Qaeda and the Internet: The Danger of ‘Cyberplanning’.* Fort Leavenworth: Foreign Military Studies Office (ARMY) (2003).

8. La Rue, Frank. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue” Paper presented at the United Nations General Assembly Human Rights Council, 17th session. London, United Kingdom. May 16, 2011. (Document A/HRC/17/27)

10. Zelin, Aaron Y. “al-Malāḥim Media presents a new issue of al-Qā’idah in the Arabian Peninsula’s magazine: ‘Inspire #14’.” *Jihadology*. Last modified September 9, 2015. Accessed November 16, 2015. http://jihadology.net/category/inspire-magazine/

11. al-A’siri, Ibrahim ibn Hassan. “Charlie Hebdo: Military Analysis.” *Inspire Magazine: Assassination Operations,* issue 14: 38-42. Summer 2015.

12. Ernst, Douglas. “Terrorist ‘moron’ reveals ISIS HQ in online selfie; U.S. Air Force promptly destroys compound.” *The Washington Times*, June 4, 2015. Accessed November 16, 2015. http://www.washingtontimes.com/news/2015/jun/4/air-force-bombs-islamic-state-hq-building-after-te/

13. Mroue, Bassem. “Here’s A Breakdown Of The Oil Assets ISIS Now Controls.” *Business Insider: Military & Defense*, September 25, 2015. Accessed November 16, 2015. http://www.businessinsider.com/breakdown-of-the-oil-assets-isis-controls-2014-9

14. Kaplan, Eben. “Tracking Down Terrorist Financing.” *Council on Foreign Relations,* April 4, 2006. Accessed November 16, 2015. http://www.cfr.org/terrorist-financing/tracking-down-terrorist-financing/p10356

CHAPTER 2

1. La Rue, Frank. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue” Paper presented at the United Nations General Assembly Human Rights Council, 17th session. London, United Kingdom. May 16, 2011. (Document A/HRC/17/27)

2. A Human Right. “Projects.” *A Human Right*, last modified 2015. Accessed November 16, 2015. http://ahumanright.org/projects.php

3. Zuckerberg, Mark. Facebook post. March 27, 2014, accessed November 16, 2015. https://www.facebook.com/zuck/posts/10101322049893211

4. Tasch, Barbara. "ISIS wants to shut down private internet access in the capital of its 'Caliphate'." *Business Insider: Military & Defense.* July 20, 2015. Accessed November 16, 2015. http://www.businessinsider.com/isis-wants-to-fully-control-internet-access-in-the-capital-of-its-caliphate-2015-7

5. Nav, Chander. "Advanced IP Services and Cloud Connectivity with AT&T's MPLS-Enable Virtual Private Network Solution." White Paper by *International Data Corporation,* sponsored by AT&T. January 2014. http://www.business.att.com/content/whitepaper/Advanced-IP-MPLS-VPN.pdf

6. Cebrowski, Arthur K. and John J. Garska. "Network-centric warfare: Its origin and future." *US Naval Institute Proceedings* Vol. 124 No. 1 (1998): 28-35

7. "Information Warfare Officer." *United States Navy*. Accessed November 16, 2015. http://www.navy.com/careers/information-and-technology/information-warfare.html

8. Krebs, Brian. "Bidding for Breaches, Redefining Targeted Attacks." *Krebs on Security*. September 23, 2015. Accessed November 16, 2015. http://krebsonsecurity.com/2015/09/bidding-for-breaches-redefining-targeted-attacks/

9. Krebs, Brian. *Spam Nation: The Inside Story of Organized Cybercrime – from Global Epidemic to Your Front Door.* Naperville IL, Sourcebooks, 2014.

10. Fisher, Ali. "How Jihadist Networks Maintain a Persistent Online Presence." *Perspectives on Terrorism* 9, no. 3 (2015).

11. Anderson, Kenneth. "Targeted Killing in US counterterrorism strategy and law." *Available at SSRN 1415070* (2009).

12. Winter, Charlie. "Documenting the Virtual 'Caliphate'." *Quilliam Foundation* (2015).

14. O'Brien, Lauren B. "The Evolution of Terrorism Since 9/11." *FBI Law Enforcement Bulletin.* Last modified September 2011. Accessed November 16, 2015.

15. Landler, Mark. "Digital Fears Emerge After Data Siege in Estonia." *New York Times.* May 29, 2015. Accessed November 16, 2015. http://www.nytimes.com/2007/05/29/technology/29estonia.html

16. Chang, Rocky KD. "Defending against flooding-based distributed denial-of-service attacks: a tutorial." *Communication Magazine, IEEE* 40, no. 10 (2002): 42-51

17. Abu Rajab, Moheeb, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. "A multifaceted approach to understanding the botnet phenomenon." In *Proceedings of the 6th ACM SIGCOMM conference on internet measurement*, ACM (2006): 41-52

18. Gaffney, Frank J. *Guilty Knowledge: What the US Government Knows about the Vulnerability of the Electric Grid, But Refuses to Fix*. Center for Security Policy Archival Series (January 26, 2014).

19. Weisse, Elizabeth. "U.S. Postal Service hacked, told Congress Oct. 22." *USAToday*, November 10, 2014. Accessed November 16, 2015. http://www.usatoday.com/story/tech/2014/11/10/us-postal-service-post-office-hacked/18795289/

20. Gibson, Zach. "Russian Hackers Read Obama's Unclassified Emails, Officials Say." *New York Times.* April 25, 2015. Accessed November 16, 2015. http://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html

21. "Global Cybersecurity Index" By *ABI Research* at the request of *International Telecommunication Union.* December 9, 2014.

CHAPTER 3

1. Cheng, Hsing Kenneth, Subhajyoti Bandyopadhay, and Hong Guo. “The debate on net neutrality: a policy perspective.” *Information Systems Research* 22, no. 1 (2011): 60-82.

2. Lee, Robin S. and Tim Wu. “Subsidizing creativity through network design: Zero-pricing and net neutrality.” *The Journal of Economic Perspectives* (2009): 61-76

3. May, Randolph J. “New Neutrality Mandates: Neutering the First Amendment in the Digital Age.” *ISJLP* 3 (2007): 197.

4. “Open Internet.” *Federal Communication Commission.* Accessed November 16, 2015. https://www.fcc.gov/openinternet

5. “S.968 – Protect IP Act of 2011” *U.S. 112th Congress.* Sponsored by Sen. Leahy, Patrick J. Introduced May 12, 2011.

6. “H.R.3261 – Stop Online Piracy Act” *112th Congress.* Sponsored by Rep. Smith, Lamar. Introduced December 16, 2011.

7. “Stop SOPA 2014.” *We the People Petition (web).* Started Feb 17, 2014. Accessed November 16, 2015.

8. “S.754 – Cybersecurity Information Sharing Act of 2015.” *114th Congress.* Sponsored by Sen. Burr, Richard. Introduced 3/17/2015. Passed Senate 10/27/2015.

9. Vasilescu, Cezar. “"Kybernetické útoky: nové hrozby pro kritickou informační infrastrukturu ve 21. století Cyber Attacks: Emerging Threats to the 21st Century Critical Information Infrastructures." *Defense and Strategy EU.* June 15, 2012. doi: 10.3849/1802- 7199.12.2012.01.053-062

10. Greenwald, Glenn. *No Place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillian, 2014.

11. Ovide, Shira. “US Official Releases Details of Prism Program.” *The Wall Street Journal,* June 8, 2013. Accessed November 16, 2015.

12. Manyika, James, Michael Chui, Brad Brown, Jacquest Bughin, Richard Dobbs, Charles Roxburgh, and Angela H. Byers. “Big data: The next frontier for innovation, competition, and productivity.” Report for *McKinsey Global Institute*. May 2011.

13. Bigo, Didier, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Rossi Ragazzi, and Amandine Scherrer. “Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law.” *Liberty and Security Papers* 61 (2013).

14. “Keyless Signature Infrastructure.” *E-stonia Digital Society (web).* Accessed November 16, 2015. https://e-estonia.com/component/keyless-signature-infrastructure/

15. Buldas, Ahto, Andrew Kroonmaa, and Risto Laanoja. “Keyless Signatures’ Infrastructure: How to Build Global Distributed Hash-Trees.” *Secure IT Systems*. Springer Berlin Hedelberg (2013): 313-320

16. Abrial, Stephanie. “NATO Builds Its Cyberdefenses.” *The New York Times*, February 27, 2011. http://www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html

17. “Cyber Security.” *NATO Official Website.* Last updated September 1, 2015. Accessed November 16, 2015.

18. Anil, Suleyman. “NCIRC (NATO Computer Incident Response Capability)” *11th TF-CSIRT Meeting at Madrid, Spain*. Jan 15, 2004.

19. Gierow, Hauke Johannes. “Cyber Security in China: New Political Leadership Focuses on Boosting National Security.” *China Monitor* no. 20. December 9. 2014.

20. “Cybersecurity 500” *Cybersecurity Ventures*. July 31, 2015. Accessed November 16, 2015. http://cybersecurityventures.com/cybersecurity-500/

21. “Current Threats” *FireEye.* Accessed November 16, 2015. https://www.fireeye.com/current-threats.html

22. “HP Cyber Risk Report 2015.” *HP Security Research.* 2015. Accessed November 16, 2015.

23. Paulsen, Celia, Ernest McDuffle, William Newhouse, and Patricia Toth. “NICE: Creating a cybersecurity workforce and aware public.” *IEEE Security & Privacy* 3 (2012): 76-79

24. “What is Cyber Threat Intelligence and why do I need it?” *iSightPartners Inc*. 2014. Accessed November 16, 2015.