THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

ENABLERS OF TERRORISM: TECHNOLOGY AND THE WEB

BRETT BURAN

Fall 2011

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in SECURITY AND RISK ANALYSIS
with honors in SECURITY AND RISK ANALYSIS

Reviewed and approved* by the following:

Dr. Peter Forster
Senior Instructor
Thesis Supervisor

Dr. Peng Liu
Professor
Honors Advisor

Colonel Jacob Graham
Professor of Practice
Faculty Reader

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

Over the last decade, digital technologies have vastly improved. No longer are users required to sit at their desk to access valuable resources on the Internet. With the click of a button on a phone, laptop, iPad, or any other mobile device, users can scour the vast world of the World Wide Web. This can be used by people to connect with other people through social networking and purchase items online through online distribution channels.

Unfortunately, this information is not always used for good. It can be used to identify potential targets to attack by malicious people. With the help of search engines like Google and Bing as well as virtual maps such as Google Maps, crucial vulnerabilities in security measures can be discovered. Terrorists are one benefactor of information accessibility. They use information in planning and selecting targets. Using legal means, terrorists are able to obtain eighty percent of the information they need to plan an attack.

Advancements in digital technologies have helped to enable terrorist recruitment, attack coordination, and command and control. It seems as if terrorists are always one step ahead of counter terrorism organizations. Only once we fully understand terrorism and how terrorists are integrating new technology will we be able to be ahead of terrorists and save American lives.

TABLE OF CONTENTS

LIST OF FIGURES iii

LIST OF TABLES iv

ACKNOWLEDGEMENTS v

Chapter 1 Introduction 1

Chapter 2 Brief Evolution of Terrorism: From Turn of Century 7

Chapter 3 Recruitment and Training 11

Chapter 4 Attack Coordination 22

Chapter 5 Command and Control 31

Chapter 6 Conclusion 34

Appendix A Terrorist Organizations 37

- Al-Qaida 37
- Ansar al-Islam 38
- Fuerzas Armadas Revolucionarios de Colombia (FARC) 39
- Harakat Al-Muqawama Al-Islamia (Hamas) 40
- Hezbollah 42
- Lashkar-e-Taliba 43

Footnotes 45

Bibliography 51

LIST OF FIGURES

Figure 1-1 IED Attack Continuum 4

Figure 2-1 Al-Qaida Structure Pre 9-11..........8

Figure 2-2 Hezbollah Structure as of 2008..........8

Figure 2-3 Al-Qaida Current Cell Structure 9

Figure 2-4 Al-Qaida’s Core Structure Post 9-11 9

LIST OF TABLES

Table 1-1 Research Variables 5

Table 3-1 Cyber Terrorism Appeals 19

Table 5-1 Terrorist Telephone Conversation 1 32

Table 5-2 Terrorist Telephone Conversation 2 32

Table 5-2 Terrorist Telephone Conversation 3 32

ACKNOWLEDGEMENTS

This thesis would not have been possible to finish if it were not for the support and dedication of both Colonel Jacob Graham and Dr. Peter Forster.

Chapter 1

Introduction

Over the last decade, digital technologies have been improving exponentially. Computers are getting faster, cellphones are gaining more features, and service providers are able to offer faster Internet speeds to their customers. These digital advances have positive and negative impacts on society. For example, terrorists are becoming aware of the advantages of using these technologies to achieve their goals of inflicting fear and harm into the world. While many of the technologies selected by terrorists are not the newest and greatest, they are still very effective for terrorists' purposes: recruitment, attack coordination, and command and control.

Digital technologies have influenced many aspects of life. Social networking, email, and chat rooms are indispensable to many. However, digital technologies are a doubled edged sword. While there are positive aspects, there are also negative aspects such as the use of digital technologies for terrorist activities. It is nearly impossible for technology producers to anticipate every dual use of their technology; there are too many to consider. Another problem is that many companies do not care what their products are being used for as long as they are being purchased and bringing in revenue. Some dual uses of technology are simply impossible to prevent, such as the use of a cellphone to detonate an improvised explosive device (IED) because cellphones are built to send and receive signals. Another use of cellphones, that was thought to be impossible at one point, is the use of cellphones for social networking and online shopping from distributers.

Over the past decade, social networking has become very popular due to its ability to enable people to communicate anywhere there is an internet connection and keep up friendships, relationships, and much more, such as plan vacations, keep up with their favorite bands (through the band's fan page), and share pictures. Along with the ability to communicate with friends, social networks are incorporating games and applications; enabled by both the demand and advancements in new digital technologies—allowing more complex applications to be written for the web.

Enterprises are using social networking tools like Facebook and Twitter to increase productivity and awareness. Enterprises that use social networking on their internal network have many benefits, such as collaboration and the publishing of public corporate information. Employees can communicate with each other using many social networks' built-in chat feature. This enhances corporate productivity because employees will not need to leave their desk to ask a question—they can just send the question over the social networking chat tool, allowing faster and more immediate communication than email.[1] Companies can also use it to publish information to customers and potential employees. Some examples of information that can be disseminated over social networking sites are information sessions, upcoming initiatives, and the opening of new branches of the enterprise. Thanks to all of these features, enterprises are able to increase productivity and more easily disseminate information.

Before the advent of 3G and 4G cellphones, the only way to access social networking sites was to sit down at a computer, either in a cybercafé or at home. Today, people can access social networking sites wherever they receive signal. Social networking sites have created applications that users can download to their phone to make it easier to access the site. Due to its popularity, the Facebook application comes pre-downloaded on many phones, including the popular Motorola Droid. Not only can one communicate with another person via social networking, people can find each other too. Facebook offers a "places" feature which allows users to share their personal locations. Many other companies have features that do this too—Google Latitude is one example. Therefore, the advent of 3G and 4G cellular technology has helped the advancement of social networking features.

Along with enabling social networking, digital technologies have also enabled distribution channels. Distribution channels are the channels that consumers can go through to obtain items. The Internet has enabled major distributors, like Wal-Mart and Sears, to have websites which consumers use to order supplies and get them shipped to various locations around the world. As cellular technology improved and cellphone consumers had the Internet on their phone, companies like Amazon and Newegg developed applications for smart phones that consumers could use to purchase items. The Amazon application not only uses the Internet but also the camera on cellphones. Consumers can take a picture of the barcode, or the item, and have the application search the Amazon database for items. This way, consumers can comparison shop while they are in a store. These advantages of technology have been used for terrorism. For example, the plane tickets for Mohammad Atta, the leader of the September 11 terrorist attacks, were purchased via the Internet; allowing him to utilize distribution channels through the use of digital technologies. [2]

Not only are terrorists using digital technologies to purchase materials online, but they are using them to enhance their ability for recruitment, attack coordination, and command and control. Cellphones are used for communication, Google Earth supplies tactical maps, and virtual worlds enhance organization, financing, attack rehearsal, and coordination. There are many different digital technologies that terrorists utilize from recruitment to attack. As digital technologies enabled social networking and distribution channels, they also enabled terrorists to use them, but for different purposes.

Colleen LaRose, a Pennsylvania woman also known as *Jihad Jane*, used digital technologies to aid herself and her co-conspirators in a plot to assassinate Swedish citizen and artist Lars Vilks. The reason behind the plot was because Vilks, in 2007, drew a comic that depicted the Prophet Muhammad as a dog; angering many Muslims to the point of a hit being ordered on him. Through the Internet, *Jihad Jane* received instructions to kill Vilks, but never succeeded; only starting the plot to accomplish the task. By using the Internet, she and her co-conspirators were able to establish relationships with each other as well as communicate their plans which included, “martyring themselves, soliciting funds for terrorists, soliciting passports, and avoiding travel restrictions to wage violent Jihad.”[3] The use of digital technologies aided and abetted her ability to organize the terrorist plot against the Swedish resident as well as recruit other members into the *Jihad*. This is just one example of many where digital technologies have aided terrorists in recruiting new members and coordinate the attack.

For many years, counter-terrorist agencies have been trying to understand terrorists with some success. However, it always seems as if the terrorists are always one step ahead. This paper aims to explore how the digital technologies have influenced three crucial stages of terrorism: recruitment, attack coordination, and command and control.

This study is valuable because terrorism continues to effect the United States and its allies in the 21st century. Every day, terrorists are developing new ways to harm and inflict fear in the world, and their attack methods are extremely effective against Western technology; IED finding robots and drones for example. With only a few dollars' worth of explosives and a garage door opener, terrorists are capable of killing and destroying anything that is in range of the IED.[4] To combat the evolving terrorist threat that is embracing digital technologies, we must understand how terrorists are using digital technologies for the various aspects within the IED Attack Continuum provides on opportunity.

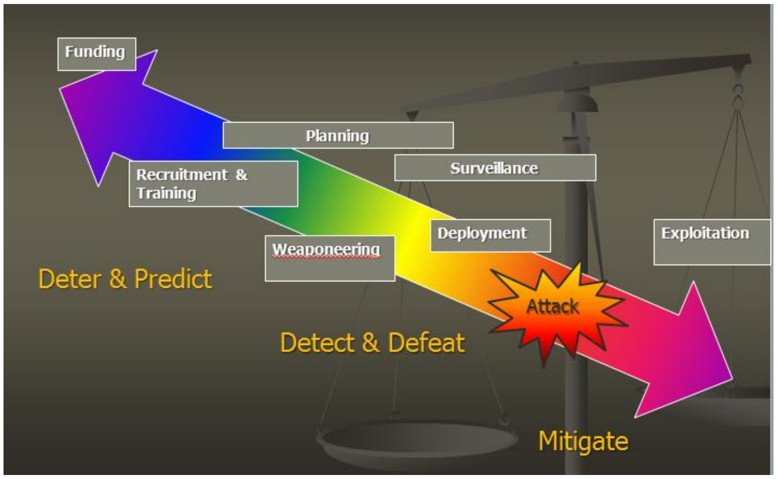

Figure 1-1 IED Attack Continuum[5]

As seen in the figure, different steps in terrorism lie at different ends of the spectrum. By dissecting the continuum, we can begin to understand the impact of digital technologies. The variables in the model are funding, recruitment and training, planning, weaponeering, surveillance, deployment, attack, and exploitation. Each of these will be analyzed in different sections of this study; recruitment and training in the recruitment section; funding, planning, surveillance, and weaponeering in the attack coordination section; and deployment, attack, and exploitation in the command and control section. Previously, each aspect of the IED attack continuum had to be conducted face to face. Now they are conducted through the use of digital technologies. This paper will help discover which technologies are being used in each stage. To discover how terrorists are using digital technologies against us, this paper will undertake a qualitative research study using journal articles, interviews, and manuscripts to explore how digital technologies have impacted these processes. Using the IED continuum as a model for understanding terrorist methodology, the research will focus on the following variables:

Table 1-1 Research Variables

1. Recruitment
2. Attack Coordination
3. Command and Control

Each of these variables is impacted by the use of digital technologies. Recruitment is defined as, "gathering supporters to play a more active role in supporting terrorist activities or causes."[6] Attack coordination is the communication of critical information between various groups and members regarding the terrorist event as well as the ability to cooperate quickly during the event.[7] Command and control is defined arranging various aspects into a single unit to function in environments where attacks are carried out.[8] These definitions are not the only meaning of the term, but it is the definition that will be used for the remainder of the paper.

Once the research is conducted and compiled, it will be clear how terrorists are using digital technologies to enable recruitment, attack coordination, and command and control. To offer a context, this paper will briefly discuss the evolution of terrorism from 2000-2011; exploring how terrorist cell structure is changing and how terrorism has become more of a global nature. Following this section, the paper will explore how terrorist are using digital technologies for three fundamental processes recruitment, attack coordination, and command and control. The paper will then conclude with a summary of key findings and final thoughts. To help the reader understand a little about the various terrorists that are mentioned, there will be a biography section at the end.

Defining digital technologies is an important part of this paper. Digital technologies are computer based electronics that can store, process, and transmit and receive data. These include: cellphones, satellites, and most importantly, the computers, servers, routers, and switches that comprise the Internet. Another key definition to define is terrorism, but there is no single definition. For the purposes of this paper, terrorism will be defined by the definition included in Title 22 of the United States Code, Section 2656f(d). Title 22 defines terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience.”[9] There are also many goals of terrorism, but Mariusz Dabrowski from Towson University identifies a goal that encompasses most goals: to instill “fear, panic, and instability through the populace.”[10] These definitions provide a foundation from which to delve into the how terrorism has evolved and how digital technologies are being used.

Chapter 2

Brief Evolution of Terrorism: From Turn of Century

For the past decade, violent Islamists extremism (VIE) as espoused by al-Qaeda and its Associated Movements (AQAM) has evolved to become more of a loosely interconnected organization that can operate on an international level. A terrorist organization is a “social unit deliberately constructed and managed to achieve rational cooperation as it pursues specific goals.”[11] Over the past decade, the Internet has allowed al-Qaida to evolve from hierarchical organizations with designated leaders to one with a less hierarchical and more loosely interconnected, semi-independent cells with no one command hierarchy.[12] Groups sharing a similar ideology were able to evolve into these loosely interconnected cells because digital technologies have reduced transmission time and cost of communicating as well as increased, in both variety and complexity, the types of information that can be shared.[13] No longer do messages need to be sent by messenger. They can be sent through text messaging, email, and chat clients.

With the increased capabilities for communications and information sharing, geographic location of cells is irrelevant. Now, “small and previously isolated groups or individuals can communicate, collaborate and link up to conduct coordinated actions as never before.”[14] Also terrorist groups are not only connecting within their group but they are also connecting with members of other terrorist organizations.[15] By terrorist groups becoming more decentralized, it makes it harder for counterterrorism organizations to identify, observe, infiltrate, and monitor.[16]

Before September 11, 2001, al-Qaida’s cell structure consisted of four layers. (See figure 2-1).

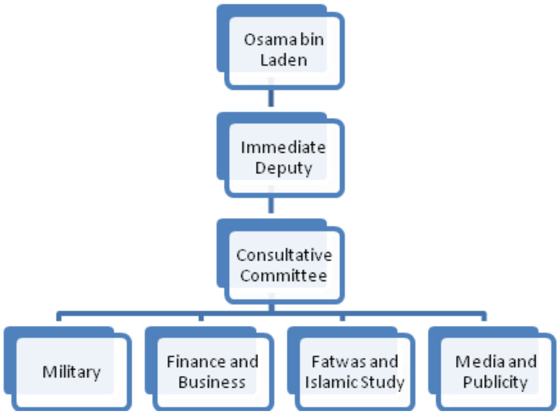

Figure 2-1 Al-Qaida Structure Pre 9-11

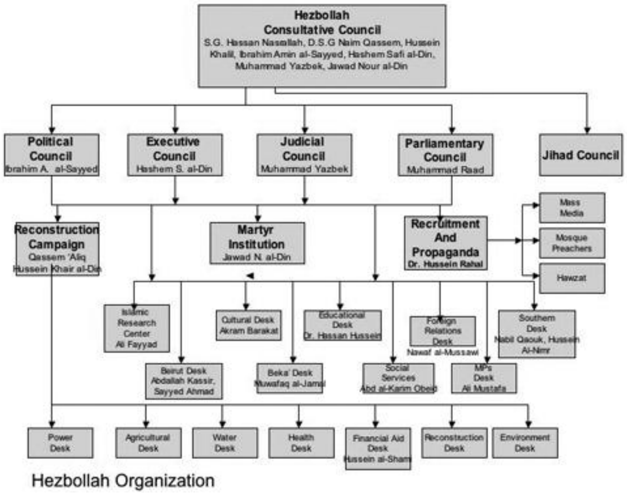
Hezbollah Consultative Council
S.G. Hassan Nasrallah, D.S.G Naim Qassem, Hussein Khalil, Ibrahim Amin al-Sayyed, Hashem Safi al-Din, Muhammad Yazbek, Jawad Nour al-Din
Political Council Ibrahim A. al-Sayyed
Executive Council Hashem S. al-Din
Judicial Council Muhammad Yazbek
Parliamentary Council Muhammad Raad
Jihad Council
Reconstruction Campaign Qassem 'Aliq Hussein Khair al-Din
Martyr Institution Jawad N. al-Din
Recruitment And Propaganda Dr. Hussein Rahal
Mass Media
Mosque Preachers
Hawzat
Islamic Research Center Ali Fayyad
Cultural Desk Akram Barakat
Educational Desk Dr. Hassan Hussein
Foreign Relations Desk Nawaf al-Mussawi
Southern Desk Nabil Qaouk, Hussein Al-Nimr
Beirut Desk Abdallah Kassir, Sayyed Ahmad
Beka' Desk Muwafaq al-Jamal
Social Services Abd al-Karim Obeid
MPs Desk Ali Mustafa
Power Desk
Agricultural Desk
Water Desk
Health Desk
Financial Aid Desk Hussein al-Sham
Reconstuction Desk
Environment Desk
Hezbollah Organization

Figure 2-2 Hezbollah Structure as of 2008[17]

Comparing the terrorist organizations, it can be seen that the two organizations are similar except that Hezbollah, being a political party in Lebanon, has a larger, more compartmentalized organization that is responsible for taking care of the citizens. Instead of just having the three main focus areas reconstruction, martyr, and recruitment and propaganda, they have separated those groups into smaller, more focused areas such as agriculture, water, and health.

As seen in the pre 9-11 al-Qaeda organizational chart, the top layer was Osama bin Laden. Directly below his was an immediate deputy or emir, who was Abu Ayoub al-Iraqi at that time. Next was the consultative committee comprised of Soviet-Afghan war veterans who swore allegiance to bin

Laden. Two members of this committee were al-Zawahiri and Mohammed Atef. At the bottom were four operational committees: military, finance and business, fatwas and Islamic study, and media and publicity.[18] This structure is a strict hierarchy. Since the September 11 attacks in 2001, Al-Qaida has become a “decentralized organization relying on either semi-autonomous cells or affiliated groups.”[19]

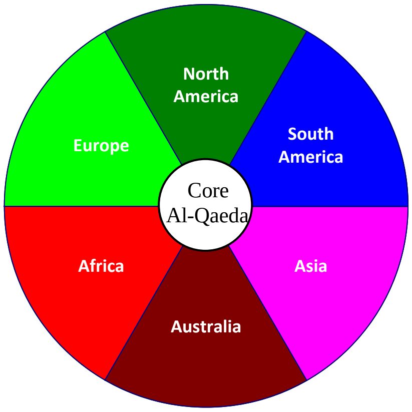

Figure 2-3 Al-Qaida Current Cell Structure

While al-Qaeda does still have a central core, it now has branches that are spread across the World, instead of being located in the same geographic region. The central core is still a hierarchical organization and is displayed in figure 2-4.

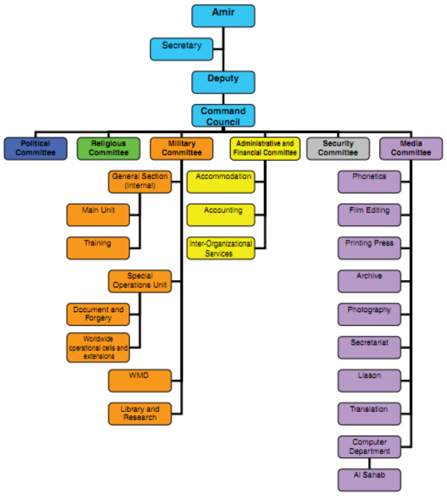

Figure 2-4 Al-Qaida’s Core Structure Post 9-11[20]

This figure shows how the core of al-Qaida is still a hierarchical organization. It has its leader, the Amir, second in command, Deputy, and the Command Regent whom each of the divisions report to. Each division has its own purpose within the organization. As seen in comparison with the pre 9-11 and post 9-11 structure, al-Qaida has gone from a strictly hierarchical organization to a decentralized organization with cells located on the major continents around the world.

Chapter 3

Recruitment and Training

Digital technologies, especially the Internet, aid terrorists in recruiting individuals to their cause by influencing “supporters to play a more active role in supporting terrorist activities or causes,”[21] and are largely responsible for building the armies of modern terrorism.[22] In attempt to recruit new members, terrorist organizations target three types of audiences: current and potential supporters, the international community, and their enemies. One way terrorists are appealing to current and potential supporters is through the sale of merchandise items, such as shirts and flags. To reach out to the international community, terrorist websites include background information regarding their organization in multiple languages. Finally, to appeal to the enemy, terrorists include threats and warnings.[23] However, before a supporter becomes a terrorist, they must go through the radicalization process.

The radicalization process consists of four steps: pre-radicalization, self-identification, indoctrination, and jihadization. Pre-radicalization is the “point of origin for individuals before they began this progression.”[24] Many of the involved individuals were ordinary citizens who had little or no criminal background and had regular jobs. The next step, self-identification is where “individuals, influenced by both internal and external factors, begin to explore Salafi Islam.”[25] In this step the individual starts to disassociate with their previous identity and start associating themselves with individuals who have the same radical ideologies, adopting them as their own. The third step is indoctrination where “an individual progressively intensifies his belief, wholly adopts jihadi-Salafi ideology and concludes that the conditions and circumstances exist where action is required to support and further the cause.”[26] In this step the individual is no longer interested in goals like getting a good job or earning money but in goals that achieve the “greater good.” The final stage, jihadization, is where "members accept their individual duty to participate in jihad and designate themselves holy warriors."[27] This phase is where individuals can see themselves as a part of a hardened group that will carry out an attack on a target.

One of the first terrorist organizations to appeal to multiple audiences through the World Wide Web (WWW) was Hezbollah, who established multi-lingual, interconnected websites. [28] This allowed not only current, Arabic speaking supporters, but also the international, English speaking community to be able to understand Hezbollah's message. Hezbollah's website, al-Manar, is used, "to indoctrinate the minds of young and old alike with the idea that those who seek martyrdom will be rewarded with more pleasure than can ever be achieved during this earthly lifetime."[29] Al-Manar is the official website for the television station al-Manar, and has been successful in indoctrinating Muslims beyond the Middle East region with its approximate $10 million annual budget.[30] [31]

To gain supporters, terrorist organizations must make it seem as if they are the ones who are being repressed and that they are the good guys trying to make the world better. An example of this would be an attempted suicide attack on a United States installation in Iraq. The suicide bomber detonated his belt too early, and instead of killing Americans, killed a number of Iraqis. Before the United States could spread pamphlets detailing the attack, insurgents spread the word through the Internet that the United States carried out a missile strike on the Iraqis, causing a riot that almost got out of hand near a United States installation.[32] Al-Jama'a al-Salafiya, an Iraqi Sunni resistance anti-US organization, claimed responsibility for many terrorist attacks on United States forces in Iraq through the use of videos on their website that show the attack being conducted.[33] The Ansar al Sunna terrorist organization posted multiple propaganda videos on its website claiming over 200 attacks with over 1000 people killed. In 2004, one year after officially announcing their formation, they became well-known after their posting of the beheading of Nick Berg, an American citizen.[34] With the ability for terrorists to spread propaganda quickly through the use of the Internet, the number of terrorist websites has climbed from fewer than a dozen in 1997 to close to 5000 in 2006.[35]

Originally, terrorist propaganda was spread through paper pamphlets and word of mouth. With the evolution of digital technologies, such as the Internet, terrorists are now able to reach a more diverse audience at the speed of light. [36] Terrorists use various types of video for propaganda purposes: produced, operational, hostage, statement, tribute, internal training, and instructional. Produced videos are videos that vary between one and two hours and include a wide variety of material: news footage and group member statements for example.[37] An operational video varies between one and eight minutes and includes clips of the attack. Hostage videos do not have a set length because they consist of a live video feed that are used to show what is happening and increase media attention towards the capturers. Statement videos are used to boost terrorist morale and often detail mid to senior level members of the organization. Tribute videos are used to praise important group members who have died or when a large number of members are killed by counterinsurgency forces. Internal training videos and other instructional videos are used to train members in certain skill sets.[38]

Along with differing types of Jihadi videos, within each category, varying techniques are used to convey the video to different audiences. For example, the suicide bombers of the Riyadh terrorist attack on May 12, 2003 recorded their wills, which were later posted on the Internet in October 2003, to convey different messages; some of the wills were in English while some were in Arabic with their dialogue conveying the differing messages.[39] The videos aimed at the Muslim population were trying to, “raise sympathy, support, and understanding while relying on religious sources,” while the videos aimed at the Americans conveyed a message of extreme hate for the Americans and any supporters of America. [40]

In an attempt to gain more followers, terrorist groups are claiming responsibility for everything that goes wrong. For example, the Northeast and Midwest blackout of 2003 in the United States and Canada was claimed by al-Qaida in what is known to the terrorist community as “Operation Quick Lightning in the Land of the Tyrant of this Generation.”[41] The true cause of the blackout was a tree that had not been trimmed, and a power line that, on a warm summer day, sagged till it came too close to the tree causing a fault. This led to many other failures that caused the blackout to expand to cover from the Midwest, Northeast, and into Canada.[42]Another way al-Qaida has used the Internet to gather more followers is through their Center for Islamic Studies and Research. This group publishes Swat al-Jihad or the Voice of Jihad, a biweekly magazine that preaches, "violence as Jihad's only way."[43]

The Committee for the Commemoration of Martyrs of the Global Islamic Campaign published an online application which allows people to sign up to martyr themselves. They have received approximately 10,000 interested participants, each with at least one of the three options they can commit martyrdom against:

- "occupiers of the holy sites,
- occupiers of Jerusalem,
- or carrying out the death sentence of the infidel Selman Rushdie[*]."[44]

Following September 11, 2001, thousands of volunteers flocked to join al-Qaida and take their part in terrorism.[45] Events like this that are successful create a rush of "jihaditism" (Jihadi patriotism). With the vast media network today, terrorists do not have to produce any propaganda films (other than the wills of the terrorists) following the terrorist attack—they can just rely on media sites like Fox and CNN to broadcast it for them. It is important to reiterate the differences between violent extremism and radicalization. Extremism is the, "radical views, philosophy, and rhetoric that is highly advertised and becoming more and more fashionable among young Muslims in the West."[46] Radicalization a process in which a terrorist becomes a member of the Jihad; pre-radicalization, self-identification, indoctrination, and jihadization.[47] It is estimated that approximately 500,000 Muslims (4%) have become radicalized.[48]

To recruit younger generations, terrorists are using Jihadi websites to publish comic-book style stories that attract childrens' attention while encouraging them to become martyrs. One well-known group that uses this tactic is Hamas.[49] Al-Feteh, Hamas's website, includes propaganda aimed at young

[*] Rushdie is a British journalist who has been hiding from terrorist groups for over eight years because of his novel *The Satanic Verses* which blasphemes Islam.

children also includes graphics, children's songs, colorful drawings, and a list of suicide bombers. Also on this website, Hamas posts the wills of several suicide bombers, including the suicide bomber who bombed the teen club Dolphinarium on June 1, 2001 in Tel Aviv, Israel. [50] Terrorist are also disseminating Jihadi based video games and videos; for example, "Special Force," developed by Hezbollah Central Internet Bureau.[51] In-game, players take up the role of a Jihadi for Hezbollah in actual military operations that took place against Israel.[52] The game also has the ability for players to conduct target practice on the Israeli Prime Minister.[53] Tawhid Wal Jihad, led by Abu Musab al-Zarqawi, hosted an al-Qaida video teaching young boys techniques used by terrorists; "commando training, marching in formation, running military-style obstacle course, rappelling, and reading written statements in Arabic."[54] With all of this material available to young children, studies have been conducted on its effect. Dr. Massalha, a psychologist in Palestine who studied children between the ages of six and eleven reported that over 50 percent of children exposed to this material in the Middle East dream of becoming suicide bombers wearing explosive belts.[55] At this age, children are very vulnerable to being brainwashed. It was reported that during the invasion of Iraq, over 170 Iraqi juveniles were detained for engaging in combat with Allied Forces.[56] These children that are being trained as terrorists are being trained because children are a low-cost method to create an army as well as advantages when fighting forces like the United States who do not shoot back at children (or do not inspect them as closely at checkpoints).[57] The use of children also attracts much wanted media attention by terrorist groups.[58]

Terrorists recognize that the Internet provides a way for them to ease lonely people's loneliness by connecting them with people who have commonalities.[59] Potential supporters do not always need to contact the terrorist organization to show their interest, instead, through the use of website monitoring, terrorists are able to capture information about the individuals who are surfing their website, and once deemed a potential supporter, the terrorist organization contacts them. [60] [61] For example, Colleen LaRose reached out over the Internet and recruited five co-conspirators to help support the Jihad.

Together, they established relationships and discussed plans to martyr themselves as well as raise funds for terrorism.[62] Due to the publicized success of recruiting members over the Internet, many groups realize its importance and will attempt to recruit members of their own via the Internet.

Another example of someone being recruited through the use of digital technologies is Ziyad Khalil. He attended Columbia College in Missouri as a computer science major. On campus, he became a Muslim activist and developed several websites that supported Hamas. With his support for terrorist groups and with the help of the Internet, Bin Laden's lieutenants discovered him and recruited him as al-Qaida's procurement officer in the United States. His job involved purchasing equipment such as: satellite telephones, computers, and other electronic surveillance technologies until his arrest on December 29, 2001 by Jordanian officials.[63] [64]

The Internet houses vast amounts of information that are used by terrorists to increase their knowledge of terrorist activities such as operations and training that is disseminated through various channels such as chat rooms and websites. In December 2004, an online chat room on a terrorist website contained a twenty-six minute video with instructions on how to make a suicide bomb. The sections of the video included: required materials, instructions for assembly and mounting the suicide belt, and testing the destructive impact of the belt. Not only did the video contain information about how to create the bomb, but it also included a demonstration of the suicide belt's use on a model bus filled with passengers.[65] The passengers on the bus were not real people, but dummies. This chat room did not create an interactive environment for terrorists and was just a passive chat room where one could read and watch material.

Along with chat rooms, there are many handbooks that are used by terrorists to educate other terrorists in how to create a variety of weapons ranging from poisons, to conventional bombs, to nuclear and biological weapons, to planning assassinations, and all are accessible from different terrorist websites. *The Terrorist's Handbook* and the *Anarchist Cookbook* contain detailed instructions on how to make a wide variety of bombs, while the *Mujahedeen Poisons Handbook* contains instructions about how to make various homemade poisons, poisonous gases, and other deadly materials.[66] The *Encyclopedia of Jihad* contains instructions about how to establish an underground organization as well as how to execute attacks, and if the terrorist is interested in planning an assassination or anti-surveillance, he can reference the *Sabotage Handbook* which contains different methods for this.[67] The *Encyclopedia of Preparation* contains a large variety of methods ranging from kidnapping officials to constructing nuclear devices.[68] The Al Battar Training Camp publishes a bimonthly online magazine that contains a variety of articles ranging from cell organization and management to weapons training, to physical fitness, to wilderness survival. Some of the issues included instructions on how to conduct kidnappings, negotiate hostage releases, and conduct surveillance.[69] *The Art of Kidnapping—The Best and Quickest Way of Kidnapping Americans* includes information for "planning raids, how to choose members for the support crews, general rules for these crews to follow, observation points, kidnapping suggestions, and methods of capturing Americans."[70]

The websites housing these manuals require little technical knowledge to create.[71] A typical website has information regarding the "history of the group; biographies of its leaders, founders, heroes, and commanders; information on the political, religious, or ideological aims of the organization; and news bulletins and updates."[72] These are used to keep supporters up to date on the most recent activities of the group. Because terrorist websites are constantly being taken down by activists, Internet Service Providers (ISP), and counterterrorism organizations, several terrorists groups have moved to short life websites that are only used for communication purposes. When a short life website is created, members of that group are alerted via an encrypted email with its location, and once they are done downloading the information, the website disappears without counterterrorism organizations becoming aware of its existence. This method is effective because it decreases the likelihood that counterterrorism organizations will be able to track the IP address and physically locate the site.[73] Disrupting websites is counterproductive because it requires counter terrorist organizations to use resources to locate the new websites that opened in place of the one that was shutdown. If they did not shutdown the website, they could just use resources to monitor the website to find out who is accessing the site and what materials are being used to train terrorists; allowing them to take countermeasures against the methods being taught to the terrorists.

Today, to continue the war with the United States, websites are used as al-Qaida's central strategic tool.[74] Al-Qaida uses its websites to connect with and disseminate information to supporters and sympathizers around the world.[75] Its websites have also established portals through which interested supporters can connect to the group. Supporters can view online training through the use of computer based training (CBT). The CBT lessons detail instructions on how to use weapons and create and deploy bombs.[76] Along with CBT lessons, al-Qaida has a library site where supporters can read over 3,000 books and monographs written by respected Jihadi philosophers.[77] Al-Qaida also publishes several magazines, outlining instructions for, "communicating with cell members, defining tactics and procedures, and constructing explosives, among other topics."[78] In May of 2004, al-Qaida operatives in Saudi Arabia posted on their website detailed plans on how to assassinate Prince Nayef bin Abdel Aziz, Saudi Arabia's Minister of the Interior.[79] The plot was unsuccessful because Prince Nayef bin Abdel Aziz suspected that his security plans had been blown so he did not proceed to his secure house.[80] If he had, there is a good chance that the attack would have been successful.

HAMAS is another terrorist group that has an Internet presence and uses it for a "Military Academy" that offers fourteen lessons in bomb making as well as instructions on how to make rockets and light aircraft. The goal of this campaign is to increase the number of its supporters who know how to make bombs.[81]

Beyond training, others have sought to enhance their comrades understanding of the Internet's power. Irhabi 007, Younis Tsouli from West London, was a cyber terrorist who used the internet to train other cyber jihadists on how they can use their computer for terrorism by posting a "Seminar on Hacking Websites" onto the Ekhlas forum.[82] Irhabi is the Arabic word for terrorist while 007 is a reference to the James Bond.[83] The message was twenty pages and included information on how to hack and listed vulnerable websites where media could be uploaded. [84] [85] Training on how to hack has become very popular among terrorists because of its ability to inflict "mass hysteria and economic fallout that can be detrimental to global economy."[86]

While there have not been any significant cyber terrorist attacks, the first recorded use of cyber terrorism was a denial of service (DoS) attack by the Tamil Tigers against Sri Lankan embassies around the world, cyber-terrorism remains a threat to be considered. [87] The term cyber terrorism varies widely without one sole definition. The National Infrastructure Protection Center (NIPC) defines cyber terrorism as, "a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies."[88] Special Agent of the FBI, Mark Pollitt, defines cyber terrorism as the, "premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents."[89]

The improvement of digital technologies has increased the opportunities for terrorists to penetrate crucial commercial and financial systems as well as potentially disrupt the national infrastructure.[90] Terrorists are capable obtaining, altering, or destroying valuable data from many organizations, especially banks.[91] The threat of terrorists' ability to do this is undeniable, and a successful attempt to alter or destroy valuable data on a large scale could cause mass panic and the economy to crash.

Cyber terrorism appeals to modern terrorist because:

Table 3-1 Cyber Terrorism Appeals

1. It is cheaper and easier than traditional terrorist methods
2. It provides more anonymity than traditional terrorist methods (But it must ultimately be attributable to be terrorism)
3. The variety and number of targets are enormous
4. Attacks can be launched from a distance
5. It can potentially harm more people than a traditional terrorist attack[92]

An aspect of cyber terrorism that is not appealing to terrorists is the ability for anti-terrorism organizations to data mine. This data mining could range from monitoring terrorist communications to extracting information about the group to discovering how an attack is going to be conducted.

Even though cyber terrorism is a large concern for many countries, few terrorist organizations have used cyber terrorism. They have, however, shown an interest in using the Internet as a weapon and a target.[93] The Internet has been approved for use by radical Muslim terrorists by Sheik Abdul Aziz al-Alshaikh through his "blessing;" causing several Saudi hackers to attempt to hack FBI and Pentagon Web sites.[94]

The Muslim Hackers Club is a group of cyber terrorists whose goals is to develop software tools, distribute them, and conduct cyber-attacks. The club operates a website that has tutorials on how to create and deploy various cyber terrorism weapons such as viruses. It also provides information on how to devise hacker stratagems and how to conduct network sabotage. This website also contains links to United States sites that disclose sensitive information that the United States Secret Service uses for code names and radio frequencies.[95] To date, there has not been any evidence that their material has successfully orchestrated a major cyber-attack on the United States.

While recruiting new members, terrorists reach out to current and potential supporters, international community, and their enemies. Each audience is targeted in different ways with different goals in mind. Once they reach out to potential supporters, those who are willing will go through a four step radicalization stage: pre-radicalization, self-identification, indoctrination, and jihadization. Those who are interested in learning more about a specific terrorist group can refer to the organizations' websites. Terrorist websites are used to make the terrorists seem repressed through making a terrorist attack seem necessary to respond to United States actions. Through using the websites, information about a “United States attack on citizens”[†] spreads like wildfire and causes citizens to riot at the nearest U.S. base. Terrorists’ use of the Internet has vastly helped terrorists get their message out to the public and increase support for their cause.

[†] Previously discussed terrorist who detonated his belt too early and killed Iraqi citizens instead of United States personnel.

Chapter 4

Attack Coordination

Terrorists are using digital technologies to coordinate attacks among the group members and between groups. Digital technologies positively enhance their interactive planning and communication, and greatly increase the likelihood of a successful attack with maximum impact. Terrorists use digital technologies for fundraising, surveillance, and weaponeering. This section is going to explore each of these factors and what technologies are being to coordinate attacks. To do this, terrorists need to obtain funds, gather information about the target, and determine which weapons are going to be used for the attack.

Acquisition of funds is critical to any terrorist organization. One way terrorists obtain funds is through the use of virtual worlds using in-game currency. This is done by first buying virtual currency with real money, then conducting in-game transactions using the in-game currency, and finally converting the in-game currency back into real cash.[96] For example, John just started playing Second Life. He converted $100 United States Dollars (USD) into about 25,000 Linden Dollars (L$).[‡] Now, John uses those $25,000 L$ to buy an island and build a house on it. After he has completed the house, the land is worth $30,000 L$. He then sells the land, converts the $30,000 L$ back to USD with a $20 USD profit. The conversion rate fluctuates using the stock exchange model.[97] The exchanges are not monitored so if there is a problem with the exchange or something strange is happening, the user must contact Linden Laboratory. This model allows anyone to make money by buying while low and selling high in a virtual environment. An example of a case where large sums of money have been made in Second Life is a woman (who wishes to remain anonymous) who has virtual currency holdings that are

[‡] Approximate exchange rate on 31 March 2011

worth $250,000 in real USD. However, all of her money is in virtual property.[98] This woman has built her company around buying and selling Second Life property. This is one method that the terrorists could use to raise money.

In addition to virtual worlds, terrorists engage in raising funds via the use of Jihadi websites and charity fronts. Jihadi websites can be utilized for fundraising through the request for user donations or subscriptions.[99] On several terrorist websites, terrorist groups have also been known to post bank account numbers into which people can deposit funds. Depending on the group, these numbers change on a daily basis.[100] Another use of Jihadi websites is for online stores where items such as books, audio and video tapes, flags, and t-shirts are sold.[101] Not only are terrorist groups asking for supporters to purchase merchandise and donate funds, but terrorist groups are also asking for the donation of computers and accessories.[102]

On its website, Hezbollah allows supporters to sponsor a Jihadi in various ways. For just $12,000 a year, supporters can sponsor an injured Jihadi operative. Supporters also have the option to sponsor the orphan of a martyr for $360 a year with the additional option of donating $300 or more per year to educate that orphan. If someone is interested in sponsoring the widow of a martyr, $300 a year is needed.[103] Another example of a terrorist group using their website for fundraising is the Chechens. They use their website to post bank account numbers; one account was located in the United States.[104] A third example is the Islamic Assembly of North America (IANA), which sold language videos to teach people Arabic.[105]

The use of charities is also a popular method that terrorists can use to obtain funds. Many of the terrorist-funding charities also legitimately provide aid and support to the proposed cause. However, not all of the money goes to the cause—some is funneled to a terrorist organization.[106] Four charities that were shut down for this reason are the Holy Land Foundation for Relief and Development (HLF), Benevolence International Foundation, Global Relief Foundation, and Al-Harmain Foundation.[107] These charities were able to obtain donations through wire transfers, credit cards, donations of stocks, and regular bank deduction, as the Global Relief Foundation had before it was shut down.[108] In 2001, it was reported that the Global Relief Foundation raised more than $5 million in the United States. The exact amount of money that was funneled off for terrorism is unknown but it is estimated to be greater than $250,000.[109] Al-Qaida heavily depends on its global fundraising network of donations, charities, and non-governmental organizations. It has also used Internet-based chat rooms and forums to solicit requests for funds.[110]

The use of digital technologies has allowed terrorist organizations to receive funds from the use of online donations, merchandise sales, and charitable contributions. Through the use of the Internet, many terrorist groups have been able to raise large sums of money to support their cause. IANA was able to procure $3 million from the sale of its language lessons.[111] While this is not the largest sum of money related to terrorism, any small amount furthers their cause; including intelligence gathering.

Surveillance and intelligence gathering are another important area where terrorists have extended into the virtual environment. Attack coordination relies on planning through the gathering of information about the target. Terrorists can collect this information through the use of data mining tools as well as open source satellite imagery and photos. Data mining refers to the "terrorist's use of the Internet to collect and assemble information about specific target opportunities."[112] Facebook and Twitter are two data mining tools that allow terrorists to research an individual or organization through looking at information posted by the individual or their friends. Many open source tools are available to facilitate data mining. These include search engines, email distribution lists, and chat and discussion groups.[113] By using the Internet without hacking websites, it is possible for terrorists to gather 80% or more of the information they require about their target.[114] This information includes schedules and physical locations of targets such as transportation facilities, nuclear power plants, airports, public buildings, shipping ports, shipping activity, infrastructure information, economic data, and building maps. [115] [116] A captured al-Qaida computer contained documents downloaded from the Internet detailing engineering and structural features of a dam that allowed al-Qaida to simulate the effects of different catastrophic failures.[117]

In addition to operational information about a target, terrorists can also obtain information about the counterterrorism practices at the target. One report regarding Cincinnati's airport, revealed that "contraband slipped through over 50 percent of the time." [118] With this information, terrorists can use this airport as a staging area for getting materials into the air transportation system. Many companies also have information on their website detailing "the physical location of backup facilities, the number of people working at specific facilities, detailed information about wired and wireless networks, and specifications on ventilation, air conditions, and elevator systems."[119] The Nevada State Government website contained information on how it transported nuclear material, including the highways, railways, and weapons that can be used to attack these shipments.[120] The Nevada State Government saves the potential terrorists a great deal of time searching for information, since it has provided them with almost all of the information they need.

To supplement data mining, terrorists use surveillance to scout out weaknesses in a target and learn as much as they can about it. One way target surveillance can be conducted using digital technologies is through the use of applications like Google Earth, Google Maps, and Microsoft Virtual Earth. Some of the greatest benefits of Google Earth and Google Maps are its user friendliness and free access nature. Google Earth allows users to explore every nook and cranny on the Earth, some even in three dimensions. The three dimensional buildings are mostly in large, well-known cities like New York and Shanghai, but some are of well-known buildings in rural settings. Along with the ability to view buildings in 3D, Google Earth allows users to overlay several different features such as trees, weather, and street view—allowing users to view actual pictures of the area.

Google Earth also provides navigation tools that can be used by the terrorist to plan their escape route from the target after the attack has happened and how to get to the target.[121] Google Maps has the navigation feature, and also includes the ability for users to obtain traffic information. By having traffic information, terrorists can evaluate traffic patterns on certain roads at particular times of the day, allowing them to find a better escape route or determine when to carry out an attack to cause maximum panic and harm.

Information collection is an important aspect of organization. Digital technologies have aided terrorists' organizations in data mining and surveillance. Also, due to the amount of information companies and individuals post on their website, terrorists are able to obtain crucial information quickly. Digital technologies have not only helped terrorists collect information, but also helped them share information and communicate within their group and with their supporters.

Shared information is not just about how to make weapons but is also used to share plans for potential terrorist attacks. On the Real Irish Republican Army's (RIRA) website, there was detailed information regarding Prince William's security detail during his attendance of St. Andrews University. This included information on his bodyguards, the electronic security system that was installed in his quarters, where Prince William could be located at a range that would allow for easy attack and where a potential attacker could hide during an operation.[122] The Revolutionary Armed Forces of Columbia's (FARC) website contains a "victim database" detailing information about the various millionaires in the country and instructions to abduct them immediately if ever encountered at an illegal roadblock.[123] Al-Mohager al-Islami has posted information to, "Jihadist e-group forums, both public and password protected, regarding locations and equipment of Untied States and British government installations in Kuwait, Qatar, and other areas. The information includes photos of embassies and living areas"[124] The terrorist attacks conducted at Sharm-el Sheikh and in London during 2005, were facilitated by training that was located on the Internet.[125]

Three months before the Madrid train bombings on March 11, 2004, the plans for the bombing were found on al-Qaida's website Global Islamic Media by researchers. Only after the attack were the documents analyzed in detail.[126] This attack could have been significantly reduced in casualties, if not prevented, if the authorities had taken the plans seriously.

Another crucial part of coordination is communication, both internally and externally. Today, digital technologies have allowed terrorists organizations to communicate securely and anonymously with other organizations and cells all around the world.[127] These technologies have not only reduced the costs of communications, but have also reduced their transmission time.[128] Digital technologies such as virtual worlds, email, chat rooms, Jihadi websites, cybercafés, and phones are used by terrorists for communication. Using different means of communication makes it difficult for anti-terrorism organizations to monitor terrorist communication because they may not have the resources to have an adequate number of people to monitor the various mediums of communication.

Today, virtual worlds have in-game chat clients as well as built-in VoIP capabilities that allow users to communicate internally.[129] The in-game chat clients are integral because they provide the ability for meetings that are more secure than secure chat rooms because the message is being sent internally on a private server instead of externally on a public server.[130] Within Second Life, users are able to hear other users' discussions as long as they are in the same general vicinity as them. The personal islands that were mentioned above can be set to private so only certain users are allowed in. Since no one, other than the allowed users, will be in the general vicinity, the owners of the island can have a private conversation that may or may not be monitored by Linen Laboratory.[131] The ability to hold private meetings, outside the ears of others, increases the likelihood of a successful attack happening.

Email has been extensively used by several terrorist organizations. One of the more popular reasons for using email is the anonymity it provides; if done properly. One layer of anonymity is the ability to specify a username and password used for the account.[132] Instead of having to use one's real name, they can pick something like foxbravo1. One-time email accounts also allow terrorists to achieve anonymity because after one message is sent, the account is deleted. This makes it difficult for counterterrorism organizations to monitor email traffic from an email address because once they flag a one-time email address, no traffic will ever come from it; requiring them to discover a new email address. For these purposes, Yahoo or Hotmail accounts are a favorite due to their ease of setting up.[133]

Other features of email also allow terrorists to hide email communications. The first method is called draft email boxes. For this method, terrorists set up an email account and distribute the username and password to several other members of the organization. One member then drafts an email but never sends it. Instead, he saves it as a draft and other group members log into the account and read the message. After all members have read it, the message is deleted. This allows terrorists to hide email communications since there is no email record because the email was never sent. A second way to hide email communications is to have a secure website with an internal email server. Every member of the organization would receive an email address, and as long as all emails stay within the site, it is very difficult to intercept or trace.[134]

Email encryption allows terrorists to communicate secretly, but openly. By using email encryption, emails are sent via the public domain but require a decryption key for them to become readable. There are many free, commercial programs, such as PGP and Enigmail, which can be used for email encryption.[135] The encryption of emails gives terrorists, “a much greater degree of operational security than other means of security.”[136]

In coordinating the September 11 attacks, al-Qaida operatives relied on the use of email. They used public Internet locations as well as public email addresses, helping to preserve anonymity for the attackers during their coordination phase.[137] This still works but there are additional techniques such as email encryption, encrypted chat rooms, and draft email boxes that terrorists use to achieve this anonymity since they know this method is being monitored closely.

Chat rooms provide another method of anonymous communications.[138] Terrorists use secure chat rooms that require a series of passwords to access. These chat rooms only allow trusted terrorist operatives access to the room.[139] In this way, secure chat rooms give terrorists anonymity and create a problem for counterterrorism organizations to trace and monitor these chat rooms.[140] For these chat rooms, security is preserved through the use of passwords.

Each of these methods provides their own level of security, and when combined, provides a very high degree of security. These methods of communicating allow terrorists to share the information they gathered during surveillance and determine which weapons will work the best for the plan, known as weaponeering.

Weaponeering is, "the process of determining the quantity of a specific type of lethal or nonlethal weapons required to achieve a specific level of damage to a given target, considering target vulnerability, weapons characteristics and effects, and delivery parameters."[141] One example of weaponeering comes from the information that the Nevada State Government posted. Because terrorists know that they are going to be defending against those weapons, they will need to select a different weapon that are not being defended against that will work to attack the convoy on either the highway, side roads, or railway.

The selection of the appropriate weapon is crucial for terrorists. By being able to select the appropriate weapon and yield, they will be able to inflict the maximum damage. However, to select the appropriate weapon and yield, terrorists must conduct research on the target. Unfortunately, with the aid of digital technologies, terrorists are able to obtain large sums of data on their target, increasing their ability to conduct successful weaponeering. This information gathered includes defenses at the targets, personnel, location, and much more that is crucial in planning an attack. David Headley, a member of Lashkar-e-Taliba conducted surveillance for the Mumbai attacks two years preceding the attacks. His surveillance, Headley took photos of the hotels to be attacked, photos of possible landing sites, and video of the Mumbai harbor. His extensive surveillance helped make the Mumbai attack so successful.[142]

Through the use of digital technologies, terrorists have been able to coordinate their attacks through funding, surveillance, and weaponeering. Digital technologies have not only improved their ability to organize but have made it easier because they no longer need to be in the same geographic region. They can organize across vast distances that were previously difficult and expensive before. With the use of Jihadi websites, terrorists can reach a wider, more diverse population. Since digital technologies have increased the ability for terrorists to organize, terrorists' abilities to implements different attack strategies have also increased.

Chapter 5

Command and Control

Over the years, terrorists have been able to improve their ability for command and control during attack exploitation. The attacks on Mumbai in 2008 represent a series of highly successful operations that effectively used digital technologies. This attack represented terrorist innovation and raised new concerns among counter-terrorist organizations globally.

Ten terrorists, from the Lashkar-e-Taliba (LeT) terrorist group based in Pakistan, were able to wreak havoc in the Indian financial capital Mumbai for three days.[143] They landed in Mumbai via the sea with the aid of a Global Positioning System (GPS) to determine the best location to land.[144] After landing, the attack started on November 26, 2008 and ended on November 29, 2008 with the death of nine terrorists and the capture of one.[145] Over the course of the attack, approximately 200 people were killed with hundreds injured.[146] The attack used various combinations of tactics that made them very difficult to stop.

The various methods used by the Mumbai terrorists helped increase their situational awareness, which is defined as "understanding the state of the environment."[147] One method was the monitoring of real time media coverage of the attack. This method allowed them to determine which tactics law enforcement were using; allowing them to compensate and change their tactics. Previously, to prevent this, power was cut off to the building; however with the terrorist's use of handheld devices, they were able to receive directions from their handlers in Pakistan.[148] The terrorists' handlers, running the operation from Pakistan, were using multiple open source venues, such as television, web, and social media to obtain information regarding anti-terrorism reaction to the attack as well as provide this information to the terrorists conducting the attack. [149]

During the attack, the Indian government intercepted phone conversations between the terrorists and their handlers depicting how the terrorists were able to obtain situational information through the use of monitoring live media and websites—allowing the remote handlers to be able to make decisions on where and how to mount their attacks, as well as who to kill in the process. The remote handlers' ability to do this greatly increased the ability for the terrorists to conduct the attack.[150] Below are some conversations that took place between the terrorists and their remote handlers in Pakistan.

Table 5-1 Terrorist Telephone Conversation 1

Handler:	"Everything is being recorded by the media. Inflict the maximum damage. Keep fighting. Don't be taken alive"[151]

Table 5-2 Terrorist Telephone Conversation 2

Handler:	"See, the media is saying that you guys are now in room no. 360 or 361. How did they come to know the room you guys are in? ... Is there a camera installed there? Switch off all the lights…If you spot a camera, fire on it…see, they should not know at any cost how many of you are in the hotel, what condition you are in, where you are, things like that…these will compromise your security and also our operation."
Terrorist:	"I don't know how it happened…I can't see a camera anywhere."[152]

The following phone conversation is able to show how the terrorists were able to use the Internet to obtain information on certain hostages. This information was then used to make a decision on whether or not to kill the hostage.

Table 5-2 Terrorist Telephone Conversation 3

Terrorist:	"He is saying his full name is K.R. Ramamoorthy."
Handler:	"K.R. Ramamoorthy. Who is he? … A designer … A professor … Yes, yes, I got it …" [The caller was doing an internet search on the name, and a result showed up a picture of Ramamoorthy] "… Okay, is he wearing glasses?" [The caller wanted to match the image on his computer with the man before the terrorists.]
Terrorist:	"He is not wearing glasses. Hey, where are your glasses?"
Handler:	"Is he bald from the front?"
Terrorist	"Yes, he is bald from the front …he is fat and he says he has got blood pressure problems"[153]

In this scenario, the terrorists were able to discover that one of the hostages, who survived the attack, was one of the top Indian business persons, K.R. Ramamoorthy.

Their use of digital technologies greatly enhanced their ability to prevent law enforcement from finding out where they were as well as which hostages they could use to try and ransom to gain more time. The confusion of the law enforcement helped the terrorists achieve the maximum damage.

Chapter 6

Conclusion

Information technology has changed how the world interacts. The change started with fall of the Berlin Wall.[154] After the wall fell, the world economy opened up and countries started working as a whole. The next major change to IT was the creation of the PC. [155] The PC started the transition from paper to digital media. The Internet's invention and release to the public changed the way business was conducted and the way people communicated. No longer do people have to drive three hours to attend a meeting. Now they can use VoIP or Telepresence to take part in the meeting from their office.

Overall, the digital technologies that have improved world commerce and communication have significantly aided terrorists; increasing their ability to organize both internally and externally allowing organizations to no longer stay within their own organization to organize, but to form coalitions with other organizations.[156] They share information with each other and thus help increase each other's knowledge and ability to conduct terrorist attacks.

In the past decade, terrorism has greatly evolved from using traditional means to using modern, conventional means. Digital technologies have made terrorist organizations harder to disrupt because there is no longer a sole leader of a group. When one person gets eliminated, communication will be routed to another person and someone will absorb their role. When a whole cell gets removed, that cell's responsibilities will either be transferred to another cell or they will be transferred to members who are going to replace the cell.

Recruitment has also become easier for terrorists. Terrorists use digital technologies to reach out to potential recruits that were previously unreachable—increasing the number of recruits gained. Technologies have also allowed for recruitment that is difficult to trace and discover. Every day, there are new and innovative ways for terrorists to recruit new members. However, by using digital technologies, it enables counter terrorism organizations to be able to more closely monitor terrorist recruitment activities (only after the method has been discovered).

Through the use of digital technologies, terrorists are able to obtain funds through the Internet, allowing for more supporters to donate money to the cause. Instead of having to send a check or cash, supporters can do a direct deposit into an account that is found on the terrorists' website or through merchandise purchasing. New technologies on the open market are not only used for their intended purposes, but are also used by terrorists for their goal. The intended purpose of a cell phone is to allow its users to communicate with each other across a vast distance, but the terrorists are using it as a remote detonator. For example, a cell phone was used as a remote detonator for an IED in Iraq.[157] Other technologies, such as encryption programs and improved and stronger algorithms, are being used to improve communication security which make it more difficult for counter terrorism organizations to monitor terrorist communications; making communications more secure for terrorists. However, some terrorist organizations use open source encryption algorithms that allow counter terrorism organizations to more easily crack the key.

Through the use of digital technologies, terrorists are able to communicate with remote sources before, during, and after an attack. As seen in Mumbai, the terrorists were able to obtain crucial information through the Internet and media that helped them conduct a successful attack and help prevent the law enforcement officials from being able to plan an assault on one location through the ability to know what the law enforcement officials knew, and then changing their location/tactic. The tactics that the terrorists used were impossible to stop. The only way that communication between the terrorists and their handlers could have been stopped was to cut power to the building, cell network, TV stations, as well as the satellites that were being used for the phone conversations. This combination of resources used by the terrorists helped to prevent Indian law enforcement from understanding the terrorist situation completely because the terrorists were using this information to adapt their tactics constantly.

Terrorism tactics change on a daily basis, and sometimes terrorists revert to decades old tactics. Therefore, there can never be enough research on terrorism. With the threats that terrorists pose to the United States and its allies, terrorist methods must be understood. Terrorists are constantly developing new and clever methods for organizing. These include, but are not limited to, recruitment and training, attack coordination, and command and control. This paper only includes a handful of the methods the terrorists have in their arsenal as well as paves the way for research into the other digital technologies that are being used as well as the new methods they have developed since this paper.

The methods that the terrorists are using to organize must be understood repetitious. They must be discovered and counter measures to it must be put into place. The threat of terrorism will never be over, but we can find how they are using these technologies and develop methods to counter them, and save American lives.

Appendix A

Terrorist Organizations

Al-Qaida

Al-Qaida was established in 1988 by Osama Bin Laden. The original members of al-Qaida were Arabs who fought in the Afghanistan-Soviet Union war. Its goal is to establish a pan-Islamic caliphate throughout the Muslim world. They also seek to unite Muslims around the world to fight the West, especially the United States. They are also interested in uniting Muslims to defeat Israel. In June 2001, they merged with the Egyptian Islamic Jihad (al-Jihad).

On September 11, 2001, 19 al-Qaida members hijacked and crashed four US commercial jets—two into the World Trade Centers in New York City, one into the Pentagon near Washington, D.C., and a fourth into a field in Shanksville, Pennsylvania—leaving nearly 3,000 people dead. They also directed the October 12, 2000 attack on the USS Cole in the port of Aden, Yemen, killing 17 US sailors and injuring another 39. The August 1998 bombings against US embassies in Nairobi, Kenya, and Dares Salaam, Tanzania, killing 224 people and injuring more than 5,000 were also conducted by al-Qaida. Since 2002, al-Qaida and affiliated groups have conducted attacks worldwide, including in Europe, North Africa, South Asia, Southeast Asia, and the Middle East.

In 2005, Bin Laden's deputy, Ayman al-Zawahiri, publicly claimed al-Qaida's involvement in the July 7, 2005 bombings in the United Kingdom. In 2006, al-Qaida was also planning to detonate explosives on 10 transatlantic flights originating from London's Heathrow airport, but it was foiled by British security services. Also in 2006, al-Zawahiri announced that the Algerian Salafist Group for Preaching and Combat had joined al-Qaida, adopting the name al-Qaida in the Lands of the Islamic

Maghreb. In 2009, extremist leaders in Yemen and Saudi Arabia reportedly announced they had merged to fight under the banner of al-Qaida in the Arabian Peninsula.

From early 2008 through 2010, al-Qaida lost significant parts of its command structure, based in the tribal areas of Pakistan, in a succession of blows as damaging to the group as any since the fall of the Afghan Taliban in late 2001. Key leaders killed included Abu Shaykh Mustafa Abu al-Yazid, one of al-Qaida's most senior leaders; Abu Khabab al-Masri, the group's leading expert on explosives and chemical attacks; Khalid Habib, al-Qaida's military chief; Abu Layth al-Libi, a key military commander and link between al-Qaida and its affiliates in North Africa; and Osama al-Kini, an operational planner who was involved in the 1998 embassy bombings in East Africa.

Despite leadership losses, al-Qaida remains committed to conducting attacks in the United States and against American interests abroad. In April 2009, senior al-Qaida leader Abu Yahya al-Libi advocated attacking US military, political, economic, and financial targets. Al-Qaida trained and deployed Najibullah Zazi, who was arrested in September 2009 for conspiring to use explosives within the United States. Al-Qaida is also focused on attacking Europe and has encouraged affiliates to target European interests. Al-Qaida also has increased its support for and participation in attacks inside Pakistan, working closely with Pakistani militant allies.[158]

Ansar al-Islam

Ansar al-Islam (AI), formerly known as Ansar al-Sunna (AS), is a Sunni extremist group consisting of Iraqi Kurds and Arabs intent on establishing a Salafi Islamic state in Iraq. AI has worked with al-Qaida senior leadership and al-Qaida in Iraq in the past and has carried out joint operations in Iraq. Some AI members trained in al-Qaida camps in Afghanistan, and the group provided safehaven to al-Qaida fighters in northern Iraq before Operation Iraqi Freedom commenced in March 2003.

Now detained, Ansar al-Sunna leader Abu ‘Abdallah al-Shafi‘I, in December 2007, announced that the group was reverting to its original name of Ansar al-Islam, previously used from the time of its establishment in 2001 until mid-2003. Al-Shafi‘i claimed the change was intended to signify a consolidation of the group’s Salafi jihadist principles. It may have also been an attempt to distance itself from members of AS who, in May 2007, announced an agreement with the Islamic Army in Iraq and the Army of the Mujahidin to form a united group called “The Jihad and Reformation Front.” In late July 2009, several AI members, including the group’s deputy and operational commander, Mullah Halgurd, were arrested. In May 2010 Iraqi security forces arrested AI leader al-Shafi‘i. The capture of al-Shafi‘i, along with other key AI figures, represents a significant blow to the group’s operational capabilities.

AI operates primarily in northern Iraq and consistently claims the second-largest number of Sunni jihadist attacks in Iraq (behind al-Qaida in Iraq). The group regularly targets Coalition forces, Iraqi Government and security forces, and Iraqi political parties, including the suicide bombing of a US military dining facility in Mosul in December 2004 that killed 22 US and Coalition soldiers. AI continues to conduct and claim responsibility for car bombings, assassinations, and kidnappings in Iraq.

In the first seven months of 2010, Ansar al-Islam released 54 statements claiming responsibility for attacks on US and Iraqi forces or expressing ideological and political messages. In their statements, Ansar al-Islam criticized the Iraqi elections, praised attacks on US and Iraqi military forces, eulogized the death of al-Qaida in Iraq leader Mustafa Abu al-Yazid, and discussed religious decrees and rulings.[159]

Fuerzas Armadas Revolucionarios de Colombia (FARC)

Established in 1964 as the military wing of the Colombian Communist Party, the Revolutionary Armed Forces of Colombia is Latin America’s oldest, largest, most capable, and best-equipped insurgency of Marxist origin—although it only nominally fights in support of Marxist goals today. The FARC primarily operates in Colombia, with some activities—extortion, kidnapping, weapons acquisition, and logistics—in neighboring countries.

FARC tactics include bombing, murder, mortar attack, kidnapping, extortion, and hijacking, as well as guerrilla and conventional military action against Colombian political, military, and economic targets. The FARC has well-documented ties to a range of drug trafficking activities including taxation, cultivation, and distribution. The group considers US persons to be legitimate military targets because of US support for the Colombian Government.

The group had a number of setbacks in 2009 highlighted by the loss of several key mid-level commanders and the continuing decline of its fighting force, now down to 8,000 members. The FARC in October 2009 attempted to confront the Colombian Government with an offensive aimed at a wide range of military and civilian targets. Colombian security forces largely thwarted the attacks in another setback for the group. Bogota frustrated similar FARC attempts to disrupt the March 2010 congressional and May 2010 presidential elections. In September 2010, Colombian forces killed veteran FARC military commander Victor Julio Suarez Rojas, better known as Mono Jojoy.

Juan Manuel Santos, elected as president in May 2010, will likely continue Bogota's policy of aggressive military operations—known as Democratic Security—against the FARC. Santos, a former defense minister, has publicly vowed to strengthen Colombia's military and police forces in order to defeat the FARC and end the conflict, now nearly 50 years long.[160]

Harakat Al-Muqawama Al-Islamia (Hamas)

Hamas was formed in late 1987 at the beginning of the first Palestinian Intifada (uprising). Its roots are in the Palestinian branch of the Muslim Brotherhood, and it is supported by a robust social/political structure inside the Palestinian territories. The group's charter calls for establishing an

Islamic Palestinian state in place of Israel and rejects all agreements made between the PLO and Israel. More recently, Hamas has publicly expressed a willingness to accept a long-term cessation of hostilities if Israel agrees to a Palestinian state based on the 1967 borders with Jerusalem as its capital. Hamas's strength is concentrated in the Gaza Strip and areas of the West Bank.

Hamas has a paramilitary arm, the Izz al-Din al-Qassam Brigades, which, beginning in the 1990s, has conducted many anti-Israeli attacks in Israel and the Palestinian territories. These have included large-scale terrorist bombings against Israeli civilian targets, as well as small-arms attacks, improvised roadside explosives, and the launching of rockets into Israel. While the group receives some support from foreign countries and movements, it remains independent.

In early 2006 Hamas won legislative elections in the Palestinian territories, ending the secular Fatah party's hold on the Palestinian Authority and challenging Fatah's leadership of the Palestinian national movement. Hamas continues its refusal to recognize Israel or renounce violence against Israelis and, over the past few years, has conducted one suicide bombing, which killed one civilian, and numerous mortar and rocket attacks that injured civilians. The US Government has designated Hamas as a Foreign Terrorist Organization.

Hamas in June 2008 entered into a six-month agreement for calm with Israel that significantly reduced rocket attacks. Following the temporary calm, Hamas resumed its rocket attacks, which precipitated the launching of a major military operation by Israel on December 27, 2008. After destroying much of Hamas's infrastructure in the Gaza Strip, Israel declared a unilateral cease-fire on January 18, 2009. Through 2009 and into 2010, HAMAS has worked to rein in attacks from other groups and enforce the cease-fire, though sporadic low-level attacks against Israeli forces along the Gaza border have continued.

In May 2010, the Israel Defense Forces intercepted a flotilla of humanitarian aid vessels bound for the Gaza Strip, which since 2007 has been under a strictly enforced Israeli blockade. The seizure of the ship led to a violent confrontation and resulted in the death of nine passengers. Hamas publicly condemned the incident, which it characterized as a massacre, and urged international activists to continue their attempts—with additional flotillas if necessary—to break the blockade. In late August, an Izz al-Din al-Qassam Brigades spokesman claimed responsibility for the shooting deaths of four Israeli settlers, an attack widely believed to be aimed scuttling peace talks between Palestinians and Israelis in Washington.[161]

Hezbollah

Hezbollah ("Party of God") was formed in 1982 in response to the Israeli invasion of Lebanon. They are a Lebanon-based radical Shia group that advocates Shia empowerment within Lebanon. Hezbollah also supports Palestinian rejectionist groups in their struggle against Israel and now provides training for Iraqi Shia militants attacking Coalition forces in Iraq. Hezbollah is known or suspected to have been involved in or provided support to numerous anti-US terrorist attacks, including the suicide truck bombings of the US Embassy in Beirut in April 1983, the US Marine barracks in Beirut in October 1983, and the US Embassy annex in Beirut in September 1984, as well as the hijacking of TWA 847 in 1985 and the Khobar Towers attack in Saudi Arabia in 1996.

Hezbollah primarily operates in the Al Biqa' (Bekaa Valley), Hermil, the southern suburbs of Beirut, and southern Lebanon. The group has established cells in the Middle East, Europe, Africa, South America, North America, and Asia.

Since the passage of UN Security Council Resolution 1559 in fall 2004, which called for the disarmament of all armed militias in Lebanon, Hezbollah has focused on justifying its retention of arms by casting itself within Lebanon as the only reliable bulwark against Israeli aggression. To this end, Hezbollah kidnapped two Israeli soldiers on the Israeli side of the Israel-Lebanon border on July 12, 2006 in a gambit to negotiate the release of Lebanese and other Arab prisoners being held by Israel. In response, Israel launched an extensive military campaign against Hezbollah in Lebanon with the aim of eradicating the organization. Following the UN-brokered cease-fire in August 2006, Hezbollah claimed victory by virtue of its survival and has since sought to use the conflict to justify its need to retain its arms as a Lebanese resistance force.

In February 2008, Hezbollah's military chief 'Imad Mughniyah was killed by a vehicle bomb set off by unknown persons in Damascus. Hezbollah Secretary General Hassan Nasrallah publicly blamed Israel and continues to promise retaliation.

Press reporting since 2009 has cast Hezbollah as the main suspect in the UN Special Tribunal for Lebanon's (STL) investigation of former Lebanese Prime Minister Rafiq al-Hariri's assassination—Hariri was killed by a car bomb in Beirut on February 14, 2005. In a March 2010 television interview, Nasrallah agreed to cooperate with the STL under certain conditions but continues to stress the role of Hezbollah members as witnesses instead of suspects. He stressed Israel was the first to accuse Hezbollah of involvement in al-Hariri's killing, and repeated past claims that Israel and the United States are driving the investigation.

The group is also known as the Islamic Resistance, Islamic Jihad, Revolutionary Justice Organization, and Organization of the Oppressed on Earth.[162]

Lashkar-e-Taliba

Lashkar-e-Taliba (LeT), also known as Army of the Righteous, is one of the largest and most proficient of the Kashmir-focused militant groups. LeT formed in the early 1990s as the military wing of Markaz-ud-Dawa-wal-Irshad, a Pakistan-based Islamic fundamentalist missionary organization founded in the 1980s to oppose the Soviets in Afghanistan. Since 1993, LeT has conducted numerous attacks against Indian troops and civilian targets in the disputed Jammu and Kashmir state, as well as several high-profile attacks inside India itself, and concern over new LeT attacks in India remains high. The United States and United Nations have designated LeT an international terrorist organization. The

Pakistani Government banned the LeT and froze its assets in 2002. In 2008 the US Treasury Department imposed sanctions on four senior LeT leaders.

The Indian Government implicated LeT in the November 26–28, 2008 attacks in Mumbai. Pakistani authorities have detained and are prosecuting several LeT leaders for the Mumbai attacks. David Headley, an American citizen who acknowledged attending LeT training camps, pleaded guilty in March 2010 to scouting targets for the Mumbai attacks. India also implicated LeT for other high-profile attacks, including the July 11, 2006 attack on multiple Mumbai commuter trains that killed more than 180 people, and the December 2001 armed assault on the Indian Parliament building that left 12 dead. Indian authorities have speculated that LeT also may have contributed surveillance and planning for the February 13, 2010 bombing of a German bakery in Pune.

LeT's exact size is unknown, but the group probably has several thousand members, predominantly Pakistani nationals seeking a united Kashmir under Pakistani rule. Elements of LeT are active in Afghanistan and the group also recruits internationally, as evidenced by Headley's arrest and the indictment of 11 LeT terrorists in Virginia in 2003. LeT maintains facilities in Pakistan, including training camps, schools, and medical clinics. In March 2002, senior al-Qaida lieutenant Abu Zubaydah was captured at an LeT safe house in Faisalabad, suggesting that some LeT members assist the group.

LeT coordinates its charitable activities through its front organization, Jamaat-ud-Dawa, which spearheaded humanitarian relief to the victims of the October 2005 earthquake in Kashmir. JUD activities, however, have been limited since December 2008 by the UN's designation of the group as an alias for LeT. During the 2010 floods in Pakistan, Jamaat-ud-Dawa and an affiliated charity, the Falah-i-Insaniyat Foundation, were widely reported to have provided aid to flood victims.[163]

Footnotes

[1] Lesley Meall, "Get the Message," *Accountacy* 136, no. 1346 (2005): 92, http://web.ebscohost.com/ehost/detail?sid=ea06ecca-f666-4942-8ee9-803fadc70550%40sessionmgr12&vid=1&hid=7&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=buh&AN=18598772 (accessed March 31, 2011).

[2] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 130.

[3] Department of Justice, "Pennsylvania Woman Indicted in Plot to Recruit Violent Jihadist Fighters and to Commit Murder Overseas," http://www.justice.gov/opa/pr/2010/March/10-ag-238.html (Accessed March 9, 2011).

[4] Robert Charette, "Open-Source Warfare," *IEEE Spectrum* 44, no. 11 (November 2007): 27, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4378455&isnumber=4378443 (accessed January 31, 201).

[5] Colonel Jacob Graham, "Understanding IEDs: a Preliminary Study," (PowerPoint slides, Pennsylvania State University, University Park, PA, ON, April 28, 2011).

[6] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 9-10.

[7] Arie Perliger, Ami Pedahzur, and Yair Zalmanovitch, "The Defensive Dimension of the Battle against Terrorism – An Analysis of Management of Terror Incidents in Jerusalem," *Journal of Contingencies and Crisis Management* 13, no. 2 (2005): 82, http://onlinelibrary.wiley.com/doi/10.1111/j.1468-5973.2005.00460.x/pdf (accessed May 31, 2011).

[8] Air University, "Unit 1Topic 3: Terrorism," http://www.au.af.mil/au/awc/awcgate/navy/gmt_terrorism.pdf (accessed April 16, 2011).

[9] Office of the Law Revision Counsel, U.S. House of Representatives, "22 USC sec. 2656f," Foreign relations and Intercourse, http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t21t25+2620+0++%28terrorism%20definition%29%20%20AND%20%28%2822%29%20ADJ%20USC%29%3ACITE%20AND%20%28USC%20w%2F10%20%282656f%29%29%3ACITE%20%20%20%20%20%20%20%20 (accessed April 17, 2011).

[10] Towson University, "Terrorism: Goals of Terror Tactics," Towson University, http://www.towson.edu/polsci/ppp/sp97/terror/goals.html (accessed April 17, 2011).

[11] JB Wolf, "Organization and Management Practices of Urban Terrorist Groups," *Studies in Conflict & Terrorism* (1978), http://www.informaworld.com/smpp/content~db=all~content=a789423350 (accessed April 16, 2011).

[12] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 115.

[13] Gabriel Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," United States Institute of Peace, p 9, http://www.usip.org/publications/wwwterrornet-how-modern-terrorism-uses-internet (Accessed March 2, 2011)

[14] Kathy Crilley. "Information warfare: new battlefields Terrorists, propaganda, and the Internet," *Aslib Proceedings* 53(July/August 2001): 252.

[15] Maura Conway, "Terrorist 'Use' of the Internet and Fighting Back," *Information & Security* 19 (2006): 15, http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/maura_conway.pdf (accessed March 1, 2011).

[16] Frank Bolz Jr, Kenneth J. Dudonis, and David P. Schulz, *The Counterterrorism Handbook: Tactics, Procedures, and Techniques*, 3rd ed. (Boca Raton, Fla.: CRC Press, 2005): 27.

[17] Robert G. Rabil, "Hezbollah: Lebanon's Power Broker," The Journal of International Security Affairs (2008), http://www.securityaffairs.org/issues/2008/15/rabil.php (accessed September 15, 2011).

[18] Angel Rabasa, et al, "Beyond al-Qaida Part I: The Global Jihadist Movement," *RAND Organization* (2006): 27-29, http://www.rand.org/pubs/monographs/2006/RAND_MG429.pdf (accessed April 16, 2011).

[19] House of Representatives, Subcommittee on International Terrorism, Nonproliferation, and Hunan Rights, Committee on International Relations, "Al-Qaeda: The Threats to the United States and Its Allies." http://psi.praeger.com.ezaccess.libraries.psu.edu/pdfs/46.pdf (accessed April 16, 2011).

[20] Rohan Gunaratna and Aviv Oreg, "Al Qaeda's Organizational Structure and its Evolution," *Studies in Conflict & Terrorism* 33 (2010): 1055, http://www.tandfonline.com/doi/pdf/10.1080/1057610X.2010.523860 (accessed October 22, 2011).

[21] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 9-10.

[22] Gabriel Weimann, “Terrorist Dot Com: Using the Internet for Terrorist Recruitment and Mobilization,” in *The Making of a Terrorist: Recruitment, Training, and Root Causes*, ed. James J.F. Forest (Westport: Praeger Security International, 2006), 1: 53.

[23]Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 61-62.

[24] The New York City Police Department, “Radicalization in the West: The Homegrown Threat,” http://www.nyc.gov/html/nypd/downloads/pdf/public_information/NYPD_Report-Radicalization_in_the_West.pdf (accessed April 16, 2011): 6.

[25] Ibid.

[26] Ibid., 7.

[27] Ibid.

[28] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 88.

[29] Maura Conway, “Terror TV? An Exploration of Hezbollah’s al-Manar Television,” in *Countering Terrorism and Insurgency in the 21st Century*, ed. James J.F. Forest (Westport: Praeger Security International, 2007), 2: 406.

[30] Brigitte L. Nacos, “Communication and Recruitment of Terrorists,” in *The Making of a Terrorist: Recruitment, Training, and Root Causes*, ed. James J.F. Forest (Westport: Praeger Security International, 2006), 1: 50.

[31] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 89.

[32] James J.F. Forest et al, *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*, ed. James J.F. Forest (Westport: Praeger Security International, 2007), 1: 369-370

[33] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 98.

[34] Ibid., 98-99.

[35] Robert Charette, “Open-Source Warfare,” *IEEE Spectrum* 44, no. 11 (November 2007): 29. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4378455&isnumber=4378443 (accessed January 31, 2011).

[36] Kathy Crilley. “Information warfare: new battlefields Terrorists, propaganda, and the Internet,” *Aslib Proceedings* 53(July/August 2001): 250.

[37] IntelCenter, “Evolution of Jihadi Video (EJV) v1.0,” http://www.intelcenter.com/EJV-PUB-v1-0.pdf (accessed March 16, 2011).

[38] Timothy L. Thomas, “Cyber Mobilization: the Neglected Aspect of Information Operations and Counterinsurgency Doctrine,” in *Countering Terrorism and Insurgency in the 21st Century*, ed. James J.F. Forest (Westport: Praeger Security International, 2007), 1: 360.

[39] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 62.

[40] Ibid., 63.

[41] Ibid., 69.

[42] Bryan Walsh, “Can We Prevent Another Blackout?,” *Time* (August 11, 2008) http://www.time.com/time/health/article/0,8599,1831346,00.html (accessed March 7, 2011).

[43] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 70.

[44] Gabriel Weimann, “Terrorist Dot Com: Using the Internet for Terrorist Recruitment and Mobilization,” in *The Making of a Terrorist: Recruitment, Training, and Root Causes*, ed. James J.F. Forest (Westport: Praeger Security International, 2006), 1: 58.

[45] Brigitte L. Nacos, “Communication and Recruitment of Terrorists,” in *The Making of a Terrorist: Recruitment, Training, and Root Causes*, ed. James J.F. Forest (Westport: Praeger Security International, 2006), 1: 43.

[46] The New York City Police Department, “Radicalization in the West: The Homegrown Threat,” http://www.nyc.gov/html/nypd/downloads/pdf/public_information/NYPD_Report-Radicalization_in_the_West.pdf (accessed April 16, 2011): 8.

[47] Ibid., 6.

[48] Mark E. Stout, Jessica M. Huckabey, John R. Schindler, and Jim Lacey, *The Terrorist Perspectives Project: Strategic and Operational Views of Al Qaida and Associated Movements* (Annapolis: The United States Naval Institute, 2008), 190.

[49] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 83.

[50] Ibid., 91.

[51] Ibid., 92.

[52] Ibid.

[53] Ibid.

[54] Gabriel Weimann, “Terrorist Dot Com: Using the Internet for Terrorist Recruitment and Mobilization,” in *The Making of a Terrorist: Recruitment, Training, and Root Causes*, ed. James J.F. Forest (Westport: Praeger Security International, 2006), 1: 58.

[55] Daphne Burdman, "Education, Indoctrination, and Incitement: Palestinian children on their way to martyrdom," *Terrorism and Political Violence* 15, no. 1 (2003): 107. http://www.tandfonline.com/doi/pdf/10.1080/09546550312331292977 (accessed October 15, 2011).

[56] P.W. Singer. "The New Children of Terror." Brookings:107, http://www.brookings.edu/views/papers/singer/chapter8_20051215.pdf (accessed October 15, 2011).

[57] Ibid.,108.

[58] Ibid.

[59] Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004): 161

[60] Robert W. Taylor, Tory J. Caeti, Kall Loper, Eric J. Fritsch, and John Liederbach, *Digital Crime and Digital Terrorism*, (Upper Saddle River: Pearson Education, Inc., 2006): 30.

[61] Gabriel Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," United States Institute of Peace, http://www.usip.org/publications/wwwterrornet-how-modern-terrorism-uses-internet (Accessed March 2, 2011).

[62] Department of Justice, "Pennsylvania Women Indicted in Plot to Recruit Violent Jihadist Fighters and Commit Murder Overseas," http://www.justice.gov/usao/pae/News/2010/mar/larose_release.pdf (accessed November 1, 2011).

[63] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 119.

[64] Matthew Epstein, "Arabian Gulf Financial Sponsorship of Al-Qaida via U.S.- Based Banks," US House: 13, http://financialservices.house.gov/media/pdf/031103me.pdf (accessed October 15, 2011).

[65] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 127.

[66] Gabriel Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," United States Institute of Peace, 9 http://www.usip.org/publications/wwwterrornet-how-modern-terrorism-uses-internet (Accessed March 2, 2011).

[67] Ibid., 9.

[68] Jarret M. Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," *Fletcher Forum of World Affairs* 30, no. 2 (Summer 2006): 152.

[69] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 9.

[70] James J.F. Forest et al, *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*, ed. James J.F. Forest (Westport: Praeger Security International, 2007): 1: 370

[71] Kathy Crilley, “Information warfare: new battlefields Terrorists, propaganda, and the Internet,” *Aslib Proceedings* 53(July/August 2001): 252.

[72] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 52.

[73] Abdel B. Atwan, *The Secret History of al-Qaida*, (Berkley And Los Angeles: University of California Press, 2006): 133.

[74] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 65.

[75] Ibid., 64.

[76] Malcolm W. Nance, *Terrorist Recognition Handbook*. 2nd ed.(Boca: CRC Press, 2008): 360-361.

[77] Jarret M. Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," *Fletcher Forum of World Affairs* 30, no. 2 (Summer 2006): 152.

[78] Ibid., 152.

[79] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 130.

[80] Free Republic, "Riyadh Attack Was First Al Qaeda Attempt on Life of Saudi Royal," http://www.freerepublic.com/focus/f-news/1311887/posts (accessed November 1, 2011).

[81] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 125.

[82] Rita Katz and Michael Kern, "Terrorist 007, Exposed," *The Washington post*, March 26, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html (accessed October 16, 2011).

[83] Abigail Cutler, "Web of Terror," *The Atlantic*, June 2006, http://www.theatlantic.com/magazine/archive/2006/06/web-of-terror/4998/?single_page=true (accessed October 16, 2011).

[84] Brian Forst, *Terrorism, Crime, and Public Policy* (New York: Cambridge University Press, 2009): 186.

[85] Ibid., 187-188.

[86] Michael R. Ronczkowski, *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations* (New York: CRC Press, 2007): 26.

[87]S M. Furnell and M J. Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium," *Computers and Security* 18, no. 1 (1999): 32, http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V8G-3W31NRB-6&_user=209810&_coverDate=12%2F31%2F1999&_rdoc=1&_fmt=high&_orig=gateway&_origin=gateway&_sort=d&_docanchor=&view=c&_searchStrId= (accessed April 28, 2011).

[88] Scott Berinato, "Cybersecurity - The Truth About Cyberterrorism," *CIO*, March 15, 2002, p. 2, http://www.cio.com/article/30933/CYBERSECURITY_The_Truth_About_Cyberterrorism?page=2&taxonomyId=3089 (accessed April 28, 2011).

[89] Robert L. Maley, "Cyber Terrorism," Commonwealth of Pennsylvania, (accessed April 28, 2011).

[90] Michael R. Ronczkowski, *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations* (New York: CRC Press, 2007): 219.

[91] Ibid., 25.

[92] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 154- 155.

[93] Ibid., 158.

[94] Ibid., 122.

[95] Ibid., 113.

[96] Steven P. Bucci, Ph.D., “The Confluence of Cyber Crime and Terrorism,” *Heritage Lectures* 1123(May 2009): 5. www.heritage.org/Research/NationalSecurity/hl1123.cfm (accessed February 9, 2011).

[97] Linden Lab Official:Xstreet Currency Exchange, Second Life, http://wiki.secondlife.com/wiki/Linden_Lab_Official:Xstreet_Currency_Exchange (accessed February 9, 2011).

[98] Robert D. Hof, “My Virtual Life,” *Business Week*, May 2006, http://www.businessweek.com/magazine/content/06_18/b3982001.htm (accessed February 9, 2011).

[99] Kathy Crilley. “Information warfare: new battlefields Terrorists, propaganda, and the Internet,” *Aslib Proceedings* 53(July/August 2001): 252.

[100] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006), 134.

[101] Ibid., 13.

[102] Ibid., 138.

[103] Ibid., 141.

[104] Ibid., 134.

[105] Ibid., 135.

[106] Steven Cherry, “Terror Goes Online,” *IEEE Spectrum* (January 2005): 73, http://ieeexplore.ieee.org/search/srchabstract.jsp?tp=&arnumber=1377883&queryText%3Dterror+goes+online%26openedRefinements%3D*%26searchField%3DSearch+All (Accessed March 1, 2011).

[107] Gabriel Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," United States Institute of Peace, http://www.usip.org/publications/wwwterrornet-how-modern-terrorism-uses-internet (Accessed March 2, 2011).

[108] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 139.

[109] Matthew A. Levitt, "Hearing on "The Role of Charities and NGOs in the Financing of Terrorist Activities," US Senate, http://banking.senate.gov/02_08hrg/080102/levitt.htm (accessed October 16, 2011).

[110] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 134.

[111] Ibid., 135.

[112] James J.F. Forest et al, *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*, ed. James J.F. Forest (Westport: Praeger Security International, 2007): 2: 370

[113] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 112.

[114]Maura Conway, "Terrorist 'Use' of the Internet and Fighting Back," *Information & Security* 19 (2006): 17, http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/maura_conway.pdf (accessed March 1, 2011).

[115] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006), 112.

[116] Steven Cherry, “Terror Goes Online,” *IEEE Spectrum* (January 2005): 72, http://ieeexplore.ieee.org/search/srchabstract.jsp?tp=&arnumber=1377883&queryText%3Dterror+goes+online%26openedRefinements%3D*%26searchField%3DSearch+All (Accessed March 1, 2011).

[117] Ibid., 72-73.

[118] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 113.

[119] Ibid., 112.

[120] Ibid., 114.

[121] Steven P. Bucci, Ph.D., “The Confluence of Cyber Crime and Terrorism,” *Heritage Lectures* 1123(May 2009): 4, www.heritage.org/Research/NationalSecurity/hl1123.cfm (accessed February 9, 2011).

[122] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 154.

[123] Malcolm W. Nance, *Terrorist Recognition Handbook*. 2nd ed,(Boca: CRC Press, 2008): 122.

[124] James J.F. Forest et al, *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*, ed. James J.F. Forest (Westport: Praeger Security International, 2007): 1: 370.

[125] Ibid., 403.

[126] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006), 133.

[127] Frank Bolz Jr, Kenneth J. Dudonis, and David P. Schulz, *The Counterterrorism Handbook: Tactics, Procedures, and Techniques*, 3rd ed. (Boca Raton, Fla.: CRC Press, 2005): 27.

[128] Robert W. Taylor, Tory J. Caeti, Kall Loper, Eric J. Fritsch, and John Liederbach, *Digital Crime and Digital Terrorism*, (Upper Saddle River: Pearson Education, Inc., 2006): 29.

[129] Edward M. Roche, *Virtual Worlds Real Terrorism: Virtual Worlds as a Platform for Criminal Consipiacy, Espionage, Counter-Intelligence Operations & Terror*, (Den Haag, Netherlands: Aardwolf Publications, 2009): 29.

[130]Steven P. Bucci, Ph.D., “The Confluence of Cyber Crime and Terrorism,” *Heritage Lectures* 1123(May 2009): 5, www.heritage.org/Research/NationalSecurity/hl1123.cfm (accessed February 9, 2011).

[131] Sujoyini Mandal and Ee-Peng Lim, "Second Life: Limits Of Creativity Or Cyber Threat?," IEEE. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4534503, (accessed October 10, 2011): 499.

[132] Kathy Crilley, “Information warfare: new battlefields Terrorists, propaganda, and the Internet,” *Aslib Proceedings* 53(July/August 2001): 252.

[133] Abdel B. Atwan, *The Secret History of al-Qaida*, (Berkley And Los Angeles: University of California Press, 2006): 133.

[134] Jonathan R. White, *Terrorism and Homeland Security*, 6th ed. (Belmont: Wadsworth Cengage Learning, 2009): 83.

[135] Malcolm W. Nance, *Terrorist Recognition Handbook*. 2nd ed.(Boca: CRC Press, 2008): 122.

[136] Steven P. Bucci, Ph.D., “The Confluence of Cyber Crime and Terrorism,” *Heritage Lectures* 1123(May 2009): 4. www.heritage.org/Research/NationalSecurity/hl1123.cfm (accessed February 9, 2011).

[137] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: Endowment of the United States Institute of Peace, 2006): 129-130.

[138] Joseph Liberman and Susan Collins, "Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat," United States Senate, (May 2008): 10.

[139] Malcolm W. Nance, *Terrorist Recognition Handbook*. 2nd ed.(Boca: CRC Press, 2008): 360.

[140] Steven P. Bucci, Ph.D., “The Confluence of Cyber Crime and Terrorism,” *Heritage Lectures* 1123(May 2009): 4. www.heritage.org/Research/NationalSecurity/hl1123.cfm (accessed February 9, 2011).

[141] Department of Defense, http://www.dtic.mil/doctrine/jel/doddict/data/w/8880.html (accessed May 31, 2011).

[142] Department of Justice, "Chicagoan David Headley Charged with Conspiracy in 2008," http://www.justice.gov/usao/iln/pr/chicago/2009/pr1207_01.pdf (accessed November 1, 2011).

[143] Joseph I. Liberman, "Lessons from the Mumbai Terrorist Attacks," Senate Committee on Homeland Security & Government, http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&&FileStore_id=8dceea32-d846-4496-b48f-f77a22b41c24 (accessed June 10, 2011).

[144] Charles E. Allen, "Lessons from the Mumbai Terrorist Attacks," Senate Committee on Homeland Security & Government, http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=e481708b-ff25-4e65-8667-407b8dc96283 (accessed June 10, 2011).

[145] Joseph I. Liberman, "Lessons from the Mumbai Terrorist Attacks Part II," Senate Committee on Homeland Security & Government, http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&&FileStore_id=e3e649f5-2de1-4cf5-ae0c-b81ed164e590 (accessed June 10, 2011).

[146] Ibid.

[147] Onook Oh, Manish Agrawal, and Raghav Rao, "Information control and terrorism: Tracking the Mumbai terrorist attack through twitter," *Information Systems Frontiers* 13, no. 1 (2010): 36.

[148] Raymond W. Kelly, "Lessons from the Mumbai Terrorist Attacks," Senate Committee on Homeland Security & Government, http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=c026e17b-2d79-4169-8829-28a3650d2311 (accessed June 10, 2011).

[149] Onook Oh, Manish Agrawal, and Raghav Rao, "Information control and terrorism: Tracking the Mumbai terrorist attack through twitter," *Information Systems Frontiers* 13, no. 1 (2010): 33.

[150] Ibid., 34.

[151] Ibid., 37.

[152] Ibid., 37.

[153] Ibid.

[154] Thomas L. Friedman, *The World is Flat: A Brief History of the Twenty-First Century*, (New York: Farrar, Straus and Giroux, 2005): 53.

[155] Ibid., 55.

[156] Maura Conway, "Terrorist 'Use' of the Internet and Fighting Back," *Information & Security* 19 (2006): 15, http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/maura_conway.pdf (accessed March 1, 2011).

[157] Robert Charette, "Open-Source Warfare," *IEEE Spectrum* 44, no. 11 (November 2007): 27, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4378455&isnumber=4378443 (accessed January 31, 201).

[158] NCTC, "Al-Qa'ida," http://www.nctc.gov/site/groups/al_qaida.html (accessed June 17, 2011).

[159] NCTC, " Ansar al-Islam(AI)," http://www.nctc.gov/site/groups/ai.html (accessed June 17, 2011).

[160] NCTC, " Revolutionary Armed Forces of Columbia (FARC)," http://www.nctc.gov/site/groups/farc.html (accessed June 17, 2011).

[161] NCTC, " Hamas," http://www.nctc.gov/site/groups/ **h**amas.html (accessed June 17, 2011).

[162] NCTC, "Hezbollah," http://www.nctc.gov/site/groups/hizballah.html (accessed June 17, 2011).

[163] NCTC, " Lashkar-e-Talibar (LT or LeT; Army of the Righteous)," http://www.nctc.gov/site/groups/let.html (accessed June 17, 2011).

Bibliography

Air University. “Unit 1Topic 3: Terrorism.” http://www.au.af.mil/au/awc/awcgate/navy/gmt_terrorism.pdf (accessed April 16, 2011).

Allen, Charles E. "Lessons from the Mumbai Terrorist Attacks." Senate Committee on Homeland Security & Government. http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=e481708b-ff25-4e65-8667-407b8dc96283 (accessed June 10, 2011).

Atwan, Abdel B. *The Secret History of al-Qaida*. Berkley And Los Angeles: University of California Press, 2006.

“Author Salman Rushdie talks about 'living day to day.” CNN. http://www.cnn.com/WORLD/9702/14/rushdie/ (accessed June 17, 2011).

Bardon, Debbie. 2004. Online SOCIAL networking for business: An interview with Konstantin Guericke marketing VP, LinkedIn. *Online* 28, no. 6: 25, http://search.proquest.com/docview/199927510?accountid=13158.

Barnes, Nancy Dupre and Frederick R. Barnes. 2009. Equipping your organization for the social networking game. *Information Management Journal* 43, no. 6: 28, http://search.proquest.com/docview/227726153?accountid=13158.

Berinato, Scott. "Cybersecurity - The Truth About Cyberterrorism." *CIO*, March 15, 2002, p. 2. http://www.cio.com/article/30933/CYBERSECURITY_The_Truth_About_Cyberterrorism?page=2&taxonomyId=3089 (accessed April 28, 2011).

Biersteker, Thomas J., and Sue E. Eckert, eds. *Countering the Financing of Terrorism*. New York: Routledge, 2008.

Bolz Jr, Frank, Kenneth J. Dudonis, and David P. Schulz. *The Counterterrorism Handbook: Tactics, Procedures, and Techniques*. 3rd ed. Boca Raton, Fla.: CRC Press, 2005.

Brachman, Jarret M. "High-Tech Terror: Al-Qaeda's Use of New Technology." *Fletcher Forum of World Affairs* 30, no. 2 (Summer 2006): 149-164.

Bruck, Tilman, ed. *The Economic Analysis of Terrorism*. New York: Routledge, 2007.

Bucci, Steven P., Ph.D., “The Confluence of Cyber Crime and Terrorism,” *Heritage Lectures* 1123(May 2009). www.heritage.org/Research/NationalSecurity/hl1123.cfm (accessed February 9, 2011).

Bunt, Gary R. *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments*. Sterling: Pluto Press, 2003.

Bunt, Gary R. *Virtually Islamic: Computer-mediated Communications and Cyber Islamic Environments*. Llandybie: Dinefwr Press, 2000.

Burdman, Daphne. "Education, Indoctrination, and Incitement: Palestinian children on their way to martyrdom." *Terrorism and Political Violence* 15, no. 1 (2003): 96-123. http://www.tandfonline.com/doi/pdf/10.1080/09546550312331292977 (accessed October 15 2011).

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol: O'Riley Media, Inc., 2010.

Cassara, John A. *Hide & Seek: Intelligence, Law Enforcement, and the Stalled War on Terrorist Finance*. Washington DC: Potomac Books, Inc., 2006.

Cherry, Steven. “Terror Goes Online.” *IEEE Spectrum* (January 2005): 72-73. http://ieeexplore.ieee.org/search/srchabstract.jsp?tp=&arnumber=1377883&queryText%3Dterror+goes+online%26openedRefinements%3D*%26searchField%3DSearch+All (Accessed March 1, 2011).
Crilley, Kathy. “Information warfare: new battlefields Terrorists, propaganda, and the Internet.” *Aslib Proceedings* 53(July/August 2001): 250-264.

Charette, Robert. “Open-Source Warfare.” *IEEE Spectrum* 44, no. 11 (November 2007): 26-32. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4378455&isnumber=4378443 (accessed January 31, 2011).

Colarik, Andrew M. *Cyber Terrorism: Political and Economic Implications*. Hershey: Idea Group Publishing, 2006.

Conway, Maura. "Terrorist 'Use' of the Internet and Fighting Back." *Information & Security* 19 (2006): 9-30. http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/maura_conway.pdf (accessed March 1, 2011).

Costigan, Sean S., and David Gold. *Terrornomics*. Hampshire: Ashgate Publishing Ltd, 2007.

Cutler, Abigail. "Web of Terror." *The Atlantic*, June 2006. http://www.theatlantic.com/magazine/archive/2006/06/web-of-terror/4998/?single_page=true (accessed October 16, 2011).

Department of Defense. http://www.dtic.mil/doctrine/jel/doddict/data/w/8880.html (accessed May 31, 2011).

Department of Justice. "Chicagoan David Headley Charged with Conspiracy in 2008." http://www.justice.gov/usao/iln/pr/chicago/2009/pr1207_01.pdf (accessed November 1, 2011).

Department of Justice. "Pennsylvania Woman Indicted in Plot to Recruit Violent Jihadist Fighters and to Commit Murder Overseas." http://www.justice.gov/opa/pr/2010/March/10-ag-238.html (Accessed March 9, 2011).

Department of Justice. "Pennsylvania Women Indicted in Plot to Recruit Violent Jihadist Fighters and Commit Murder Overseas." http://www.justice.gov/usao/pae/News/2010/mar/larose_release.pdf (accessed November 1, 2011).

Dyson, William E. *Terrorism: an investigator's handbook*. 2nd ed. Menands, N.Y.: Matthew Bender & Company, Inc, 2005.

Epstein, Matthew. "Arabian Gulf Financial Sponsorship of Al-Qaida via U.S.- Based Bankes." US House. http://financialservices.house.gov/media/pdf/031103me.pdf (accessed October 15, 2011).

Forest, James J.F., ed. *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*. Vol. 1. Westport: Praeger Security International, 2007.

Forest, James J.F., ed. *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*. Vol. 2. Westport: Praeger Security International, 2007.

Forest, James J.F., ed. *The Making of A Terrorist: Recruitment, Training, and Root Causes*. Vol. 1. Westport: Praeger Security International, 2006.

Free Republic. "Riyadh Attack Was First Al Qaeda Attempt on Life of Saudi Royal." http://www.freerepublic.com/focus/f-news/1311887/posts (accessed November 1, 2011).

Friedman, Thomas L. *The World is Flat: A Brief History of the Twenty-First Century*. New York: Farrar, Straus and Giroux, 2005.

Furnell, S M., and M J. Warren. "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium." *Computers and Security* 18, no. 1 (1999): 28-34. http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V8G-3W31NRB-6&_user=209810&_coverDate=12%2F31%2F1999&_rdoc=1&_fmt=high&_orig=gateway&_origin=gateway&_sort=d&_docanchor=&view=c&_searchStrId= (accessed April 28, 2011).

Gunaratna, Rohan. *Inside Al Qaeda: Global Network of Terror*. London: C. Hurst & Co. Ltd, 2002.

Hobson, David. 2008. Social networking – not always friendly. *Computer Fraud & Security* 2008 (2) (2): 20.

Hof, Robert D. “My Virtual Life.” *Business Week*, May 2006, http://www.businessweek.com/magazine/content/06_18/b3982001.htm (accessed February 9, 2011).

House of Representatives, Subcommittee on International Terrorism, Nonproliferation, and Hunan Rights, Committee on International Relations. “Al-Qaeda: The Threats to the United States and Its Allies.” http://psi.praeger.com.ezaccess.libraries.psu.edu/pdfs/46.pdf (accessed April 16, 2011).

Howard, Russell D., Reid L. Sawyer, and Natasha E. Bajema. *Terrorism and Counterterrorism: Understanding the New Security Environment*. 3rd ed. New York: McGraw-Hill, 2009.

Katz, Rita, and Michael Kern. "Terrorist 007, Exposed." *The Washington post*, March 26, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html (accessed October 16, 2011).

Kelly, Raymond W. "Lessons from the Mumbai Terrorist Attacks." Senate Committee on Homeland Security & Government. http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=c026e17b-2d79-4169-8829-28a3650d2311. (accessed June 10, 2011).

Kilcullen, David. *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. Oxford: Oxford University Press, Inc., 2009.

Kinney, Michael. *From Pablo to Osama: trafficking and terrorist networks, government bureaucracies, and competitive adaptation*. University Park: The Pennsylvania State University Press, 2007.

Levitt, Matthew A. "Hearing on "The Role of Charities and NGOs in the Financing of Terrorist Activities."." US Senate. http://banking.senate.gov/02_08hrg/080102/levitt.htm (accessed October 16, 2011).

Liberman, Joseph I. "Lessons from the Mumbai Terrorist Attacks." Senate Committee on Homeland Security & Government. http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&&FileStore_id=8dceea32-d846-4496-b48f-f77a22b41c24 (accessed June 10, 2011).

Liberman, Joseph I. "Lessons from the Mumbai Terrorist Attacks Part II." Senate Committee on Homeland Security & Government. http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&&FileStore_id=e3e649f5-2de1-4cf5-ae0c-b81ed164e590 (accessed June 10, 2011).

Liberman, Joseph, and Susan Collins. "Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat." United States Senate.

Linden Lab Official:Xstreet Currency Exchange, Second Life, http://wiki.secondlife.com/wiki/Linden_Lab_Official:Xstreet_Currency_Exchange (accessed February 9, 2011).

Maley, Robert L. "Cyber Terrorism." Commonwealth of Pennsylvania. (accessed April 28, 2011).

Mandal, Sujoyini, and Ee-Peng Lim. "Second Life: Limits Of Creativity Or Cyber Threat?." IEEE. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4534503 (accessed October 10, 2011).

Meall, Lesley. "Get the Message." *Accountacy* 136, no. 1346 (2005): 92-93. http://web.ebscohost.com/ehost/detail?sid=ea06ecca-f666-4942-8ee9-803fadc70550%40sessionmgr12&vid=1&hid=7&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=buh&AN=18598772 (accessed March 31, 2011).

Menn, Joseph. *Fatal System Error: the hunt for the new crime lords who are bringing down the Internet*. New York: Public Affairs, 2010.

Nance, Malcolm W. *Terrorist Recognition Handbook*. 2nd ed. Boca: CRC Press, 2008.

NCTC. "Al-Qa‘ida." http://www.nctc.gov/site/groups/al_qaida.html (accessed June 17, 2011).

NCTC. "Ansar al-Islam(AI)." http://www.nctc.gov/site/groups/ai.html (accessed June 17, 2011).

NCTC. "Hamas." http://www.nctc.gov/site/groups/hamas.html (accessed June 17, 2011).

NCTC. "Hezbollah." http://www.nctc.gov/site/groups/hizballah.html (accessed June 17, 2011).

NCTC. "Lashkar-e-Talibar (LT or LeT; Army of the Righteous)." http://www.nctc.gov/site/groups/let.html (accessed June 17, 2011).

NCTC. "Revolutionary Armed Forces of Columbia (FARC)." http://www.nctc.gov/site/groups/farc.html (accessed June 17, 2011).

Office of the Law Revision Counsel, U.S. House of Representatives. “22 USC sec. 2656f.” Foreign relations and Intercourse. http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t21t25+2620+0++%28terrorism%20definition%29%20%20AND%20%28%2822%29%20ADJ%20USC%29%3ACITE%20AND%20%28USC%20w%2F10%20%282656f%29%29%3ACITE%20%20%20%20%20%20%20%20%20 (accessed April 17, 2011).

Oh, Onook, Manish Agrawal, and Raghav Rao. "Information control and terrorism: Tracking the Mumbai terrorist attack through twitter." *Information Systems Frontiers* 13, no. 1 (2010): 33-43.

Perliger, Arie, Ami Pedahzur, and Yair Zalmanovitch. "The Defensive Dimension of the Battle against Terrorism – An Analysis of Management of Terror Incidents in Jerusalem." Journal of Contingencies and Crisis Management 13, no. 2 (2005): 79-91. http://onlinelibrary.wiley.com/doi/10.1111/j.1468-5973.2005.00460.x/pdf (accessed May 31, 2011).

Rabasa, Angel, et al. “Beyond al-Qaida Part I: The Global Jihadist Movement.” RAND *Organization* (2006). http://www.rand.org/pubs/monographs/2006/RAND_MG429.pdf (accessed April 16, 2011).

Roche, Edward M. *Virtual Worlds Real Terrorism: Virtual Worlds as a Platform for Criminal Consipiacy, Espionage, Counter-Intelligence Operations & Terror*. Den Haag, Netherlands: Aardwolf Publications, 2009.

Ronczkowski, Michael R. *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations*. 2nd ed. Boca Raton: CRC Press, 2007.

Sageman, Marc. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004.

Schwartau, Winn. *CyberShock: Surviing Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption*. New York: Thunder's Mouth Press, 2000.

Singer, P.W. "The New Children of Terror." Brookings. http://www.brookings.edu/views/papers/singer/chapter8_20051215.pdf.

Stout, Mark E., Jessica M. Huckabey, John R. Schindler, and Jim Lacey. *The Terrorist Perspectives Project: Strategic and Operational Views of Al Qaida and Associated Movements*. Annapolis: The United States Naval Institute, 2008.

Taylor, Robert W., Tory J. Caeti, Kall Loper, Eric J. Fritsch, and John Liederbach. *Digital Crime and Digital Terrorism*. Upper Saddle River: Pearson Education, Inc., 2006.

The New York City Police Department. “Radicalization in the West: The Homegrown Threat.” http://www.nyc.gov/html/nypd/downloads/pdf/public_information/NYPD_Report-Radicalization_in_the_West.pdf (accessed April 16, 2011).

Treverton, Gregory F., Carl Matthies, Karla J. Cunningham, Jeremiah Goulka, and Greg Ridgeway. *Film Privacy, Organized Crime, and Terrorism*. Santa Monica: RAND Corporation, 2009.

Towson University, “Terrorism: Goals of Terror Tactics,” Towson University, http://www.towson.edu/polsci/ppp/sp97/terror/goals.html (accessed April 17, 2011).

Verton, Dan. *Black Ice: the Invisible Threat of Cyber-Terrorism*. Emeryvile: McGraw-Hill/Osborne, 2003.

Walsh, Bryan. “Can We Prevent Another Blackout?.” *Time* (August 11, 2008) http://www.time.com/time/health/article/0,8599,1831346,00.html (accessed March 7, 2011).

Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenges*. Washington DC: Endowment of the United States Institute of Peace, 2006.

Weimann, Gabriel. "www.terror.net: How Modern Terrorism Uses the Internet." United States Institute of Peace. http://www.usip.org/publications/wwwterrornet-how-modern-terrorism-uses-internet (Accessed March 2, 2011).

White, Jonathan R. *Terrorism and Homeland Security*. 6th ed. Belmont: Wadsworth Cengage Learning, 2009.

Wolf, JB. “Organization and Management Practices of Urban Terrorist Groups.” *Studies in Conflict & Terrorism* (1978). http://www.informaworld.com/smpp/content~db=all~content=a789423350 (accessed April 16, 2011).

Academic Vita of Brett Alan Buran

Education: The Pennsylvania State University University Park, PA
Schreyer Honors College
B.S. Security and Risk Analysis, Fall 2011

Thesis: Enablers of Terrorism: Technology and the Web

Technology Skills:

- Cisco IOS
- Windows Server Update Service
- SharePoint
- Symantec Server
- Microsoft SQL
- Windows XP and 7
- PHP
- Perl
- HTML
- Java
- Windows Server 2003 and 2008

Activities:

- President, IST Student Government
- Vice President, IST Student Government
- IST Honors Society
- Teaching Intern: SRA 211

Awards

- IST Student of the Year, Freshman Year
- Dean’s List
- Letter of Recognition – General Douglas M. Fraser
- Eagle Scout