2009

Cyberterrorists: Their Communicative Messages And The Effect On Targets

Elizabeth Minei
University of Central Florida

CYBERTERRORISTS: THEIR COMMUNICATIVE MESSAGES AND THE EFFECTS ON TARGETS

by

ELIZABETH MINEI
B.A. Queens University of Charlotte, 2003

A thesis submitted in partial fulfillment of the requirements
for the degree of Master of Arts
in the Nicholson School of Communication in the College of Sciences
at the University of Central Florida
Orlando, Florida

Spring Term
2009

ABSTRACT

This qualitative study provides a semiotic perspective on cyberterrorism and its opportunity to cause maximal damage while using terrorist propaganda. The very definition of cyberterrorism refers to Internet use, technology, and computer-based networks against critical infrastructures. The application of Stamper’s Semiotic Ladder– morphological, empirical, syntactical, semantic, pragmatic and social world –to the various methods of propaganda utilized by cyberterrorists will uncover aspects on the transition from traditional to modern methods of attack, cyberterrorist communication, and the recruitment of new members to their cause. Additionally, this research focused on the role of the media in the equation of planning by propaganda to the fruition of an attack. Interviews were collected from ten participants during 30-60 minute segments.

Based on the data, five themes emerged: (1) Acknowledgement of the Existence of Cyberterrorism, (2) Postmodern Propaganda and Publicity, (3) Detrimental Effects on Targets, (4) Media Implications , and (5) Communicative Messages. This provides readers with an organized order to the data and provides a way to progressively detail cyberterrorism, with a specific focus on the actual effects of their semiotic intents on targets, on the public, and on the world at large or what is being conveyed. Ultimately, the themes that emerged follow Stamper’s Semiotic Ladder, starting with surface level understanding of cyberterrorism and work up to the global impact of cyberterrorism on various aspects of culture, beliefs, and expectations.

Dedicated to all the men and women who work diligently to protect us.

ACKNOWLEDGMENTS

"Learn everything you can, anytime you can, from anyone you can - there will always come a time when you will be grateful you did." – Sarah Caldwell

I will always look upon this thesis as a road trip. At times, I read the map incorrectly and veered off course. Other times led me to places I didn't know existed. I thank God every day for granting me the opportunity to stretch the boundaries of my knowledge and for allowing me to travel one step closer to reaching my potential.

To the ultimate co-pilot, Dr. Jonathan Matusitz: There are not just enough words in English, French, Dutch, Hebrew, Spanish or German to express my gratitude for your unending support and dedication during this journey. The passion for research and love of teaching that you have showed me in the past two years are more important than 1,000 research studies combined. Your guidance throughout this thesis has made me a better student and researcher and for that I am profoundly grateful. I profusely thank you.

To Dr. Sally Hastings: Thank you so much for your endless patience during the all of the "can I drop in for a quick 5-minute meeting" conversations. Your words of encouragement and fresh perspective were a blessing during the times that I may have stalled on this excursion. I will always be profoundly grateful for the advice and words of wisdom you have shared, as well as for teaching me about the merits of data reduction.

To Dr. Burt Pryor: From day one, you have been a supportive and reassuring voice during a time when I could have veered off course. Thank you for each and every opportunity you have given me in addition to the knowledge you have imparted along the way.

To my parents, Mindy and Larry Minei: “Knowledge is Power.” I have learned dedication, a good work ethic, honesty, loyalty, confidence, critical thinking, humor, values and love from you both. Thank you for your unlimited support and guidance, for your patience and understanding. You have taught me to laugh and take pride in my work. Mindy, thank you especially for your part in this project and for the Marjory/Vicki/Carol moments to come.

To Kirsten Seitz: Thank you for the laughter and for every single minute of every single office hour I ever held. Without you, graduate school would not have been as fun as it turned out to be. Thank you also providing the necessary distractions. I look forward to many more moments in this dance of life (prom or otherwise).

To Mel Sabo: Thank you for spending the past two years working through the “shuffle” of graduate school with me. I have enjoyed our time and the thesis support you have given me from your rightful place on your couch.

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

With every passing year, the changes in technology have provided people across the globe with devices that are smaller and more efficient, electronics that are faster, and networks that hold more information. The Internet alone has proven to bring connectivity to many areas of the world through emails, Webcam opportunities, and a network of information available to anybody, at any given time. With these technological advances growing at such a rapid pace, it comes as no surprise that the technology that is being used by criminals has also had a postmodern upgrade, with the intent of causing maximum damage at minimal cost to the attacker. One such example of destruction has been the distribution of computer viruses, such as the Macro Virus, Melissa the Bugbear virus, and the MSBlaster worm (West, 1999). As global communities display more and more dependence on technology to moderate daily activities and regulate practices carried out by the Internet, the global community becomes increasingly vulnerable to the negative use of Internet technology: cyberterrorism (Clem, Galwankar, & Buck, 2003). Cyberterrorism, a method of attack that damages, shuts down, tampers with, or destroys critical points of national infrastructure by manipulating and controlling computer networks (Sloan, 2006), poses a serious threat to the world's leading countries specifically for the fact that these countries possess economies that are increasingly dependent on technology and computers (Aldrich, 2000).

This initial definition may seem like a screenwriters' dream, and while there have been recent movies, such as *Firewall* in 2006 (Bernstein, Iwanyk & Loncraine, 2006) and *Live Free or Die Hard* in 2007 (Fottrell & Wiseman, 2007), the real life scope of damages featuring cyberterrorism as the predominant weapon of choice is actually ongoing outside of Hollywood. Cyberterrorism either damages the health of human communities or causes a fear of this harm (Clem, Galwankar, & Buck, 2003). In addition, the rationale behind cyberterrorism is predominantly based on motives of an ideological or political nature because cyberterrorists aspire to gain notoriety for their cause (Jain, 2005). Cyberterrorism is not only technical; it is also communicative in nature because it aims at sending messages of violence designed to publicize the attacker's status of power and legitimacy. One of the motives of cyberterrorism is the need for publicity and recognition of propaganda. Cyberterrorists accomplish their goals of power by using propaganda that creates a mindset in which there are clear "us" v "them" mentalities laid out in such a way so that the "enemy" becomes nothing more than a faceless and nameless other (Keen, 1991). When this mindset is widely accepted, it is much less complicated for a criminal to compromise electronic networks, power grids, and other elements of critical infrastructures with intents that may not be exclusively aimed at creating damage (Schweitzer, 2002). It is also fair to say that in addition to garnering recognition, cyberterrorism aims at achieving political goals. One of the key components of cyberterrorism is the use of the Internet, technology, and computer-based networks against critical infrastructures. The Internet revolutionizes the methods in which cyberterrorists communicate, how new members are recruited, and how they advertise propaganda for their cause.

Purpose of Study

The main premise of this study is to explore the communicative intents behind attackers through the use of propaganda and examine how this corresponds to the damage that they cause.

The purpose of this study is to analyze what steps must be taken by cyberterrorists to cause severe damage to targets (both nationally and internationally) with minimal involvement on the cyber attackers' part. As the literature review will explain, cyberterrorists seek publicity; they advertise their deeds and messages. Yet, more research needs to be conducted on the actual effects of their semiotic messages on targets, on the public, and on the world at large. In order to investigate this, I used the method of qualitative interviewing. The research required that qualitative methodology be used and data were collected via in-depth conversational (face-to-face) interviewing. One of the reasons the methodology was qualitative. Was based on the fact that a certain number of the participants are highly secure people (e.g., law enforcement agents and possible FBI agents) who, because of legal constraints, refused to fill out surveys. According to them, one of the conditions to answer my questions was to see the researcher face-to-face. The research was driven by four questions of which the essence was captured in the literature review:

Research Question 1: What are the communicative motives being conveyed through propaganda being utilized by cyberterrorists?

Research Question 2: How do the media play a role in the perpetuation of the propaganda?

Research Question 3: What aspects of the social world, according to Stamper's Semiotic model, are being met?

Research Question 4: How are the aspects of Stamper's Ladder in regards to the social world being carried out?

Now that we know what drives this study, it might prove useful to give a preview of the main points of this thesis. Following a brief explanation of the purpose of the study, a rationale will be given about the aspects of cyberterrorism and semiotics that have been studied as well as the direction of this thesis that will provide fresh insight into semiotics and cyberterrorism. This thesis will continue with a description of cyberterrorism that includes the traditional methods of communication through the Internet, the media that are separate from the computer, past instances of cyber attacks, and the current status of cyberterrorism. Following the overview of cyberterrorism are the explanation and application of the different levels of Stamper's Semiotic Ladder – morphological, empirical, syntactical, semantic, pragmatic and social behavior – to cyberterrorism. Next is an analysis of the documented uses of propaganda by cyberterrorism to date (such as websites, videos, and online forums) that then turn into cyber weapons. A methodology section details the process of finding participants and the collection and reduction of data followed by data analysis that will focus on five themes that emerged throughout the study. Finally, after the data and analysis sections, a discussion of the study including limitations and directions for further research will be provided.

Rationale for Conducting this Semiotic Analysis

This study addresses, from a semiotic standpoint, the significance associated with cyberterrorist attacks and provides examples of how these attacks can be analyzed by applying the theoretical semiotic framework. Thus far, the most up-to-date debate in regards to social sciences and the application of cyberterrorism is rooted in theoretical approaches of game theory (i.e., Lye & Wing, 2005), social network analysis (i.e., Arquilla & Ronfeldt, 2001a, 2001b), and social learning theory (i.e., Jaishankar, 2008). Although semiotic-based models of cyberterrorism have been analyzed by O'Hair and Heath (2005) and Desouza and Hensgen (2007)**,** what has been the primary focus in these studies is an emphasis on the "publicity" that conventional terrorists look to use. To be more exact, what has been established by previous scholars is that cyberterrorists gain publicity for their deeds by evoking fear through strategic images or messages, virus sending, or by outmuscling specific targets (e.g., defacing websites of foreign presidents or prime ministers) by defacing their personal websites or sending other attacking visual symbol.

For purposes of clarification, this researcher fully corroborates with the previously established sentiment that cyberterrorism is a communicative process (O’Hair & Heath, 2005) and would like to further note that there is no disagreement with the longstanding belief of the notion that semiotics is directly connected to the power of symbol and visuals. The semiotic act that can be seen in the form of symbols, signs, media images, and messages are all pertinent to the technologically-saturated interests of the modern world (Miller, Matusitz, O’Hair, & Eckstein, 2008). It is almost obviously apparent those semiotics directly coincide with cyberterrorism when looking at the propaganda that is utilized. Cyberterrorism is perpetuated and publicized through new media communication, it is advocated through the Internet, it is campaigned and recruited for virtually, and this all occurs through public communication channels. By using and exploiting new media, the motives of cyberterrorism to frighten and coerce are ultimately accomplished through semiotics. As an additional component, these messages will be exemplified through instances such as the World Fantabulous Defacers (WFD), cracking into and defacing the official website of Israeli Prime Minister Ariel Sharon, and various cyberterrorism acts in another semiotic function: one that communicates political meaning that conveys more of an ideological statement than a substantial material threat.

With the intent of gaining new insight on the matter of cyberterrorism, this study applies Stamper’s Semiotic Ladder to the phenomenon of cyber terror. To put it briefly, Stamper’s

Semiotic Ladder provides a model of “organizational semiotics,” which expands from the general semiotic approach as a whole. Organizational semiotics constructs the categorization of semiotic understanding by displaying the various and escalating degrees of intensity called the Semiotic Ladder (Stamper, 1996). The construction of this ladder doubles as a depiction of hierarchy by using various points in the system, coupled with a solid theoretical foundation from the recognition that all technology (including that of human skills), knowledge, understanding, and competence must possess some semblance of organization (Filipe, 2000). Stamper’s ladder, working up from lowest to highest, represents six levels: morphological, empirical, syntactical, semantic, pragmatic and social world (Hengsen, Desouza, Evaristo, & Kraft 2003; Hengsen, Desouza, & Kraft, 2003).

Propaganda as a semiotic tool for cyberterrorism is also a heavy focus in this study, with the media being one of the most prominent ways by which terrorists utilize this propaganda (Cowen, 2006). Cyberterrorists use the Internet as another medium for propaganda (Hoffman 2003). Present-day terrorists recognize that the media is a way in which they can manipulate the system, by information gaining as well as spreading awareness and creating the desired images and feelings about deeds conducted, penetrating the attitudes of the public sphere (Laqueur, 2006).

CHAPTER TWO: LITERATURE REVIEW

Cyberterrorism: Definition

In order to understand the full scope of how destructive and powerful cyberterrorism can be, it is important to gain a basic understanding of the actual word. The word cyberterrorism comes from the merging of two words (Conway, 2002): “cyberspace,” meaning the makeup of data, algorithms, and computer networks, and “terrorism,” which is the premeditated, politically motivated violence committed against innocent persons or noncombatants (Deutsch, 1997). Cyberterrorism, at its basic form, is a method of attack designed to damage, tamper with, or destroy critical points of national infrastructure by controlling and manipulating computer networks (Sloan, 2006). The prefix “cyber” suggests that this type of terrorism occurs throughout cyberspace and is, in turn, accessible through computers (Conway, 2002). The basic premise of traditional terrorism is the threat, or the actual use of violence against people or property, with the intention of inflicting enough harm to garner attention, create fear, and influence decision-making (Sloan, 1981). A different concept than conventional crime, terrorism has roots in strong ideological motives, often with a goal of imposing principles and beliefs by illegal and violent means.

Though most instances of cyberterrorism occur with use of the Internet, it is important to recognize that the lesser utilized mechanisms of the telephone also play a role in conducting denial-of-service attacks (i.e., D.O.S. attacks), which render computer networks inaccessible, inoperable, or ineffectual, thus easing the transmission and distribution of propaganda by the attacker (Brown, 2006). One such example of a D.O.S. attack would be a victim who is injured attempting to get help by dialing 911, only to be met with continuous dropped phone calls or just a dead line. In causing attacks, a cyberterrorist has access to any given nation vulnerable to attacks of a grand scale. What this means is that irreparable damage can be caused due to a nation's heavy reliance on critical infrastructure that is rooted in computer networks (Lewis, 2002). Using a universal weapon as seemingly harmless as the computer, cyberterrorists have at their fingertips a medium that allows them to cause great damage with minor consequence (Gorge, 2007). Files can be stolen and corrupted, computer viruses can be spread and these are all due to the easy access provided by the Internet. There is a multiplied threat in some cases, when the attacker is a former employee, familiar with the computer network, and wishing to cause harm (Misra, 2005). The destruction of websites, knowingly crashing selected networks, causing denial of service in crisis situations, spreading malicious computer viruses, causing physical destruction and tampering with financial interactions, all while inducing panic and causing psychological harm to targets, are all utilized methods commonly known as information warfare (Paul, 2008).

This form of attack holds greater appeal than that of the conventional methods used in the past for many reasons. For example, the costs of such an attack greatly diminish when, all things considered, the equipment needed for such an attack does not go beyond that of a computer and an online connection rather that the traditional weapons of guns or bombs used in terror situations of the past (Weimann, 2005). Previous examples of traditional terrorist attacks that were carried out in real time, required massive amounts of organized locations in which attackers utilized software such as robotic networks that globally hijack any number of targets and render them helpless (Aaviksoo, 2008). It is precisely this lack of physical presence in regards to a target that provides a foundation for the rationale behind why cyberterrorism is a preferred method. There is a level of anonymity that comes with a lack of borders, barriers, and authority that leaves an attacker virtually without consequence to target anyone or anything across the globe (Weimann, 2005). This notion reflects the idea that crimes committed via computers are of a global nature in which unleashing worms and viruses that steal information is not limited on a small scale, but can occur between entire countries and nations when attackers are given free rein to commit crimes internationally, against individuals, corporations, and governments (Cassell, 2006). Western infrastructures have been a popular target; so have highly populated areas, both domestic and foreign, which will remain primary venues that become susceptible to attacks (Gunaratna, 2005). Combined with the notion that cyberterrorism is both inexpensive and anonymous, as well as remote, an attacker is not forced into physically demanding high risk situations; nor do they have to be as crafty to outwit security systems (Weimann, 2005).

The rationale for the occurrence of cyberterrorism has symbolically included that of political motivation (Baudrillard, 2002). When emblematic western infrastructures such as banks, hotels, and utilities are considered, the sheer volume of targets becomes endless, causing the focus for an attacker to switch to a symbolic or strategic nature, where the motivation for an attack is fueled by the amount of damage that can be done (Gunaratna, 2005). An appealing factor in the equation of cyberterrorism is that the attacks are conducted from a location removed from the target (Weimann, 2005). An attacker can handpick a target based on vulnerability in various areas of government, health, commerce, and utilities (Brown, 2006). Examples that fall under the assertion of causing damage from a remote location could be that of an attacker opening a dam and releasing flood waters, causing a nuclear power plant meltdown, or causing an oil pipeline to burst (Brownlie, 1963). Because these utilities are run on complex computer systems, there is a vulnerability that is easy for an attacker to penetrate and exploit (Weimann, 2005). For this reason, the shift from traditional methods of attack to the more modern form of cyberterrorism is appealing because physical demands are diminished, the risk of death decreases, and the amount of time contributed by an attacker has less of a psychological effect. This, in turn, eases the burden for terror organizations to maintain the number of members dedicated to the cause (Weimann, 2005). Lastly, and most importantly, there is a media motivational aspect for attackers (Weimann, 2005). As a concrete example of the motivation derived from media attention, in cases such as the I LOVE YOU virus, a virus that caused an estimated $10 billion in damages on 350,000 computers in over 20 different countries (Deal, Gage, & Schueneman, 2001), the media coverage garnered from that incident was larger in volume than could be expected had the incident occurred in one place (Subramanya & Lakshminarasimhan, 2001). When each incident is covered with such depth by the media, an inflated sense of importance and meaning is attributed to each attack.

Now that there is a foundation for understanding exactly what cyberterrorism is and the scope it encompasses, a focus on the communicative aspect is warranted. It is not enough to know that these attacks are occurring. One must seek to uncover not only the method of communication, but the meaning behind the communication as well. One note to mention when attempting to analyze the “intent” of another is the very concept of “intent.” When talking about motives, one must keep in mind that such a concept is intangible and as such will be immeasurable. As a researcher who cannot be certain of the exact motive behind the actions of an individual, one must look at overall behavior to tease out patterns and analyze the symbolic meaning behind those actions. In doing so, an understanding of semiotics is needed in order to place symbolic meaning in context.

Semiotics: A Description

Though it is important to note that any attack can leave irreparable damage, it is the significance behind the attacks that this thesis proposal seeks to address and why an attack can be attributed so much importance. Semiotics is the study of signs and symbols, providing explanations for how meaning is constructed and understood (Eco, 1976). Charles Sanders Pierce, the originator of the concept of semiotics, constructed a basis for understanding, allowing semiotics to make sense of signs, understand their meanings and associations, and process their evolution (Hensgen et al., 2003a). Pierce suggests that words, objects and actions are symbols in life that have meaning because they relate to how the symbols are organized into larger patterns that help understand how the world works, who we are as people, what is important to us and how to act in life (Littlejohn & Foss, 2008). Semiotics provides a basis for the research and analysis of the inner workings of any given organization's culture, systems, and common themes, taking what could be interpreted as mundane or meaningless and approaching it critically, providing an insight to hidden aspects of that culture (Barley, 1983). The meaning-making behind semiotics allows for interpretation to be taken from many forms including that of text and displays from media (Chandler, 2002). The broadest interpretation of places where meaning can be derived has roots in verbal and nonverbal contexts as well as messages that are independent from the source or the recipient due to the nature of the message being recorded. This includes that of video and audio recording, as well as that which had been written (Chandler, 2002). Semiotics can also help to uncover the constructed truth and values of a particular culture or organization, regardless of exactly how much is accurate truth outside of the members of that culture or organization (Kress, 1993). Especially when the idea of modality enters the equation, the boundaries of reality for a certain group may exceed the boundaries recognized outside the specific group in question (Chandler, 2002). When talking about reality, Kress and van Leeuwen (2001) recognize that,

> a social semiotic theory of truth cannot claim to establish the absolute truth or untruth of representations. It can only show whether a given “proposition” (visual, verbal or otherwise) is represented as true or not. From the point of view of social semiotics, truth is a construct of semiosis, and as such the truth of a particular social group, arising from the values and beliefs of that group (p. 159).

Organizational semiotics, a subsection of semiotics as a whole, has led scholars to categorizing semiotic understanding into varying degrees of intensity called the Semiotic Ladder (Stamper, 1996). The reason for this hierarchy and categorization of various points in the system generates roots from the recognition that all technology (including that of human skills), knowledge, and competence need to have some semblance of organization (Filipe, 2000). The ladder, starting from lowest level and working up, represents six different levels: morphological (also called physical world), empirical, syntactical, semantic, pragmatic and lastly social behavior (Stamper, 1996). Morphological, which is the most elementary of the phases, is rooted in physical objects and is regulated to observing individual occurrences in which each object is scrutinized and considered to have been carried out in isolation (Ramaprasad & Rai, 1996). The morphological level is one that can be identified with by recognizing components such as “signals, traces, physical distinctions, hardware, component density, speed and economics” (Stamper, 1996, p. 351). Following the morphological level is the empirical level which is comprised of the understanding that things are observable and that groups exhibit similar characteristics and a summary is reached that categorizes various elements of behavior within groups (Desouza, 2002). Recognizable characteristics at this level fall in the identification of "pattern, variety, noise, entropy, channel capacity, redundancy, efficiency and code" (Stamper, 1996, p. 351). Following the empirical level is the syntactical level which offers a multifaceted arrangement of information by incorporating and connecting objects and agents from the previous two levels to form a new level of understanding and functioning within the organization (Desouza, Chattaraj, & Kraft, 2003). It is at this phase that behavioral patterns are established that will aid in prediction (Polderman & Willems, 1998), inner group norms are constructed (Tricker, 1992), and historical contexts necessary to understand the foundation for which the relationships in that community are built (MacIntyre, 1984). What is being valued in the syntactical level are formal structure, language, logic, data, records, deduction, software and files" (Stamper, 1996, p. 351). An important distinction to make in regard to the six levels is that the first three levels deal primarily in information systems technology with the remaining levels merging the information technology (IT) platform with human information functions. Separately, these levels have no meaning but combined, they offer a fuller semiotic framework that will aid in the recognition and understanding of signs (Stamper, 1996).

The fourth level following the syntactic level is the semantic level, in which a reality can be fashioned because boundaries are built that establish relationships within a system (Hensgen et al., 2003a). This expands the network to a broader range so that there are no restrictions on any one environment, entity or organization, but an all encompassing focus reaching units on a global and transnational level (Baraldi, 2006). This level encompasses "meanings, propositions, validity, truth, signification and denotation" (Stamper, 1996, p. 351). The fifth level, pragmatics, builds upon the previous levels in that there is now a dialogue or communication that breaches the intrapersonal level and meaning is now being formed synergistically. This can be seen through various expressions of "intentions, communications, conversations and negotiations" (Stamper, 1996, p. 351). The final level, the social world, is the culmination of all the other levels working together in action and in turn, affecting those not affiliated with the group to take some sort of action (Hensgen et al., 2003a). These attributes are represented as "beliefs, expectations, commitments, contracts, law and culture" (Stamper, 1996, p. 351). As such, the application of semiotics plays a vital role in understanding how the publicity and propaganda of cyberterrorists are made so effective, respectively, as threats (Skoll, 2007). Because cyberterrorism is a system, the purpose of a semiotic approach is so that an understanding of that system can be formed and consequently analyzed (Hensgen et al., 2003a). By focusing a spotlight on the practices of terrorists and how modern technology has allowed for modern approaches to attacks, the meaning behind the methods, be it media influence, political drive or malicious intent can be uncovered and analyzed.

Application of Semiotics to Cyberterrorism

Pierce (1955) analyzed in detail the various components needed in defining what consists of a sign: a physical representation, something to which the physical representation alludes and somebody with the ability to interpret the relationship. The various phases of Stamper's Semiotic Ladder do exactly that and can be applied to the different instances of cyberterrorism ranging from malicious to extremely harmful. There are many different uses of the Internet that cyberterrorists manipulate to achieve the goals they set out. One study, analyzing cyberterrorist organizations and their supporters found that there were thousands of websites run by these attackers that ranged from exploiting a variety of the unregulated, anonymous, and easily accessible areas on the Internet to communicating different threatening messages to a variety of audiences (Weimann, 2006). Weimann identifies a number of different methods utilizing the Internet with results ranging from psychological warfare to recruitment, networking to other attackers and for the promotion of fundraising (2006). The application of Stamper's Semiotic Ladder takes the various results that have been achieved and tracks the significance behind each choice made by the attackers. It is vital to keep in mind that in the application of semiotics to cyberterrorism, that with each level, another set of meaning emerges in a "from-the-ground-up" process as opposed to a top down arrangement typically associated with traditional patterns of organizational hierarchy (Hensgen et al., 2003a).

To start, the morphological or physical level of semiotics models the signals (events) and marks (objects) as well as the routes and destinations of transmission occurring on a basic and individual level (Stamper, 1996). The restriction of individual attacks carried out by one person can be seen in instances where attackers hope to achieve a self-fulfilling goal. One such example occurred in 2002, when a disgruntled employee, after being fired from a government job, used an Internet connection to release a million gallons of raw sewage along the coast of Queensland Sunshine (Weimann, 2005). E-crimes also fall into the category of morphological as well. Nearly $8 million dollars was stolen from Cisco Systems by two accountants who used the company's computer systems as a means of siphoning funds from company stock (Tedeschi, 2003). One last example of the isolated incidents occurring for self-fulfilling purposes happened in 1992, a discontented employee of Chevron Corporation's emergency alert network penetrated computer networks in New York and San Jose, California and compromised the firm's emergency alert system, setting it up for failure during a crisis (Denning, 1999).

On the empirical level, what have emerged are a dozen or so different occurrences of the events and objects, allowing for the tracking of the physical components of signs that have already been witnessed (Stamper, 1996). At this level, the ability to recognize a group based on characteristics of attacks, and cells (much like criminal profiling) can start to take shape, allowing for continuous tracking of patterns to occur. Specifically, recording examples of denial of service attacks, and grouping Internet Protocol (I.P.) addresses whose signals emitted similar patterns within close times of each other, aid in monitoring and predicting patterns of misuse in a uniform manner over a period of time (Hensgen et al., 2003a). IPs, for example, have common identifiable features that can be documented and tracked. At this level, along with propaganda and a network of communication, cyberterrorism could also include an organized set of attacks with financial purposes to fund subsequent terrorist efforts that aid in the ultimate goal of the organization (Wynne, 2002).

At the third level, syntactical, interdependency has formed so that the parts of the organization are working together and the strength of the mission depends on the strength of the relationships formed between agents of the organization (Lui, 2000). Combined with the synergistic work ethic, meaning is also being established that plays off the meaning of another entity specific to the group (Stamper, 1996). At this level, something critical can be achieved in regard to preventative measure. Up until this point, according to the levels, what can be traced at the morphological level are random, one-time offenses, typically conducted by individuals hoping to achieve something inherent to the self. At the empirical level, what is being seen is the emergence of patterns, but nothing definitively concrete in measures of prevention. The syntactical level displays formal structure and with this structure materializes recorded patterns displaying some logic. This interdependency of meaning at the syntactic level can be compared to a domino effect, suggesting that if one aspect malfunctions, subsequent chaos will affect the remaining aspects of the system. In 2002, the World Fantabulous Defacers (WFD), a known cyberterrorist organization hacked into the website of Ariel Sharon, the Israeli Prime Minister at the time, and defaced it. The following message was left on the website: “The Face of the World’s Biggest Murderer.” At the bottom, following the message, a calling card of the group was left. This example, the WFD’s hacking into Sharon’s official website, is an example in which deeds conducted by a cyberterrorist group could have escalated into a national Israeli crisis (Verton, 2003). In 2005, a CNN television news bulletin warned viewers that a new virus called Zotob was infecting computers, causing them to slow down considerably or reboot continuously at the network’s New York and Atlanta offices (McKenna, 2005). Shortly after, computers of companies spanning the nation were infected with the virus (Cassell, 2006). In addition to that, Zotob acted as a gateway for other malicious software to be installed allowing for sensitive information such as credit-card numbers and social security numbers to be stolen (Schneier, 2005). When the dust had settled, Zotob hit approximately 100,000 companies (Kontzer, 2005). At this level, what can be done, in regards to countermeasures, is the definition of relationships and assessment of correct linkages between these relationships. Though this is a small step, it may be one that is crucial to prevent larger and more dangerous cyber attacks (Desouza & Hensgen, 2003).

The syntactic level dealt mainly in the information level of systems and did not directly constitute connection with human function and knowledge. The semantic level, and first in human information function, is indicative of finding meaning in real world instances by mapping out specific occurrences in a system rather than mapping individual cases (Stamper, 1996). Often, in regards to cyberterrorism, this level is comprised of knowledge that only an in-group member would understand, as in the case of a cyberterrorist organization, knowing all the inner workings of their system. At this stage, certain dialogue has formed so that an infrastructure can be created; information exchanged and dialogue between social networks made meaningful (Laru & Järvelä, 2008). The extent of these organizations can be likened to a full blown subculture, existing abstractly in time in which only the members of the in-group understand the dialogue being spoken and only members of the in-group can function in the organization (Rheingold, 1993). It is at this point that the extension of cyberterrorist targets reaches beyond the scope of local or national community and even extends to the global community. Attacks at this level are primarily directed toward large scale targets with the intent of causing maximum harm, damage, and destruction (Desouza & Hensgen, 2003). One such example is that of Diab10, which occurred in 2006 when an overseer for the FBI's Cyber Action Teams received information from one of the field bases in Seattle, linking him to an email account in Washington (Schneier, 2005). The FBI team received emails from suspects with an alias "Coder" that indicated the emails were coming from Turkey and Morocco, respectively. Only after media coverage of the virus did the suspects express caution, discussing whether they should get rid of the evidence, by crashing or ditching the hard drives on their computers (Cassell, 2006).

Another example at the syntactical level is that of the FBI announcing the arrest of at least 16 individuals spanning countries such as the United States, Poland, and Romania. The criminals were involved in a credit-card theft scam, forcing the FBI to leave agents in the international countries with the intent of surveillance and information gaining (Cassell, 2006). Another example occurred following attacks on The World Trade Centers. Mount Sinai NYU Health System was the target of cyberterrorism in that the data center that handled clinical and business operations was infiltrated for three of the five hospitals that are part of its system, including NYU Downtown Hospital, three blocks from the World Trade Center, losing data and damaging patient files that stored medical and health insurance records (Haugh, 2003). In March 1997, a cyberterrorist infiltrated a telephone company computer that provided service to the Worcester Airport in Massachusetts, disrupting service to the airport control tower, causing a chain reaction among the fire department, security services, and weather service for six hours (Smith, Grabosky, & Urbas, 2004). The primary goal here is to exploit any weakness in a system with the intention of causing a domino effect throughout the rest of the network.

The second to last level of semiotics as it applies to cyberterrorism is that of pragmatics, where the focus is on communication, negotiation and intentions. The "no holds barred" approach at this level is one with rapid mobility in the cyberterrorist organization. This requires planning to the degree that the attacker has chosen a specific target (government or business) with a specific motive (political or non political) and an objective which can range from a minor nuisance to a grand scale, destructive, life-threatening attack (Mathieu, 2007). Massive amounts of preparation in the form of information gathering, detailing plans of attack, performing tests, communication throughout cyberterrorist network, hacking into databases and computer systems, spreading viruses, and attacking individual businesses are put into play in the pragmatics phase (Hensgen et al., 2003a). Another example of the pragmatic level would be websites such as www.alneda.com (Hensgen et al., 2003a) or www.azzam.com (Weimann, 2005) that carry planning messages to and from terrorist leaders (Iqbal, 2002). Likewise, personal websites, sometimes more or less politically motivated, but never implemented on a national level all the way through the attack and then assessment of attacks, are also attributed to the pragmatics phase (Mathieu, 2007). The Estonian government encountered this type of cyber attack, whereby, in early 2008, according to specialists at the U.S. Government Accountability Office, hackers gained access to the electronic control systems of the nation’s electric power grid, shutting it down and causing damage (Aaviksoo, 2008).

Lastly, in the levels of semiotics is the application of cyberterrorism to the social world. Thus far, what has been assessed are the implications of how the information systems, merged with human functions, aid cyberterrorists in planning attacks on their targets. The formation of the in-groups beliefs, expectations, and laws that emerge (and the culture that is created) are all critical aspects have relevancy to the motivations behind these attacks. It has been inferred that the signs that are displayed are directly correlated to the creation of tokens that are significant to the creation, sustainment and alteration of the (in-groups) social world. It has been argued that signs are commonly, and often subconsciously, recognized to be satisfactory indicators, of symbolic images and moods (Lasswell, 1971). These signs and meanings are thus far unknown and it is the intent of the researcher to work toward uncovering what the communicative messages are.

Uses of Propaganda

Verton (2003) explains that,

> al Qaeda cells now operate with the assistance of large databases containing details of potential targets in the U.S. They use the Internet to collect intelligence on those targets, especially critical economic nodes, and modern software enables them to study structural weaknesses in facilities as well as predict the cascading failure effect of attacking certain systems (p. 109)

This approach is considered postmodern, where the premise is that communication is directionless and leadership is not needed, nor does it exist (Matusitz, 2008a, 2008b). The Internet serves as the perfect medium for the trajectory of the modern terrorist: the cyberterrorist. While the tool (the Internet) has been indentified, previous research by Conway (2002) and Weimann (2006) shows that primary means of communication, intentional or otherwise, between cyberterrorist and their targets happen through a variety of employed propaganda. Jowell and O'Donnell (2006) state that "propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist" (p. 7). Throughout the vast history of war, there have been many documented cases in which propaganda has been used as exactly this type of catalyst, igniting motivation during wartime to increase membership in the armed forces (Lasswell, 1971), as a means of trickery (Krippendorff & Bock, 2008), as a way to or to gain a tactical advantage against the enemy (George, 1959), or most importantly, as a way to dehumanize the enemy by creating a realm of "the other" (Keen, 1991). This notion of "the other" is a method in which negative messages become continuously perpetuated, feeding into the Stamper's (1996) explanation of the social world phase. At this level, the formation of in-groups occurs, which allows for beliefs and expectations to form and laws to emerge that dictate how the enemy is portrayed. Once these perceptions of an enemy form, they add motivation behind an attack (Keen, 1991). When there is talk about "the other," entire cultures become faceless, nameless, feeling-less entities that are the target of violence and hate (Keen, 1991). The language used in World War II propaganda consisted of "us" versus "them" mentality messages with terms such as "Commie bear," "Nazi Swine," and "Dog of Capitalism" (Keen, 1991, p. 86), all of which dehumanize a given target. Because the use of propaganda is so powerful, it is important to understand how these various types of propaganda are effective, exactly what types are available for use, and what is the driving force behind that power.

In regards to the question of power, Keen (1991) suggests that propagandist messages carry with them certain influential indicators that affect the subconscious psyche of a culture (p. 56). To begin, it is essential to recognize the media as a strong and prominent outlet for terrorists to communicate propaganda (Cowen, 2006). Another prominent medium in which propaganda is used as a means of communication is through the Internet (Hoffman 2003). A traditional method of terrorist communication previously employed was the use of video as a quick and effective method of relaying terrorist messages. In addition to the main focus of the use of video being a cheap and easy means of distributing propaganda for their cause, a more aggressive and destructive utilization of propaganda using the computer and Internet is through virus spreading (Weimann, 2006). In the first half of 2005, documented worldwide cyber attacks from viruses reached a recorded 237, a 50 percent increase from the same time period, one year earlier (Hoopes, 2005).

Propaganda that follows the traditional model instructs an attacker to spend time effectively gathering intelligence on specific targets as a way to ensure that the maximum amount of damage that could possibly occur actually comes to fruition in each incident (Mathieu, 2007). Certain tactics that are put into place start with extensive target analysis, intelligence gathering, and a network of command and control are considered necessities when attacking a target, all of which are designed to utilize many different directions to assault a target (Desouza & Hensgen, 2003). To continue outlining the merging of traditional method of attack joining a modern view occurs when cyberterrorism facilitators pinpoint targets through the use of computers, by way of propaganda, recruitment, collection of data and information gathering, and member-to-member communication through forums and videos via the Internet (Weimann, 2006). An even more in-depth scope of these computer-based activities includes message posting, launching campaigns of a psychological nature, gathering information on potential targets, allowing for the synchronization of agendas and actions, allotting funds to specific areas, and using videos to conduct virtual terror training (Tzfati &Weimann, 2002).

Continuing on with the understanding of the role of the media in current terrorist operations, it has been recognized that the media can manipulate and form desired images in respect to the minds of the public (Laqueur, 1996). The example of the I LOVE YOU virus was a prime opportunity for media coverage on a massive scale, which only succeeds in fueling terrorist organizations and providing motivation for continued attacks. Publicity and media are considered a necessity in the world of cyberterrorism, outlining two of the primary themes in the motivation of the attackers. Jenkins (1975) proposes that,

> propaganda terrorist attacks are often carefully choreographed to attract the attention of the electronic media and the international press. Taking and holding hostages increases the drama. The hostages themselves often mean nothing to the terrorists. Terrorism is aimed at the people watching, not at the actual victims. Terrorism is a theater (p. 4).

With the suggestion of the motives of terrorism rooted in theatrics, it is akin to suggesting that to be recognized in a highly visible and memorable way is the purpose for the attack; qualities often attributed to media coverage (Cowen, 2006). What is meant by “terrorism as theater” is not an exclusive activity reserved only for a select group, rather a particular and precise display intended for an audience from one end of the spectrum to the other; much like a sporting event or a performance (Cowen, 2006). These “theatrical” qualities – lack of regulation, easy access, vast range of audiences, and rapid information transfer – have allowed the goals of terrorists to be achieved, an increasingly attractive option when terror via the Internet allows for easy causing of damage with decreased fear of getting caught (Rogers, 2003). Terrorist messages such as these are clearly heard worldwide due to well developed and well dispersed media contacts (Kim, Scheufele, & Shanahan, 2002).

Similarly, Internet sites produce numerous opportunities for in-group communication and publicity, documenting a trend that encapsulates cause for organizations (Arquilla & Ronfeldt, 2001). The State Department generated a list of terrorist organizations that confirmed that at least half of the known listed organizations have websites that are used for the solicitation of money and membership as well as a way for coded messages to make its way among group members (Gordon & Ford, 2002). Internet provides the luxury of non-physical contact with another member of the group where new recruits can become affiliated and commit to carrying out terrorist attacks, never actually leaving the comfort of home. In short, the use of propaganda has become the standard norm among terror groups (Harmon, 2001). Terrorist organizations require backing from supporters in the areas of both recruiting for membership and funding in order to continue to operate. Another use for propaganda is to discredit enemies (in the form of creating "the other") all while placing the organizations in a positive light. Traditional propaganda techniques such as leaflets and publications in newspapers have now been replaced by the use of websites for financial backing and membership recruiting (Wright, 1991). These leaflets and newspapers are truly an artifact of the past with the United States Department of State reported as early as 1999, that over one-third of the known Foreign Terrorist Organization (FTOs) had their own website (McGirk, 1999).

Popular radical groups of international significance such as Lebanese-based Shi'ite Islamic group, Hezbollah (Conway, 2002), operate Internet sites and use this outlet for various purposes such posting articles or agendas of upcoming events, or to publish recently filmed videos, which can be accessed by anybody in the global cyber community (Deutsch, 1996). Cyberterrorist organizations also feature disappearing and reappearing message boards and websites (Weimann, 2006). One attacker, playing cat-and-mouse games with authorities through his websites, known as Irhabi007, emerged over the Internet as a leader of an online terrorist organization. His antics included online videos with instructions for home-made car bombs and he also led forums criticizing American foreign policy, only to take them down and repost or list them under a different domain name (Fulghum, 2005). In November of 2005, as a tribute to a suicide bomber involved in the attacks on London, a full length propaganda video entitled the martyrdom will of Mohammad Sidique Khan, was posted by another terrorist group known as Sahaab (Kohlmann 2006) launched on the now-unresponsive website, www.as-sahaab.com. The video bore unassailable similarities to Irhabi007's fundamental Islamist message board that had recently disappeared prior to the attack (Kohlmann, 2006). Copycat websites playing the same cat-and-mouse games began to spring up after Irhabi007's capture in 2005, with messages such as the following: "The enemies of Allah will continuously [try to close down] our website.... We ask you to register for our mailing list so that you continue to receive the latest news of the Islamic Army in Iraq." This post urged followers to continue their membership with the organization, despite seemingly inoperable websites (Kholmann, 2006).

Ultimately causing violent methods of destruction, Internet messages communicated between terrorist groups display consistent themes ranging from hate to anger (Talbot, 2005). Attackers need a starting place. In order to inflict the most damage possible, an attacker needs to research various potential for damage in the process of building a target profile (Mathieu, 2007). In order to utilize the Internet to its fullest extent, cyberterrorists can access a multitude of international areas and databases that contain sensitive information, such as libraries. Starting with access to legally obtained information, through legitimate search engines such as Google, attackers can gather information in the form of maps, satellite images, uploaded pictures and videos and other texts available in seemingly harmless and innocent ways available in a public domain (Paul, 2008). Browsing the Internet to gain information allows attackers to start building profiles against targets using simple resources that are also very much legal. Once the information gathering process on a target has been completed and is recorded, an attacker can then use the Internet as a channel for carrying out the attack. The Internet, by way of computers, is the main tool available for assailants to coordinate and communicate on the method of attack (Paul, 2008). Encryption programs can be implemented to cover any harmful wrongdoing that could potentially be exposed throughout the course of the operation and, as this is being done, a system of hidden messages can be put into place (Paul, 2008). Many of these messages range content-wise going so far to include instructions, step-by-step illustrated renderings of how an attack should be carried out, and detailed communicated plans enclosed in a secure network that requires a designated password to access. U.S. Military computers have shown evidence of being a popular and frequent target by attackers. In 1998, cyberterrorists, cracked into computers used by the Pentagon, using these methods of attack, and downloaded technical materials sensitive in nature (Lenzner & Vardi, 2007). After a federal investigation, the source of the attacks proved to be a Moscow based series of dial-up connections. The investigation, dubbed Moonlight Maze, was ineffective in catching the attackers.

The success of the terrorist group is directly correlated with keeping membership levels at a maximum, and as such, multiple methods of recruiting new members is a major focal point in the propaganda based messages that are employed (Liu, 2000). In past efforts to increase membership among groups, traditional methods of recruitment, such as published written work, audio-video tapes, CDs, and even local prayer leaders have been employed as a means of promoting the cause (Paul, 2008). The Internet, an updated and modern element of global terrorism, is emerging with websites and electronic forums that are used to spread ideological messages and provide hyperlinks between current operatives in cyberspace in addition to sharing graphic images depicting previous successes as a call to action for potential new members (Cronin, 2006). In some instances, donations from sponsors or patrons are requested for those who wish to be supportive without being directly involved (Cronin, 2006). The content of the websites offer up a lesson on the history of the organization, and the cause the organization supports with the intent of enticing new members to join (Paul, 2008). These websites also provide a venue for cyberterrorists to plan attacks by using a variety of methods that could not be achieved through other means.

The use of video provides another powerful arena utilized by terrorist. Video has been a vital part in the process of propaganda that is cheap and globally accessible (Weimann, 2006). Films depicting anything from the morale-boosting success of radical fighters to the more macabre and disconcerting videos of executions, ambushes, and roadside bombings have emerged at a steady and continuous pace, being systematically distributed across the world (Kholmann, 2006). Terrorist group Zarqawi's media chief, Abu Mayasara, displays the power of online videos when he posted, in a forum, an online insurgent video of high ranking members of Zarqawi's organization beheading American businessman Nicholas Berg (Glasser & Coll, 2005). Mere weeks after that video was posted, additional copycat beheading videos trying to achieve the same gruesome effect as Zarqawi's conquest, and dozens of new unidentified Arabic-language message boards, appeared rapidly on radical Islamist websites across the Internet (Kholamann, 2006).

The main difference in film distribution, to compare past methods to present day, is that in previous years, the videos, produced and distributed in traceable brick-and-mortar establishments allowed for easy identification and easy prosecution of offenders, whereas present-day operations are postmodern and join Internet access with software designed for video editing and virtually untraceable upload capabilities (Kholmann, 2006).

In addition to easy access and virtual inability to be traced back to any one criminal, an appeal for the use of propaganda lies heavily in the ability to induce fear on a grand scale, affecting mass amounts of people. Participants who were exposed to clips of terrorism and threats to national security developed higher anxiety than those who were not exposed to such clips, according to one study (Slone, 2000). Perfidy or betrayal is an applicable outcome to the use of videos that rely on deceitful methods because there is a reliance on outcomes that are psychologically damaging, allowing for a tactical advantage to be achieved (Dinstein, 2004).

Damaging and deceitful perfidy could be explained in a more detailed manner in regard to video, when the false construction or the blatant alteration of images or recordings occurs specifically to make a false claim against a party (Army Field Manual, 1956). By extension, videos communicate a message to members of an organization and are used for purposes of displaying examples of previous successful attacks on a grand scale. Another example of the deceitful nature in the form of damaging messages communicated through video comes to light when a multitude of videos are altered to express meaning that had not been originally intended (Slone, 2000). Documented cases have exhibited modified and forged footage, such as falsely spliced voice recordings that depict an enemy head of state issuing orders for war crimes, or digitally altered state uniforms that have been changed to resemble enemy attire (Shulman, 1999). Tactics such as these create consequences that are short-term and steeped in deceit of a political nature. The consequences that occur long-term – that of increased fatalities, extended periods of war, and schisms in the restoration of peace – destroy any foundation of peace that have been gained previously (Army Field Manual, 1956). Additionally, propaganda allows for the perpetuation of “the other,” continuing the mindset of damaging nationalistic pride which “is the language of blood: a call to arms which can end in the horrors of ethnic cleansing” (Billig, 1995, p.48).

Thus far, there is evidence to suggest that through means of technology – video, internet, and media coverage – messages through propaganda are worthy of mention because of the implications they carry from a communicative perspective. It has been suggested that restricted media coverage of terrorist attacks would in turn decrease the amount of terrorist attacks that occur afterward because a primary communicative intent- media coverage and recognition- was not being met (Cowen, 2006). If this is the case, an interesting perspective to look for in the data would be the ties that connect the media, propaganda and the communicative messages that are being conveyed.

What the literature thus far has demonstrated is that, through semiotic gestures and the use of similar symbolic systems, cyberterrorists are capable of communicating their intents. It has been noted, as represented in the semantic and pragmatic phases of semiotics, that the intent is to utilize any output necessary to play upon the fears to the public and by association, enhancing the power cyberterrorists wield. More specifically, this output is represented in coverage by the media generating increased attention and heightening the theatrical element behind each attack. Also demonstrated is a carefully crafted network of Internet savvy members of cyberterrorist organizations who communicate power and status through online video clips, websites and through methods of destruction ranging from the malicious (denial of service), to the irreparably devastating (death). The motives of cyberterrorists are the same as those of conventional terrorists: to send images of fear. In the same way that terrorism is, first and foremost, a process of communication between terrorists and target audiences (Tuman, 2003), a key objective of cyberterrorists is to send a powerful signal, whose meaning is intended to frighten and coerce. Cyberterrorism is a semiotic act; be it a message, a symbol, or an image on a website. Our computer-based universe is wrapped up with images, signs, and symbols. Truly, there is a powerful semiotic dimension to cyberterrorism.

CHAPTER THREE: METHODOLOGY

The third section of this thesis covers the methods used to conduct the study. Before I describe, in detail, what the methods of research entail, it might prove useful to remind readers of the research questions:

Research Question 1: What are the communicative motives being conveyed through propaganda being utilized by cyberterrorists?

Research Question 2: How do the media play a role in the perpetuation of the propaganda?

Research Question 3: What aspects of the social world, according to Stamper's Semiotic model, are being met?

Research Question 4: How are the aspects of Stamper's Ladder in regards to the social world being carried out?

Why Qualitative Research?

One of the reasons the methodology is qualitative lies in the fact that some of the participants were highly secure people who, by U.S. Federal Law, were not allowed fill out surveys. In order to answer my question and give me data, they needed to see me, the researcher, face to face (in a one-on-one interview). To recruit participants working for law enforcement and other federal agencies, I used chaining. Chaining is a process whereby one person tries to get another person *entrée* into a group or community that is usually not open to the public. In the world of law enforcement (L.E.) and other federal agencies, there is a two-degree separation. I attempted, with success, to get interviews with L.E. agents using this process of chaining, that is, through an informant who can be trusted by L.E. agents.

In line with these contentions, what occurred through this process were a few cases in which the participants were not totally familiar with the way cyberterrorist strategies work or what their intents are. Nevertheless, with chaining, this scarcity of knowledge was overcome because the interview protocol allowed for an initial general discussion that determined the overall participant's knowledge of the subject. In a similar vein, I spent some time with each participant creating an informational foundation before the interview continued. I asked the participants broad, experiential queries as conversational grounds for the participant to volunteer their accounts or narratives of their experience or encounter with cyber attacks. However, with a quantitative instrument like a questionnaire (Reinard, 2001), it would be more difficult to follow the procedure described here.

Kvale's Procedures

This section will provide a detailed account of the rationale behind the structure of the interview protocol and why using observing Kvale's (1996) procedures produced positive outcomes. The research employed qualitative methodology and data were collected via in-depth conversational (face-to-face) interviewing, following the procedures given by Kvale (1996). Kvale (1996) calls for seven stages in the interview process: *thematizing*, *designing*, *interviewing*, *transcribing*, *analyzing*, *verifying*, and *reporting*. As shown in the appendix, the interview protocol is based on questions about cyberterrorists, their communicative messages, styles of propaganda, as well as various strategies they use on a daily basis. All this constitutes a semiotic gesture. The interview protocol was designed in such a way that I, the researcher, allowed for the possibility that the interviewees' responses would add fresh insights. The principles of interview set forth by Kvale (1996) suggest that questions asked in interview format are done so with professionalism in mind as opposed to the easy dialogue displayed in everyday conversation. Keeping this in mind, the questions for the interview were created in a way that provided a softened facade of a structured interview schedule, while still attempting to get the feel of an everyday conversation. To add to this, the questions were asked in a way that built upon initial questions that were less threatening (e.g., Would you be willing to provide me with a brief summary of your background in Law Enforcement/FBI/ Cyber Forensic Expertise?) to gradually getting into the topic at hand, cyberterrorism (e.g., What is a cyberterrorist?). By doing so, I was able to provide an opportunity for the informant to get sufficiently comfortable talking about the topic at hand from their own experience before jumping into questions more direct in nature. I asked the participants to recount from their personal experiences so that they had the opportunity to supplement the qualitative analysis and give me a sense of how to interpret the data later.

The Participants

The following section details the methods in which I was able to recruit participants for the study, why they were chosen, the venue in which they were interviewed, and how the identities of these informants have been protected. Data were gathered from information provided in complete interviews with 10 participants. More precisely, these participants answered my interview questions. For the face-to-face interviews, participants were asked 10 interview questions. The whole interview process was designed to last approximately 30-60 minutes and took place in a location chosen by the participant (e.g., the participant's office or a conference room in the building where the participant worked). In select circumstances, due to remote locations across the country, two participants were interviewed via the telephone. Each participant individually was individually interviewed. I met or spoke with each participant only once. Where there was consent, audio-taped interviews occurred. I informed the participants that the audio-tapes would be destroyed immediately after the information (provided by the participants) recorded on each of these tapes was transcribed. In addition to having the audio recording, I was permitted by all participants to take notes while they spoke.

To recruit participants who work in cyber forensics labs and law enforcement agencies, I consulted information located on the Internet and subsequently identified individuals who were computer security experts. My primary source of contact was by email and in some cases a phone call was warranted in which I explained to them the purpose of my study. Before agreeing to participate in my study, and before these participants answered my interview questions, I provided them with an informed consent form and obtained signatures from them. To insure protection of the participants, I assured them that their names would remain confidential and that the tapes would be destroyed after the information were transcribed.

I informed each participant that they were being asked to volunteer for a research study. This study was conducted for the University of Central Florida. I told each participant that they were selected as a possible participant because they were a cyber forensics expert or L.E. agent. I asked them to read the informed consent form and gave them the opportunity to ask any questions that they may have before agreeing to take part in this study.

Then, I informed participants about the purpose of my study. To be more precise, I informed them that this study had no known risks involved. I told them that if they felt uncomfortable answering my questions; they were allowed to not answer them. They were also informed that they could withdraw from my study at any time. I informed participants that the records of this study would be kept private. In published reports, there will be no information included that will make it possible to identify the research participant. Research records have been stored securely. I have stored the data on my computer and have kept these transcriptions safe by locking them into a program file that can only be opened with a password. I have erased each participant's email following the completion of the study. I also informed them that their name will never be mentioned. I informed participants that, to assist with accurate recording of participant responses, interviews would be recorded on an audio recording device/video recording device. Participants had the right to refuse to allow such taping without penalty. In one case the refusal of a tape recording device did occur.

Finally, I provided participants with the researcher(s) phone and email address as well as the contact information for professor directing the thesis, I also included the following statement: "You are encouraged to contact the researcher(s) if you have any questions." If they had any questions about their rights as a research participant, they could have contacted the University of Central Florida Institutional Review Board. They were given a copy of this information to keep for their records. If they were not given a copy of this consent form, they could have requested one.

CHAPTER FOUR: DATA AND ANALYSIS

Cyberterrorism thus far has been established as a complex and intricate process that spans multiple outcomes ranging from nuisance to mass destruction. Cyberterrorism can be committed in places without jurisdiction (Gorge, 2007). Attackers can target critical infrastructures such as hospitals and utility facilities (Erbschloe, 2001) and cause damage that reduces the chance for the opponent to fight back (Schmitt, 2002). One participant from the FBI said it best when he stated the following:

> In a grand nutshell, the main message [of cyberterrorists] is to instill fear in their target population, to disrupt their opponent’s web functioning, to provide information, to obtain funding, to recruit members and gain sympathy from others with similar thought patterns. A big part of this is to look powerful.

Throughout the data reduction process, many themes emerged that were distinct in what was being conveyed as well as instances of data overlapping across participants. There is no clear-cut start or end to cyberterrorism. Rather, cyberterrorism is a cause-and-effect chain of stimuli and consequences that inherently build on each other. The data that follow will be presented in a way that attempts to capture the chain reaction unfolding as each cause-and-effect is laid out. Based on the data, five themes emerged: (1) Acknowledgement of the Existence of Cyberterrorism, (2) Postmodern Propaganda and Publicity, (3) Detrimental Effects on Targets, (4) Media Implications, and (5) Communicative Messages. This will provide readers with an organized order to the data and will provide a way to progressively detail cyberterrorism, with a specific focus on the actual effects of their semiotic intents on targets, on the public, and on the world at large or what is being conveyed.

Acknowledgement of the Existence of Cyberterrorism

It is important for the purpose of this study that the participants identify and define what a cyberterrorist is and what they do. Because of the relative novelty of cyberterrorism as well as an international inability to clearly define what cyberterror consists of, or create global laws for prosecution, it was important to ask the participants what they considered a cyberterrorist to be. This provided an opportunity to work from one foundation. The responses did not vary greatly, but each answer contained an aspect or a component not mentioned by the previous informant. One participant, a cyber forensics expert, summed up the various definitions as a paradigm rather than a concrete theoretical concept. His definition is as follows:

> "Cyberterrorist" is a term that has different meanings depending upon who is using it. A narrow definition would be the disruption of computers and networks by cyberterrorist organizations to create panic to advance their political or social goals. I prefer a broader definition which would be the purposeful disruption of computers or networks to cause harm to further the perpetrators goals. These goals may vary from religious or political ends to personal vengeance.

This definition is one that allows for a greater scope of analysis so that many different considerations, such as disgruntled employees to organized networks set to do harm, may be looked at under the same principle definition. Depending on each participant's experience, there were addendums to this definition that included specific venues for threat such as, "The cyberterrorist message, generally a threat message, says ‘either change what you are doing, or the terrorist will cause significant disruptions or destruction’” or, in the case of organized networks of cyberterrorists, “They all work together to commit crimes through the Internet using computers and forms of manipulation and terrorism toward victims that brings a lot of damage to property and people.” In every interview, the participants spoke extensively on the notion of fear for personal safety, manipulation or assets and as a result, a lack of trust in the government. The participants also spoke of cyberterrorism in conjunction with not only media speculation leading to the increase of fear among citizens, but also the media as a potential source for the perpetuation of information leaking to cyberterrorists. The informants were very adamant about cyberterrorism and the effects as a system that, “If successful, reduces trust and increases anxiety and fear.” This combination of definitions is helpful in gaining a better perspective of who these people are as well as motivations behind the crimes that they commit. These definitions have all been consistent with previous research in that reasons that have been established thus far include coercing a population or government (Clem, Galwankar, & Buck, 2003), intimidation (Arquilla, Rondfeltd, & Zanini, 1999) and to further any ideologies that have already been established (Conway, 2002). The actual number of attacks committed on an annual basis is so colossal that there could not be accurate reporting on just how frequently these attacks occur. One participant, an FBI agent, says of the number of attacks,

> Some agencies, such as the National Security Agency state that they prevent 3,600 cyber attacks per year on U.S. government agencies. That is just reported attacks alone. Many cyber attacks go unreported as private and public companies lose credibility and trust as they lose personal data.

To better understand how these attacks are carried out, one must understand the full scope of tools available for manipulation, weapons available for attack and the public outlets that cyberterrorists utilize to connect with as many targets or members as possible.

Postmodern Propaganda and Publicity

It has been established thus far that cyberterrorists utilize specific technology-based tools that aid in the destruction on the targets. These tools are heavily based in what can be considered a postmodern take on crime. Postmodernism is a movement of the late twentieth century (Docherty, 1993; Jameson, 1991) that supports the idea that humans now live in an age of freedom from imposed rules and social constraint (McQuail, 2000). Cyberterrorism is a manifestation of the postmodern condition, because cyber attacks occur through cyberspace and cyberspace negates geometry. Essentially, the Internet is postmodern because it is anti-spatial (Matusitz, 2008b). Cyberterrorists – as well as the means and weapons that they use – operate in a space that is not an actual place where people can meet physically (Matusitz, 2008a).

As discussed earlier, there is the notion that there is no start or end to the communication that occurs, and no distinguishable hierarchy in regards to leadership roles (Matusitz, 2008b). There have been lists compiled that suggest that tools such as email encryptions, encrypted computer files, websites, audio and video links, circulated photographs, and email have been used as propaganda and publicity for the postmodern cyberterrorist cause. When asked about the ways that cyberterrorist use the propaganda to gain publicity, one FBI agent stated,

> Cyberterrorists are groups that have been identified the by United States State Department as being a terrorist organization that happen to use the internet to

> communicate, recruit, plan attacks, provide propaganda, market, raise funds for the cause, and scope out information about their targets.

As a reminder, Jowell and O'Donnell (2006) state that "propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist" (p. 7). Propaganda has been established thus far as a compilation of tools that a cyberterrorist can have at their disposal. The tools described below; email, virus spreading, websites, and video posts are just a few of the tools that cyberterrorists will use in order to carry out the manipulations and machinations of the task at hand. These tools, all electronically related, are what separate cyberterrorists from the traditional counterparts that came before. Once the electronic component is eliminated, what is left are weapons that similar to the weapons used in violent attacks, such as bombing or shootings.

Tools

Email

Email is one tool used mainly for communication between members of a cyberterrorist organization. As noted earlier, in a plea for the supporters of the Islamic Army in Iraq to register for the mailing list after the terrorist website was closed down (Kholmann, 2006), correspondence in this manner is a legitimate outlet for continued communication. The Diab10 was another case in which Turkish and Moroccan suspects communicated through email with the purpose of causing destruction through virus spreading (Schneier, 2005). Communication through email is a well-known method used by cyberterrorists but there is an often overlooked aspect to the merit of email for cyberterrorist purposes. One participant, a L.E. agent, suggested that there is another reason for email to be used to target victims,

> They [cyberterrorists] use legitimate and illegitimate reasons to contact people, but then may misuse the information they collect, such as identification and personal information. There are various schemes and scandals that are used through the computer, the Internet, and email.

What is occurring here is that not only are scams being pulled on those who may be unsuspecting individuals but there is a key component occurring as well: information gathering. An important and sometimes ignored component in assessing the depth of destruction in the aftermath of a crime is that there needed to be some form of information gathering on a target in the first place. As the same L.E. agent explains in his response,

> These are communications between offenders and victims. Some may be encrypted or very clear. Again, they tend to be manipulative and play on the needs and emotions of potential victims-typically those who are elderly, teenagers, children-generally the most vulnerable populations willing to buy into the scam and would more freely give up information. There may be specific targets or the victims may be chosen randomly.

Email is one way to generate information but it is not the only way. In a speech he gave in 2003, pertaining to a recovered al Qaeda training manual, Secretary of Defense Donald Rumsfeld claimed that, “Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy” (Weimann, 2006). Information gathering occurs through a variety of measures including but not limited to email and websites.

Virus

One of the most common forms of attacks on victims is that of virus spreading (Melissa Macro Virus, the Bugbear virus, and the MSBlaster worm) and the destruction that occurs following the corruption of a computer network. One L.E. agent recounts an instance of cyberterrorism that he and his unit were directly involved in:

> I personally have been involved in several cases of cyberterrorism. In most cases that were investigated by my previous agency, the cyberterrorism involved the destruction of valuable organization files by disgruntled employees, essentially acts of vengeance by a person who had felt they were wronged by the organization. In one case, for example, a computer technician, angry at a police department decision, placed a "logic bomb" in the police computer system that was employee.

Other examples of cyberterrorist employing some sort of "time bomb" virus program were in documented cases where these criminals, with the intention of closing down major switching hubs, programmed a virus to obliterate emergency 911 services throughout the eastern seaboard, in order to cause the collapse of all switches in Manhattan (Denning, 1999). Another case in which a cyberterrorist could cause destruction would be the instance in which the end goal of a cyberterrorist was to shut down an emergency medical services (EMS) dispatch center; given this, the damage could be done by launching a computer virus rather than detonating explosives, which provides a greater risk to the attacker (Berinato, 2002).

Websites

It is safe to say that in the technological age of present day, there are millions of websites being run right now, thousands of which are supported by terrorists. Websites provide an unregulated and unidentified arena where the rule of thumb is “anything goes” from transcribed speeches from political leaders hoping to change public opinion, to a gift-shop like outlet allowing for the purchase of bumper stickers, and t-shirts sponsoring the organization (Weimann, 2006). The interesting notion, as mentioned before with the cat-and-mouse nature of Islamist cyberterrorist Irhabi007 (Kholmann, 2006), is that these terrorist websites are frequently put up and taken down so they can cause their damage and still be maintained for another day. The general scope for the use of websites is so vast that they provide a forum, or a safe haven for any level of content that a cyberterrorist feels is necessary to air to keep motivation for the cause intact, for reasons of member recruitment or to raise funds from supporters. As one participant suggested, “Cyberterrorist organizations around the world have people that are dedicated and communicating back and forth to enhance and promote and fund their operations. They are organized.” Any number of these reasons can be considered practical applications for the website, as if it were a business venture. In regards to cyberterrorists and the defacement of other, legitimately purposeful websites, one participant, an FBI agent stated,

> Many cyberterrorists target sites that are in competition with them or critique them. For example, I know of several [legitimate] sites that are constantly being attacked. One group hacks the site and posts pornography links on the web site that users would find

> immoral and disgusting. Others post their group identification in the form of threats to instill fear in the usual web site visitors.

Outcomes of this nature play upon the psyche of the targets in a way that, while it is not life threatening, the outcome still retains unfavorable consequences. Another FBI agent recalls a similar instance in which the website of a government figure was defaced:

> I was peripherally involved in an investigation of an act of cyberterrorism directed against President Clinton’s White House website. The President’s website was vandalized and a number of defamatory statements were placed on the site. The cyberterrorists were quite sophisticated and defeated some excellent software. Our investigation suggested that the attack was launched from China, and may have had Chinese Government support. We found overseas attacks such as this one very hard to trace, and we were never able to fully identify the hackers.

This excerpt brings up a notion that was consistent throughout the interviews. Because of the nature of cyberterrorism, actually capturing a criminal has thus far proved to be difficult. Every participant, at some point during the interview, suggested that what can mainly be accomplished is countersecurity on the part of the United States. One L.E. agent even stated that “They use the same available tools that we could obtain from internet sites or hacker groups; it could be anybody out there with computer skills building a website to suit whatever criminal intent motivates them.” The notion that any content could be posted by any person credits the damage that could be done by an individual or network hoping to cause destruction.

Video Posts

Because websites have become a public forum for the opinion of anybody, relayed to anybody who will listen, there is no regulation on what can be posted or what ultimately does get posted on these websites. The most salient and destructive tool that could be used by a cyberterrorist network creating and maintaining their own websites is that of video footage. It was mentioned earlier that many pieces of footage could be altered to create fabricated circumstances with the intention of manipulation based on a falsehood, such as the digitally altered uniforms on soldiers, or a fake press release of a prominent figure declaring war (Shulman, 1999). A cyber forensic expert commented on the destruction that could occur from these altered videos:

> It is so harmful because these networks take footage and manipulate it in such a way that they portray terrorists as heroes, in some cases martyrs for a cause. They take video footage of the soldiers before, giving a testament to good and evil and right and wrong and they post footage of attacks on the websites for anybody to see. They can also post events where they can do everything live. Posting video, making hostage tapes like the Nicholas Berg beheading, terrorist interviews and making press releases, well those are the factors out there for anybody to witness.

Along with the video footage on these websites are running live tallies of pertinent statistics to the website: how many martyrs were killed and a running total of killed Islamic enemies (Weimann, 2006). The goal for anybody watching these tapes is ultimately to become fearful. The following is from a cyber forensic expert discussing the motivation behind the posting of videos in how they relate to attacks that are carried out after the posting of these videos,

> Well I think we see it in cyberterrorist propaganda. We see these “tapes” made by Osama bin Laden or somebody designated by him--- they come out periodically with these threats…and most of that is just rhetoric. They are trying to keep the fear level up and the intimidation level. But then periodically, obviously when something happens around the world, whether they are directly involved or not, a major explosion or something, they always try to take credit.

It is the observation that the rhetoric played out in these videos is meant to keep fear and intimidation levels up that is important in the overall understanding of cyberterrorist use of propaganda. The same idea goes back to the notion of “terrorism as theater” in which the main goal is not to harm as many hostages as possible, rather, get as many people as possible to see the harm and consequently become affected by it. This aspect allows for the duel benefit of causing immediate and recognizable physical damage as well as having the psychological damage unfold at a later point in time. By posting violent videos on websites that are self-run, they can control the arena which allows for strategically planned out content put in place for viewers.

The timing of these videos is crucial to the fear levels as well. September 11, 2001 has been touted as a day that nobody will ever forget. Even the numerical date itself (9-11) is symbolic in that the universal number for emergency response systems in the United States is 911. One FBI agent suggested that cyberterrorists play upon this as another fear tactic meant to scare:

> The biggest thing is that they get top members or leaders to put out these tapes and that’s how they actually put the message out and disseminate that threat for us to see. Our [the nation’s] threat level doesn’t change when those messages come but it sort of brings you

> back to where you were on 9/11 or where you were when a particular tragedy occurs so it sort of resonates again what the potential is. The videos are a big source of fear and then any time the anniversary and dates come up the chatter will increase and they start to make those threats again. When we prosecute the ones that were convicted or execute terrorists, those dates are very symbolic, so people sort of get nervous, like 9/11 for example for the most part is fear-driven. We will see those tapes surface right around those times as well.

As explained by this participant, there is a lot of symbolic emphasis placed upon certain dates, such as September 11th or specific dates of terrorist executions. The important aspect of his comment to pay attention to is that even though the threat levels do not escalate when these videos turn up, there is enough chatter generated to allow for people to have an emotionally trigger response. The FBI does not place emphasis on these tapes as proof of threat, but the people that may see them, that also may be affected by them are citizens that do not hold a position in the government and as such may be susceptible to increased levels of fear.

Detrimental Effects on Targets

Up until this point, there has been a strong focus on cyberterrorists and the tools utilized to cause damage or instill fear. Little has been dedicated to the targets themselves. Targets on the battlefields of war are soldiers wearing a different uniform. Targets in gang wars are those who are trespassing on “turf”. One may ask “who exactly is a target of cyberterrorism?” The answer across all the participants is that there is no answer. One L.E. agent summed up a target list best by stating, “Government, financial institutions, individuals, businesses, social groups, political parties, and the list goes on and on…" This list is so extensive and so all encompassing that the equivalent would be to say that there is nobody who is safe from attack. It is in the infinite number of possibilities, from the government to the everyman that leaves people fearful and lacking in trust in those who offer protection. While the primary goal of terrorism is a process of communication between terrorists and target audiences (Tuman, 2003), cyberterrorism also seeks to send a powerful signal meant to frighten and coerce the target. The following section will detail the various motivations behind small and large scale targets and the emotional aspects of fear for safety and lack of faith in the government that accrues from being targeted.

Small Scale

By calling this specific group of targets "small scale" targets, it is not the author's intention of minimizing what could be considered a traumatic experience. Rather, the label "small scale" refers to the amount motivation behind the attacker and the overall product left after an attack. One participant stated "Cyberterrorists, by the nature of destruction (to computers and networks) – are purposeful and designed to sow panic. The motivation is more along the lines of political or revenge as opposed to theft, or profit." By calling a circumstance "small scale," it can be classified the latter: motivation for an attack as revenge. In most of these cases, the threat comes from an attacker who may be a former employee, familiar with the computer network, wishing to cause harm (Misra, 2005). An example of cyberterrorism as an attack of revenge took place in 2000, when the Maroochy Shire Council's computer system was penetrated by an Australian cyberterrorist (a disgruntled consultant who was rejected for a job at a water treatment plant) who manipulated it to overflow raw sewage, causing contamination along the Sunshine Coast (in Australia) releasing 264,000 gallons of raw sewage into rivers and parks, (Clem, Galwankar, & Buck, 2003). Granted the release of that amount of raw sewage is not destruction on a small scale, but rather the motivation for a rejected and disgruntled job applicant was the mess that was made as an act of retaliation, as opposed to meaning to cause long term and lasting emotional damage and fear.

An additional concern and one that has been mentioned earlier is information gathering on a target for purposes of mal intent. A cyber forensic expert expounds on the notion of specifically targeted victims for purposes of gaining additional information through sources that the victims would typically trust by stating that,

> Anyone can be a target; just like other criminal activity. Even those who don't use the computer or the Internet can be conned and have their identity unknowingly stolen through computer programs used by banks and public institutions or agencies. They play on vulnerable victims. These victims tend to be sympathetic, needy and greedy- generally there is some form of mental or physical harm involved.

The overall trend in small scale targets is some other means than the notion of terrorism as theater. In both examples, the end result was raw sewage being overflowed or identity theft. These are goals in which the perpetrator would not want to draw attention to his or herself because once this occurs, the end goal has been compromised. Because these crimes have fallen into a small scale motivated by revenge or scam, they do not qualify as a large scale target.

Large Scale

Where the small-scale targets are considered to be motivated by revenge or scam, the large-scale targets have more severe outcomes like financial collapse, violent trauma for victims and fatalities. With large scale targets, there is greater potential for a chain reaction of events that cause damage. One example of this chain of reaction, given by one participant, an FBI agent said, "After an attack, major impacts are usually cost – cyber attacks lead to expensive counter measures. From there, lack of trust among people who rely on the target, and eventually the sowing of discord within a population." This example illustrates how, when there is an attack (especially one that compromises the financial and economic foundation of a country), the emotional reaction is heightened more than if it were an isolated incident like the one about the Australian employee. The next excerpt from a FBI agent clearly outlines the chain of reactions:

> I don't think you could put a monetary figure on it. I would just think it would be substantial. Huge damage could be done to the commerce of this country, to the financial base of this country, in a single keystroke if they were successful, periodically shutting things down for days and that also would instill a certain amount of fear because then people lose their sense of confidence that the government could protect them. Cyberterrorism is a little different from normal terrorism in that when a bomb going off is immediate, it's horrible, and again it brings a lot of damage to property and people. Cyberterrorism may not instantly physically hurt an individual but collectively could hurt the country substantially.

The key elements to look at here are that cyberterrorism does create damage, albeit not always in the way that traditional terrorism would cause immediate and catastrophic damage to a person's physical well being. The second element to look at is that, not only would the systemic workings of a financial entity be out of commission for up to a few days, but the result would also be people losing a sense of confidence in the ability of those whose job and expertise are protection. Another aspect to assess is that widespread damage would occur. In the case of a bombing or physical attack, the wave of how many would be effected would be those immediately targeted, family members of those who are targeted with the potential to reach others beyond the scope of familiar ties. With the instance of cyberterrorism, it is important to note that those who are affected could reach beyond the scope of immediate targets, but branch out across the country. The example of finance is perfect because of the countrywide dependence on monetary stability. The very last aspect to keep in mind is the notion of "a single keystroke." While a single keystroke may be a hyperbole, it does hold ground in the reality that, with cyberterrorism, one is not combating masked attackers with guns, or soldiers or any other picture of "enemy" that comes to mind. What one is dealing with is potentially a single individual, with one computer, pressing the right buttons. The nameless, faceless enemy plays into the fear of the unknown for those who were attacked and it has been a reoccurring theme throughout all the participants' accounts that these criminals are rarely, if ever, caught and prosecuted.

It is important to keep in mind the notion of cyberterrorism as a chain reaction of events that play upon each other. Thus far, it has been established that cyberterrorists cause destruction and target victims using the Internet. They attack others' websites and deface them and they use their own websites for communication in the group. The following comes from an FBI agent in response to the emotional impact cyberterrorism has on the targets:

> Three major groupings – databases, networks, and websites. Databases are deleted or compromised, usually involving financial institutions, causing financial panic. Networks

> are interrupted with the purpose of compromising infrastructure (electric grids, communication grids, etc.) again, disrupting the citizens lives – making people lose trust. Websites are defaced, again to make people fearful and communicate the terrorist's message.

This excerpt is important because there is recognition of the message that the cyberterrorist wants to communicate. The phrase "to communicate the terrorist's message" allows for something broader than just the pleasure one would get out of defacing a website. These criminal acts fall into the larger scale, where the motive or intent goes beyond just being a nuisance, or creating some other havoc on a target. The additional component is emotionally driven, designed to provoke a response out of the target or whoever else may be watching. It still stands to reason, even in light of preventative measures that certain elements of fear are still pervasive in the minds of citizen. The following section details two distinctive components of fear often mentioned by the participants: fear for safety and lack of trust in the government.

Fear

Up to this point, the participants have detailed effects of cyberterrorism that play a part in affecting the psyche of the population. One participant said it best when he noted,

> Quite often the terrorist action seeks a multiplier beyond the immediate damage cause by their cyberterrorism, they generally provide a threat as well of continued damage unless their demands are met. In most cases the fear, the reaction, and the uncertainty is more damaging that the actual damage wrought by the cyber attack.

This example is yet another that suggests that there is something more to an attack than what damage can be viewed at the surface level. It has been noted through multiple examples and participant responses that these important, emotionally driven aspects are a major contributor and component to the overall scope and results of cyberterrorism.

Safety

Building upon what has already been discussed, there are a lot of different outlets, such as websites, videos, and email that allow for the dissemination of cyberterrorist messages to the public. As one FBI agent comments,

> What I am being told as far as a base threat they communicate a lot over the Internet and they will intentionally send messages to each other and the pubic as a demonstration. They say "look what's happened in this area or look what's happened in that area" and they threaten to mimic those events worldwide. And that is where they basically instill fear. If there is someone associated with the organization, they can kill people or cause an explosive to go off that instills fear in other people because now people recognize that they are vulnerable and now all of a sudden that could happen anywhere. When you see that tactic go off, that's when a smaller man can create a large widespread form of fear. The group communicates in many different ways and now again those are things and information we receive that are work related but that small event can create a lot of fear where we are.

Once again, the main premise is that the end goal is not the damage that occurs from a given attack; rather, it is the ensuing fear that results from that will stay with participants for a longer amount of time that is a major premise for attackers. Additionally, when there is fear of being attacked, civilians look toward those with specialized background for help and, in some cases, there is no answer to that. Civilians may start to question who will protect them and how. Government agencies, whose job it is to protect civilians, may be at a crossroads for how to stop these attacks from occurring.

Loss of Trust

This is not to say that the government officials not aware or working on solutions to protect from cyber attacks. In fact, they are very much aware because that have been the target of attack themselves. When faced with the crossroads of how to go about protecting the public, an FBI agent discussed the FBI perspective of the attacks that have been plaguing the government,

> The cyberterrorists target what I would consider sensitive agencies and operations. I would note the fact that every day there are people using computers to get into the FBI databases for the purpose of embarrassing the FBI, or to taint the data, or somehow introduce viruses or whatever. It goes on in the Pentagon, NSA, in every major U.S. agency trying to guard itself against that type of an attack because the cyberterrorists know how a network system operates and will attempt to shut down a considerable portion of the government. If they are successful. If for no other reason it could be a prelude to a standard violent attack somewhere just to get our attention. I would say that cyberterrorism is every bit as sophisticated as we are and they are working diligently to try and penetrate every secure system the U.S. government operates at all times. I am sure that an attack on a power system or like the attack in Atlanta in the CDC, shutting down

> and penetrating their operations or get into their data base would be damage to us. If left unchecked, cyberterrorists could accomplish anything they want to. I know for a fact that the FBI and the CDC and all of the military operations are dedicating huge resources and bringing in all kinds of talent. They've been programmed to just secure the operations so that hopefully they can stay one step ahead.

This account is one that fortifies the claim that cyberterrorism is penetrating even the highest and most protected agencies in the United States. The noteworthy aspect to this account is that there are people who are put in place and whose sole job is to prevent these attacks from occurring.

Additionally, there may be situations in which the lack of trust spills over into situations of healthcare professionals. Janczewski and Colarik (2005) address the notion that there may be a lack of trust that occurs everywhere, from the civilian population to authority figures including government and medical authority. The example given for health situations stems from records that could have been tampered with in a hospital. Janczewski and Colarik (2005) give the scenario of a major political figure being admitted into the hospital for a medical issue, and have a cyberterrorist gain access to a hospitals' medical database and change the medication to something that person may be allergic to. The nurse administers the drug and that patient dies. This same scenario can occur with people who are not high profile; rather, they can be patients admitted for routine medical procedures. In the same vein, cyberterrorists could tamper with medical or health insurance records, or modify computer-based prescriptions to life-threatening doses at pharmacies (Rockel, 2005).

A lot of information was mentioned about fear for safety and the lack of trust that citizens have in the government's ability to protect them. It can be easy to fall prey to the expectations set forth in movies and television shows like *Live Free or Die Hard* and *24* that portray the most extreme aspects of cyberterrorism. In reality, the source of information about cyberterrorism that gets disseminated to the public is the media. In the following section, the role of the media will be discussed as well as the effects and consequences that occur as a result.

Media Implications

By and large, the media is an entity that plays a significant role in explaining, reporting, teaching, and at times, persuading the audience to take some sort or action or instruct them on how to feel or behave (Barry, 1990). In regards to how this pans out for cyberterrorism, it is safe to say that those who wish to do harm know the media functions and manipulate them to serve their purpose. Because the media is such a strong outlet for communication to the public, cyberterrorists are aware of the potential and seek media attention for a variety of reasons. A L.E. agent elaborates on the media's role in cyberterrorism by stating "Cyberterrorists look to attacks that will gain publicity, threaten the public, or lead people to lose faith in either their political or financial institutions. An important component of most cyberterrorism is media attention." This section will cover the functions of the media and the effects and consequences that come from media attention.

Media's Role

The role of the media was brought up many times over the course of all the interviews that were conducted. There must be a venue connected with cyberterrorism that advances the propaganda: the media (Cowen, 2006). All participants were willing to concede that the media plays a significant role in not only disseminating information to the public but quite unexpectedly, there was an overwhelming amount of criticism of the media from many of the participants. Many participants were quick to suggest that the media plays more of a negative role in the scope of cyberterrorism rather than a positive role. Participants often accused the media of being a hindrance to investigation or creating spin to influence outcomes of emotional effect on the public. The following excerpt comes from a cyber forensic expert with respect to the multifaceted roles the media plays:

> The media influences criminal activity in several ways and this holds true for cyber crime as well. (a) They bring crimes and criminal activity information to the public; (b) they investigate reports of criminal activity; (c) they often put fear into people with their reporting; (d) they tend to hype news up in order to make a name for themselves; and (e) I would guess that the media in general are not aware that the Internet can be a dangerous tool for offenders and potentially dangerous for victims.

The criticism that the media spins reports was emphatic throughout other interviews as well, with examples that participants chose from their own lives. There were many examples that participants gave from their own lives when the media interrupted or compromised investigations or caused unnecessary fear. One FBI agent, who made it clear that he was not a fan of the media's efforts in reporting, recounted a story that was unfolding at the time of the interview. The location of the agent is blanked out for privacy purposes. He stated,

> I can't think of the guy's name, local here in ----------- and he set up an internet site, he was talking a lot about the government, not that it was a crime. But he was pumping out what was happening over in Iraq and he was saying how wrong it was and how his

> beliefs were about how much support the terrorist had. The media showed up at his house and his web page was done in Arabic which was difficult to understand but they translated it over the news and they basically followed this kid and focused on why he would say such things, why would he create this web page. He was *one* person, a 20 year old kid, who worked in some type of computer programming job and he was savvy in computers, but he created this web page that just sparked an enormous response from --------- and all he did was have a P.C. and the right frame of mind. What resulted was he was on the news he-- bringing back memories of the war, bringing back negativity from what he was putting out. All he meant to do was create this web page, but, he certainly passed on a vulnerability to ---------- and we were certainly accessible. It's a propagation that is fueled by the media. They [the media] could try and foster more fear out there than probably reality warrants at times.

This excerpt is a classic example of how the media runs with a story that may not be entirely grounded in things relevant to the subject at hand. In this case, the media was calling this person a cyberterrorist, when it could have been looked at as a freedom of speech. The participant in this story references the feelings that were brought up in the community by the media taking on this story over a prolonged period of time. He mentions that from one website and the subsequent media attention, negative feelings of insecurity and vulnerability about war efforts was brought to the forefront for anybody watching the news to relive again and again.

Throughout the interviews, there was a lot of focus on the consequences that played out that were attributed to the media. In the next section, the discussion focuses primarily on the media spurring negative reactions from those who wish to do harm.

Effects and Consequences

The participants of this study time and again told of how tactics in dealing with an enemy must be chosen with care. Though there was a great emphasis on the media as a grasping entity designed to increase ratings and money, the main concern for participants was ensuring that the enemy did not get the upper hand in the attacks. A L.E. agent told of his dealings with the media and the caution that occurs when relaying information:

> I would guess that the information is limited as many in law enforcement know that the media presents stories in ways to make bucks rather than to inform. We do not want to provide details that would either lead a group to define themselves as successful or encourage further attacks.

This passage is significant because there is an emphasis on counter communication with the cyberterrorists themselves. Cyberterrorists recognize that the media must be used in order to manipulate and form desired images in the minds of the public (Laqueur, 2006). That law enforcement as a whole is looking at the media communication that they report and analyzing it is a testament to the power, good or bad, which the media yields. As a mode of communication, law enforcement is using the media as a vehicle to yield a report that will best serve the public. It does no good to any of the parties to misconstrue the details of an attack for purposes of "hype" because it has been established that while cyberterrorists can communicate by using the media, they can also be on the receiving end of communication. At this point, the media is aiding in the transaction of communication. In the next example, an excerpt by a L.E. agent, this transaction can be better identified.

> They do have a role when it comes to visual pictures and all the information they put out and that fear spreads. I am not a big fan of journalism so I have to put that up front. I think they disseminate and should pass out information on how to protect yourself and they also refuse to allow law enforcement typically to provide the basic information. There are few cyber attacks reported and if there is one, the media overplays the risks and tries to gain ratings by reporting all kinds of myths. It is possible that the media may encourage others to follow suit in a so called copycat crime. It is devastating when the media discloses information that may be used against targets. We in law enforcement try to vindicate that perception of fear and not capitalize on it

The notion of copycat crimes is the first that has been mentioned about criminals committing a crime based on something they have seen rather than the media reporting what they have seen based on a crime. Another interesting point in this excerpt is that use of “we” by the L.E. agent. It is clear that there is no love lost between law enforcement and the media, and there is definitely a tension occurring that does not allow them to work together for the good of the nation and for the good of protection.

Lastly, in regards to the media, it is also important to understand that the role of the media as a source of communication for terrorists has changed. The media was once used as a jumping-off point for terrorists to advertise their videos (Begleiter, 2001). There threats and demands would be recorded on tapes and sent to agencies (government or media) for terrorists to have demands or ideologies heard. A postmodern take on this is slowly phasing out media participation and replacing it with live feed on websites (Begleiter, 2001). With the advancement of technology and cyberterrorists advancing as well, there is less and less of a need for an intermediary in terms of getting the media to post videos. One of the most popular examples, that of the Nicholas Berg beheading (Glasser & Coll, 2005), was a testament to the circulation of videos that was completely annexed from the traditional media. This example is pertinent in that cyberterrorists no longer have to worry about the rules or censorship that accompanies the media. A cyber forensic expert broke down the cycle in the following excerpt,

> In terms of the terrorist interaction with the media, it seems that the internet is functioning as a source of change in communications. They [cyberterrorists] basically can function using a particular medium and that effected overall interactions. They have to put their events together much like any organization in the format that would be easy and palatable for a news organization. For example they call news conferences. The new media of a posted video on a website, much like the traditional consumer now allows the audience member to select the time the place and the device that they are going to get the drama. So the interactive media become much more important, unlike the news media that can censor what is heard. Now they just post the content and send it directly to an audience. There is no censor that their population sees. Most media is a two edge sword, it's liberating in terms of content but it also gives audience access of what is out there from groups that you are not comfortable with. It's much more direct now. You get a lot more live coverage produced by these cyberterrorists.

This excerpt is so important because it features an independence from the media that has not been discussed up until this point. This excerpt discusses the potential for these cyberterrorists to place anything and everything they desire on the web for anybody to access. Some people could say that the public should not access it, sparing themselves emotional consequences they might not be ready for, but in essence that does not solve the communicative problem at hand. The reality is that the content is posted, the messages are communicated, and there is very little that can be done, especially because, as it was mentioned before, these criminals are computer savvy, putting up images for and taking them down, cat-and-mouse style.

It has been discussed up to this point that a cyberterrorist uses propaganda as a means of causing emotional fear and lack of trust in the government’s ability to protect them. It has also been established that the media plays a vital role in disseminating information and facilitating a transaction of information to eventually return back to cyberterrorists. In the following section a bulk of the research questions will address the perspective of analyzing what is being communicated.

Communicative Messages

This section will detail the communicative messages that are being played out by cyberterrorists utilizing propaganda and how the semiotic aspect of Stamper’s Ladder play a part in the overall equation on the targets. To be more precise, the researcher, examined these issues, attempting to synthesize the participant’s responses.

Research Question 1

What are the communicative motives being conveyed through propaganda being utilized by cyberterrorists?

The communicative messages being conveyed by cyberterrorists are multifaceted. What the data have shown is that there are many potential motives to carrying out these actions. There have been motivations of causing unrest and fear in targets, just as there have been motivations of shaking the faith of citizens in the government’s ability to protect them from harm. There may even be emotional repercussions of those whose job is to protect manifesting in the form of doubt or questioning the ability to perform. There is also the concept of terror as theater which sparks motives of wanting attention for misdeeds. Many participants spoke on the overarching theme of cyberterrorists and the notion that the goal is not about the “kill,” but more about who is watching the kill and what follows after that. The notion of terror as a theatrical process was reinforced by one participant, an L.E. agent, as he sought to emphasize what the criminals ultimately want to convey.

> Understanding what cyber criminals want to convey can vary from case to case. I would say it is on a continuum from an unorganized plan of communication to well-organized planned communication. Often it is an issue of control; they want to “flex their muscles” and have some control over their victims, promote a cause, or put fear into a country or region, as the terrorism of Sept 11, 2001 did to the United States.

Again, the notion here is that every movement, every communication, and every web post or link to a video clip is symbolic in ulterior motives. A web video of a beheading is not constructed solely for “entertainment” purposes; it is to symbolize strength and disregards for rules. It is to say to the world at large “We know you have rules and we do not care.” It is a symbolic message that causes fear and panic and puts doubt in the minds of citizens who thought they were otherwise protected.

When cyberterrorists hack into websites and deface them, it symbolically represents a challenge. It is not just an attempt to mess with, or annoy, the website owner, especially when the owner of the website is a political figure. The message that is being sent, again, is a challenge to the authority and the integrity of the law system and the ability for the government to protect its citizens from any potential danger or damage that could occur from an attack. The message also serves as a symbol to those who are not affiliated with the website owner, but who may encounter the defacement and become alarmed.

Research Question 2

How do the media play a role in the perpetuation of the propaganda?

This research question is a continuum of what occurred previously in messages that were sent through propaganda. Without media input, there may not be as much fear circulating about cyberterrorism simply because people may not be aware of it. An overwhelming response from my participants, pertaining to questions about media, yielded sympathies that were negative or critical of the validity and caliber of reporting. Yet, it is irrefutable that the media perpetuates the propaganda be it through misreporting to create hype or simply by reporting on an occurrence which, in turn, fuels the morale of the cyberterrorist group to be recognized, and which, in turn, fuels the mission. A cyber forensic expert commented on what the media's role in inadvertently perpetuating cyberterrorism:

> There have been a number of examples of the media perpetuating cyberterrorism. The PLO is an example of a terrorist group, evolving into a political governmental amphitheater. That transition added to the Hamas right now, has gone through a transition and the goal of the terrorists group is long term, particularly if the goal is to get media coverage, recruitment and resources and makes them the dominant group in that perspective. There are triggers that I have put together such as is the media showing footage that is brutal or unique, or is there a symbolic value or are there fatalities or

> injuries. These triggers that coincide with ‘terrorism as theater’ makes sense. If you have more short term goals or if you are looking to overthrow a government or country and you don’t have any interest on the audiences then you are not going to be involved in the terrorism as theater. The benefits of coverage are not going to be the theater and would be considered counterproductive. They bring in more world help and aid for that government.

These remarks are interesting in that they directly relate to media perpetuating attacks. The participant makes the point of noting that short term goals – the purpose being an eventual end – will not generate the terrorism as theater motivation. However, when the main focus is the audience and the aim is to gain power through fear, that goal goes on forever with no clear-cut or well defined end. This notion contributes to the theory that while cyberterrorism does create harm, it is a process whose ultimate goal is larger and more abstract of a fulfillment for the attacker.

Research Question 3

What aspects of the social world, according to Stamper’s Semiotic model, are being met?

Stamper’s Semitic Ladder s begins with a physical entity which in this case would be a computer itself. At this point, it is a regular computer that has the ability to share pictures, look up recipes, find directions, and chat in real time with friends. For a cyberterrorist, a computer at the physical level is a weapon. At the empirical level, a level in which patterns have the ability to form, that computer takes the role of being a host to potential patterns of propaganda that the terrorist chooses to disseminate. This could be in the form of constantly posted propaganda displaying acts of crime or violence for anybody to see. At the syntactical level, the propaganda begins to be disseminated with a purpose. A cyberterrorist, functioning on the syntactical level, logically arranges the propaganda to be stationed in the most effective manner possible. This may be websites, email, spam mail, and encrypted files that get sent to targets. The next level, the semantic level, in which meaning becomes attached, would allow for the cyberterrorists to take a threat beyond a website into an entity that it more symbolic than “just” another computer. Every action has a purpose that becomes imbedded and will not be dislodged easily. A computer is a weapon that is capable of shutting down emergency response systems, or collapsing financial enterprises or unleashing raw sewage into the water systems. The pragmatic level is the conversation that is occurring during and as a result of the cyberterrorist attacks. People are exposed to the propaganda that was put in place to draw out a specific reaction of fear or governmental mistrust. At this point, the actual computer, the actual website, the actual words are more than words, metal, and pictures. They represent power and control and an element of the unknown to be frightened of. The targets, either having been hit, or having been exposed to this propaganda can no longer take a website, for example, as some hidden entity displayed on a computer screen. Instead, a website may have become a vehicle that threatens, that displays acts of power, and that steals the target’s sense of security be replacing it with doubt and fear.

The social world is the culmination of all the other levels of Stamper’s Semiotic Ladder working together in action. The result is the formation of beliefs, expectations, commitments, contracts, laws, and culture to form. In turn, those not affiliated with the cyberterrorist group may be inclined to some sort of action (Hensgen et al., 2003a). By action, it is understood that it could be at the governmental level, requiring that law be created stopping cyberterrorist or at the level of an everyday civilian whose action is to become fearful. Because meaning on the social level is contingent upon meaning in the other levels first, it is apparent from the testimony of my participants that there is action being spurned into place. As noted earlier, there are people working for the government, taking countermeasures to cyberterrorists and creating programs that are designed to stay one step ahead of cyberterrorism.

An important aspect is the notion that there are those that do not see cyberterrorism as a crime. Stamper's Semiotic Ladder at the level of the social world, hold in regard the formation of beliefs and expectations in regard to a catalyst. The catalyst has been cyberterrorism and the aspect that the world view created may not be the same world view as the United States world view cannot be overlooked. The next section deals with how the aspects of the social world are being carried out. As such, the topic must be assessed from the context of the global world and the implications that cyberterrorism has across the international community must be understood.

Research Question 4

How are the aspects of Stamper's Ladder in regards to the social world being carried out?

With the social world aspect of Stamper's Ladder, the focus is on the big picture and how the components in the big picture play off of each other, panning out across the globe. Cyberterrorists can work across borders without concern for jurisdiction. For example, an incident in 1998 occurred when emails reading "We are the Internet Black Tigers and we are doing this to disrupt your communications" were sent to the Sri Lankan embassy, crashing computer systems and subsequently instilling fear in those who were attacked (Denning, 2000). Meanwhile, halfway across the globe, cyberterrorists in the same year of 1998 created a "time bomb" that shut down major switching hubs in Manhattan, that destroyed emergency 911 services throughout the eastern seaboard (Denning, 1999). The importance here is to recognize that not only is cyberterrorism occurring across different geographical areas; the motives behind the action are, also, not interpreted in only one context or only by one moral code. In an interview with a cyber forensic expert, he stated that,

> There can be a two or three other audiences that are simultaneously dealing with, or participating as members of terrorist groups in other countries, with a demonstration of what *they* can do. You can have an audience of targets, supporters or even an audience of more potential kooks. It can be a message to the Muslim world. And that message can be interpreted 180 degrees different that "we can do these terrible things to you" and the terrorist sympathizers around the world say "we can do these wonderful things, we are a powerful group". That's why communication allows a single event to reach multiple audiences with different messages from that one single event. It can be through the use of the Internet, the interpretive audiences and communications can occur and the terrorist organization, through their Internet, can help steer certain light into interpretation in particular ways. They can make martyrs out of their own that were killed.

This participant highlights the possibility that for a given action and interpretation of the action by a person or a group, those same actions will be defined differently based on the person or group that commits the threat or crime. The beliefs and expectations about cyberterrorism that my participants spoke about are strongly anti-cyberterrorism, expressing anger and disgust for those who commit crimes via the internet. Because these crimes are actually committed, I can only assume that not everybody feels anger and disgust at the concept of cyberterrorism. I do not know the exact ratio of supporters to non-supporters. Nevertheless, suggesting that the whole world backs the belief of the United States would be inaccurate. It would also be potentially damaging to communications that may occur on a governmental level should there be international negotiations and attempts to regulate and prosecute cyberterrorists.

CHAPTER 5: CONCLUSION

Summary of Findings

The definition of a cyberterrorist, what the propaganda consists of, who the targets are and the emotional effects, the role of the media in the equation and the communicative messages of cyberterrorists according to Stamper's Semiotic Ladder have all been assessed. From the data analyzed in this study, it was established that a cyberterrorist message is a complex conglomeration of tactics designed to instill fear in their target population, to disrupt the web functioning of a target, to procure information, as a means to obtain funding, for the purposes of recruitment, to gain sympathy from others with similar thought patterns, and to look powerful while doing so.

Additionally, every research question was answered thoroughly. Question one asked how communicative messages are logistically being carried out. It was established through the data that messages are being conveyed in a variety of ways. Cyberterrorists lean heavily on propaganda to get the message across to the public. Being a cyberterrorist partially lies in the damage and harm that can occur. An even bigger piece of the equation is the theatrical aspects that overlap with the damage. A heavy emphasis is placed on the notoriety of these criminals to meet a list of goals. These goals include instilling fear, carving a name for oneself, alluding authority, flaunting accepted protocol or behavior, and recruiting others to join the cause that they have already embarked on. If the cyberterrorist can get into the psyche of the public and cause fear and doubt in the government to protect them, then they have succeeded in ways that meet or even surpass the physical damage that can occur. The propaganda of websites, posted videos, forums, blog posts, and email encryptions allow for these goals to be met.

Having established a foundation for how these goals are being carried out, there is the question of how outside participation of the media affects the cyberterrorist outcomes. The data revealed that the media implications lie deeper than surface level reporting and actually had adverse consequences for those fighting cyberterrorism. The data suggested that the media implications include damages to the psyche of the public due to over-exaggeration in reporting and tipping off cybercriminals to progress made by law enforcement. The most damaging consequence is allowing the goals of the cyberterrorist to be met. When this occurs, the media has additionally allowed the cyberterrorists to gain a more powerful symbolic and detrimentally psychological foothold to continue with the missions that they have embarked on.

The third and fourth research questions deal with the bigger picture, or the global implications as defined by Stamper's Semiotic Ladder. It has been stated time and again that cyberterrorism spans borders and boundaries both literally and figuratively. Documented cases have occurred not only in the parts of the United States, such as Atlanta, New York City, San Jose, and Massachusetts, but internationally as well, in countries such as Estonia, Russia, Australia, Sri Lanka, Turkey, and Morocco. The third question inquires about what aspects of the social world are being met. Because this is the aspect that deals heavily in the beliefs and the culture that can result from a given symbolic action, it is important to recognize that there are naturally going to be many different opinions that form from that act. Based on the small amount of places listed above, it stands to reason that each geographical area is replete with different political and religious viewpoints, worldviews, customs, and beliefs on "dealing with the enemy." The social world aspect (i.e., beliefs, customs, worldviews, etc.) can be witnessed in the propaganda set forth by cyberterrorists, being displayed on websites, forums, emails, and video posts. The example given before, with Irhabi007's messages of: "The enemies of Allah will continuously [try to close down] our website...." is a symbolic indicator strictly from language alone. A person with a worldview that these cyberterrorist crimes should be stopped would certainly not consider him- or herself an enemy to God. Clearly, the poster of this message disagrees, calling those whose job is to protect the targets from harm an "enemy."

The fourth research question expands upon this concept by asking how the social world aspects are being carried out. Again, the data delve into the logistical side of the equation by analyzing the aspects that make this method of crime a postmodern attack. Because of the technologically elevated aspect of the tools, there are a greater number of people who can be exposed to the various beliefs on the subject of cyberterrorism. Historically, when a terrorist wanted to post demands or brag about misdeeds that were committed, the channels that they had to go through included the media and governmental agents representing those who had been attacked. Presently, the notion that one website alone can generate thousands upon thousands of hits has greater repercussions now than they did in the past when the communicative messages of the terrorist were posted at the behest of the media. The new form of technology bypasses the intermediary and puts the control in the hands of the cyberterrorist who no longer has to wait for another to comply with their wishes for publicity.

The means of a cyberterrorist to communicate their messages is done through a variety of ways including email, virus spreading, websites, and video posts. These means are all done through the use of a computer and have been found to adversely affect targets that are exposed to these means of propaganda and publicity only to be left fearful and with less faith in their government's ability to protect them. Another component of the cyberterrorist, target equation is that of the media and their ability to either influence the emotional responses of targets or as a compromising influence on the investigation of cyberterrorist matters. The media was found to be a negative influence from the perspective of placing cyberterrorism as a crime. Lastly, there is the actual focus on cyberterrorist messages as a communicative process. Stamper’s Semiotic Ladder, once again, was helpful in illustrating, from first level, to sixth, the various ways in which an entity could be taken and manipulated to symbolically represent something else. In this case, bits of metal and plastic (computer) became a weapon. That weapon took letters and numbers and words and gave them power (threatening messages). Those threats were written as data, infused as information and displayed on a screen (website). That website was sponsored and added to and built upon until the content became more than words and numbers on a screen, but a moving image of a crime that has been committed (video post of attacks or hostages). Those video posts became symbols of power from a group of people, an organization that does not follow the rules and protocol assumed by humanity. That power grew and continues to grow stronger and more salient due to the nature of the beast. These are crimes committed by the nameless and the faceless. Keen (1991) suggested that the nameless and the faceless who produce the propaganda will never grow to be anything more than ”us” versus “them,” a tactic that takes the human out of the equation.

From Stamper’s Semiotic Ladder, it has been established that what is most human, the interpretation, the beliefs, the culture that forms thereafter, cannot be subjected to the process of being dehumanized. When there is an enemy that is nameless, faceless, and who instills fear in a population, then the propaganda that is put forth only becomes more powerful and more symbolic of that harm that could occur at the hands of that enemy. Law enforcement, FBI, and cyber forensic experts must work together to find common ground so that the power and control already established by cyberterrorism can be diminished, with the power become enervated.

As I gathered all the data and analyze them in depth, my ultimate goal was to demonstrate and provide concrete examples that cyberterrorists' communicative messages, their styles of propaganda, and their various tactics constitute a semiotic gesture. As the literature review has shown, cyberterrorists seek publicity; they advertize their deeds and intents. Yet, through further research and interviews with participants, there has been a specific focus on the actual effects of their semiotic messages on targets, on the public, and on the world at large. By providing better increasing awareness of cyberterrorist propaganda, it is hoped that this study not only opened the eyes of readers as to what may happen to their own personal computers; but also gave fresh insights to the participants themselves – that is, law enforcement agents – and their colleagues all over the world as to how to better their counter-terrorism strategies, both online and offline.

Limitations

When conducting this study, several unforeseen or unexpected limitations were found. The limitations unfolded in a sequence that seemed to expand upon itself. The most prevalent source of limitation occurred while trying to find participants to interview. In many cases, six to be exact, the participants were very willing to be interviewed but upon learning what these questions were asking, some participants were simply not versed in the subject of "cyberterrorism." There were instances in which interviews were terminated mid-way through because the participant felt that they could not provide enough material to do the topic justice.

The lack of answers from these people combined with the cases of those who do have a background in cyberterrorism, I found, could be attributed to a combination of both the nature of the material being very specific or the jurisdiction of the participants and what they were willing or able to reveal.

It was noted earlier that this study was qualitative primarily because of the sensitive nature of the material and need for trust between participant and interviewer. Face-to-face interviewing provided an opportunity to build upon that trust, but only to a certain extent. The nature of this material is very sensitive not only to the psyche of participants but also in matters of security. Because I conducted interviews with members of the FBI as well as cyber forensic experts, a few of my questions were met with hesitations by the participants prior to my receiving an answer. In some ways, I feel this may have inhibited the participants, not because they lacked trust in me but because there was a need to know to what extent the data were going to be used. Additionally, because these answers were taken from the viewpoint of those who try to stop cyberterrorism, the perspective that was given is not the same had actual cyberterrorists been interviewed.

An additional limitation concerned the researcher herself, that is, me being a communication scholar. To begin with, I did not have a strong background in cyber law and conflict studies. This was an obstacle because, prior to every interview, additional research needed to be conducted so that I would have a general idea about the jargon that could potentially have been mentioned. Because I was interviewing people in a field they felt comfortable in, and to which their vernacular consisted heavily of field related jargon, I was forced to ask for clarification in more than one instance on abbreviations or terms. All participants assisted in clarification but I cannot be sure that the impressions that I had built as a credible and knowledgeable researcher were permanent after asking for clarification.

Lastly, a major but practical limitation that occurred was the lack of time and resources available in this study. My participants were located in various places across the country. As mentioned earlier, there were a few interviews that occurred via the telephone and, while I do not think that the nature of the data collected was any better or worse for having been conducted remotely, I do think it would have been ideal to have the time and resources to go and see the participants in the same face to face settings that occurred during the local interviews.

Future Directions

As with any study, there are limitless possibilities for future research. Many aspects pertaining to cyberterrorism have been discussed in this qualitative research study with still more answers to be uncovered. One of the main aspects for future research would be to take the premise of communicative messages and talk to cyberterrorists to find out what perspective they follow. There has not been a lot of ample opportunity to study the type of people who fit the profile for cyberterrorists. If research were conducted by talking to actual cyberterrorists, or even hacker organizations to start, a profile for these criminals could start to be established. This would provide an opportunity to gain exact information about motivations and intent for any communication whether it be through email, website, or video posting.

Another possibility for future research would be to take the perspective of the media. One could potentially ascertain the rationale for what they chose to report on and why. This direct assessment of the media could possibly allow for answers to emerge that would work toward being one step closer to better working relations between law enforcement and the media with the intention of bettering the output to the public. Additionally, the media perspective would allow for a better understanding and clarification of more consequences that occur from the media broadcasts that inadvertently enhance the cause of the cyberterrorists, rather than work toward a safer outcome for the public.

Cyberterrorism could also be looked at from the scope of organized crime. Theory suggests that the main motive behind organized crime is to gain a profit. Though not all motives of cyberterrorism are profit-centered, there are, as this study suggests, aspects that focus on the financial downfall of others. Research could be done to study how the networks function systemically or how they fit into a pattern of traditional organized crime. A comparative analysis could be done using an organizational model that would fit traditional groups such as the mafia and test to see if cyberterrorism falls into a similar category.

Throughout this study, a lot of time and research were devoted to the notion of citizens and civilians being fearful of attack based on cyberterrorist propaganda as well as having faulty trust in the government's ability to protect them. One potential study that would be quantifiable could be to gather research from everyday citizens without a formal understanding or background in cyberterrorism and gauge their reactions to propaganda put out by cyberterrorists. This could be done through a manner of methods, such as showing them videos posted by cyberterrorists, or setting up scenarios of cyberterrorist attacks such as denial of service attacks that have already been documented to ascertain whether or not, or how intensely they were affected by what they witnessed.

There was one theme consistently brought up during the interviews: the similarities between what is previously considered terrorism (the brick and mortar establishments, the suicide bombers who actually strapped bombs to themselves in order to cause destruction and death) and that of cyberterrorism. At this point, there has been extensive research done on preventative measures for traditional terrorism. Research can pinpoint different aspects of both historical and cyberterrorism to access pros and cons of each, as well as looking at the overlap to see if there are any additional preventative measures that can be taken to increase protection for the public in the case of cyberterrorism.

Another theme that was brought up but not elaborated on in this study was the novelty of cyberterrorism in law enforcement and the problem of information sharing. While conducting interviews, I heard a lot from participants that information sharing was typically a battle constantly being fought. Because this is such a new area for many law enforcement officials, the potential for failure of coordination among agencies is colossal. Coordination between jurisdictions is greatly needed not only for cooperation but also for pooling of funding for education and training as well as prevention strategies. As a last suggestion, research could be conducted that addresses all of these concerns to further the protective efforts of every branch of law enforcement.

Truly, it is the researcher’s hope that this qualitative study has enlightened not only those who participated in the study but those who are in a position to build upon the knowledge. Ultimately, an ideal outcome would be for all branches of government, from law enforcement to FBI, to work on bettering communication with each other, as one group. With attention and diligence, there can be positive efforts to transform cyberterrorism from symbolically powerful to virtually insignificant.

APPENDIX A: INTERVIEW PROTOCOL

1) What is a cyberterrorist?

2) How do you recognize cyberterrorism?

3) What are cyberterrorist messages?

4) What sorts of publicity or propaganda do cyberterrorists use?

5) Who are the potential targets of cyberterrorists?

6) What kind of strategies do cyberterrorists use to communicate their intent(s)?

7) What are the effects of cyberterrorism on targets?

8) Who are the targets of cyberterrorism?

9) How do cyberterrorists feel about cyberterrorism?

10) Is there anything else you want to add that I should know?

APPENDIX B: INFORMED CONSENT

PROJECT TITLE: Cyberterrorists: Their Communicative Intents and Their Effects on Targets
PRINCIPAL INVESTIGATOR: Elizabeth Minei
CONTACT INFORMATION: (561) 721-5271

I am a UCF Master's student at the Nicholson School of Communication at the University of Central Florida and I am working under the supervision of Dr. Jonathan Matusitz. You are being asked to volunteer for a research study. You were selected as a possible participant because you are a cyber forensics expert or LE (Law Enforcement) agent. Please read this informed consent form and feel free to ask me any questions that you may have before agreeing to take part in this study.

Purpose of the Study

This study analyzes communicative intents of hackers and how they aim at sending messages of violence designed to publicize their status of power and legitimacy. The goal is also to investigate the effects of the violent attacks and/or messages of cyberterrorists on targets, and who the targets are.

Methods and Procedures

The method used in this study is interviewing lasting one hour, where you will be asked questions pertaining to the topic. This study has minimal or no risks involved. There are no direct benefits to participating, there is no penalty for not participating, and there is no compensation for participating. You do not need to answer any question that you wish to answer. You may also withdraw from my study at any time.

You must be 18 years of age or older to participate.

To assist with accurate recording of participant responses, interviews **may** be recorded on an audio recording device/video recording device. The tapes will be transcribed following the interview, then immediately destroyed. Participants have the right to refuse to allow such taping without penalty.

Any records of this study will be kept private. The consent forms will be stored separately from the interviews and other study materials. In published reports, there will be no information included that will make it possible to identify the research participant. Research records will be stored securely, for three years, in a computer file or in a safe box. I will store the data on my computer and keep these transcriptions safe by locking them into a program file that can only be opened with a password. Your name will NOT be mentioned.

Contacts and Questions

The researcher(s) conducting this study can be contacted at (561) 721-5271 or minei33@gmail.com (for Elizabeth Minei, the principal investigator) and (407) 531-5459 or jmatusit@mail.ucf.edu (for Dr. Jonathan Matusitz, the faculty sponsor). You are encouraged to contact the researcher(s) if you have any questions.

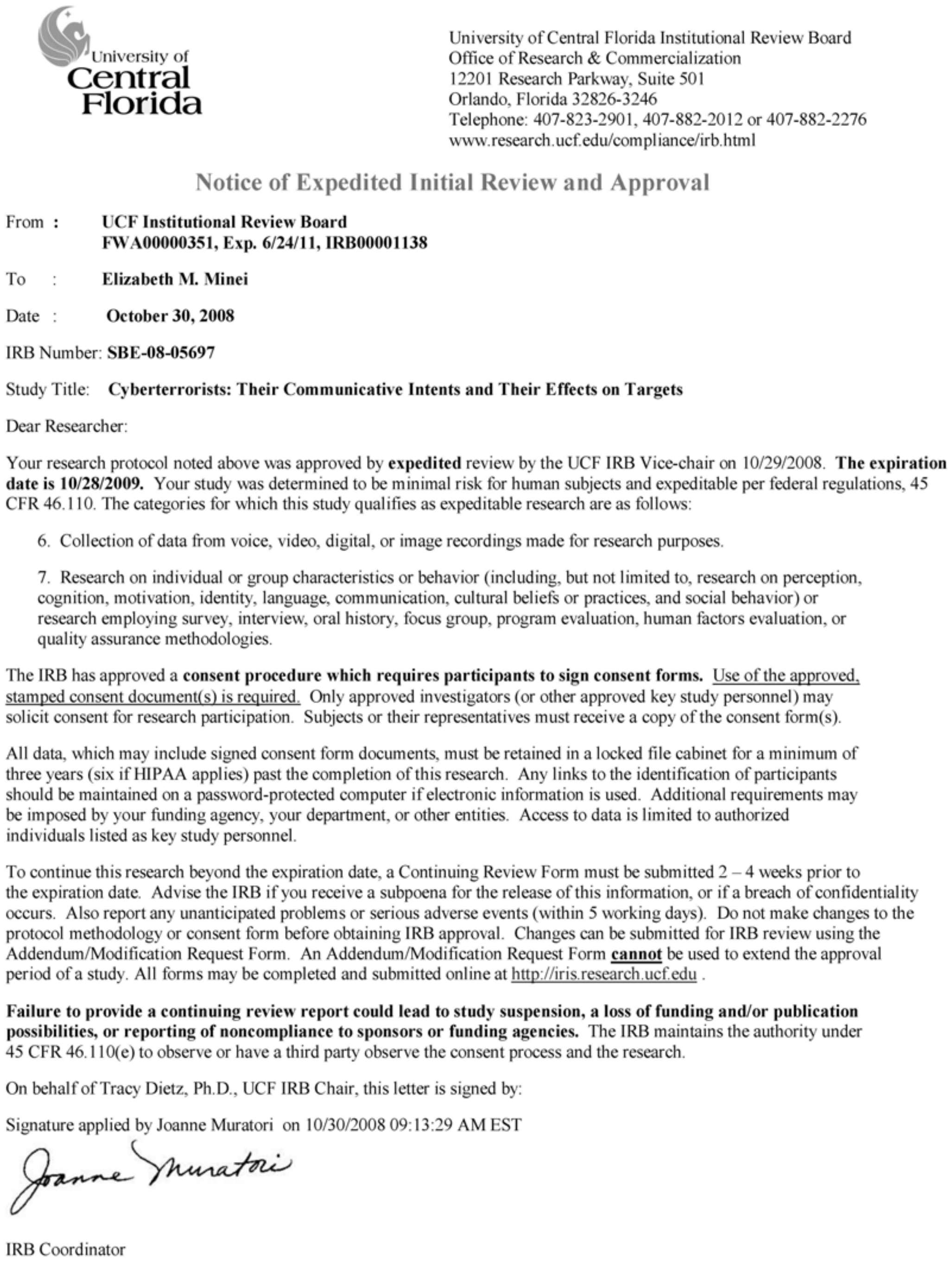
Research at the University of Central Florida involving human participants is carried out under the oversight of the Institutional Review Board. Questions or concerns about research participants' rights may be directed to the UCF IRB office, University of Central Florida, Office of Research & Commercialization, 12201 Research Parkway, Suite 501, Orlando, FL 32826-3246, or by campus mail 32816-0150. The hours of operation are 8:00 am until 5:00 pm, Monday through Friday except on University of Central Florida official holidays. The telephone numbers are (407) 882-2276 and (407) 823-2901.

I hereby agree to the terms stipulated in this informed consent form

0 I consent to the use of audio recording.
0 I do not consent to the use of audio recording.

Participant's Name: ___________________________ Date: _________________

APPENDIX C: I.R.B. APPROVAL



University of
Central
Florida

University of Central Florida Institutional Review Board
Office of Research & Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246
Telephone: 407-823-2901, 407-882-2012 or 407-882-2276
www.research.ucf.edu/compliance/irb.html

Notice of Expedited Initial Review and Approval

From : **UCF Institutional Review Board**
FWA00000351, Exp. 6/24/11, IRB00001138

To : **Elizabeth M. Minei**

Date : **October 30, 2008**

IRB Number: **SBE-08-05697**

Study Title: **Cyberterrorists: Their Communicative Intents and Their Effects on Targets**

Dear Researcher:

Your research protocol noted above was approved by **expedited** review by the UCF IRB Vice-chair on 10/29/2008. **The expiration date is 10/28/2009.** Your study was determined to be minimal risk for human subjects and expeditable per federal regulations, 45 CFR 46.110. The categories for which this study qualifies as expeditable research are as follows:

6. Collection of data from voice, video, digital, or image recordings made for research purposes.

7. Research on individual or group characteristics or behavior (including, but not limited to, research on perception, cognition, motivation, identity, language, communication, cultural beliefs or practices, and social behavior) or research employing survey, interview, oral history, focus group, program evaluation, human factors evaluation, or quality assurance methodologies.

The IRB has approved a **consent procedure which requires participants to sign consent forms.** Use of the approved, stamped consent document(s) is required. Only approved investigators (or other approved key study personnel) may solicit consent for research participation. Subjects or their representatives must receive a copy of the consent form(s).

All data, which may include signed consent form documents, must be retained in a locked file cabinet for a minimum of three years (six if HIPAA applies) past the completion of this research. Any links to the identification of participants should be maintained on a password-protected computer if electronic information is used. Additional requirements may be imposed by your funding agency, your department, or other entities. Access to data is limited to authorized individuals listed as key study personnel.

To continue this research beyond the expiration date, a Continuing Review Form must be submitted 2 – 4 weeks prior to the expiration date. Advise the IRB if you receive a subpoena for the release of this information, or if a breach of confidentiality occurs. Also report any unanticipated problems or serious adverse events (within 5 working days). Do not make changes to the protocol methodology or consent form before obtaining IRB approval. Changes can be submitted for IRB review using the Addendum/Modification Request Form. An Addendum/Modification Request Form **cannot** be used to extend the approval period of a study. All forms may be completed and submitted online at http://iris.research.ucf.edu .

Failure to provide a continuing review report could lead to study suspension, a loss of funding and/or publication possibilities, or reporting of noncompliance to sponsors or funding agencies. The IRB maintains the authority under 45 CFR 46.110(e) to observe or have a third party observe the consent process and the research.

On behalf of Tracy Dietz, Ph.D., UCF IRB Chair, this letter is signed by:

Signature applied by Joanne Muratori on 10/30/2008 09:13:29 AM EST

Joanne Muratori

IRB Coordinator

LIST OF REFERENCES

Aaviksoo, J. (2008). Cyber-terrorism. *Vital Speeches of the Day, 74*(1), 28-32.

Aeilts, T. (2005). Defending against cyber crime and terrorism. *FBI Law Enforcement Bulletin, 74*(1), 14-20.

Aldrich, R. W. (2000). Cyberterrorism and computer crimes: Issues surrounding the establishment of an international legal regime. *Institute for National Security Studies, 32*, 1-101.

Army field manual (1956). Washington, D.C.: Department of the Army.

Arquilla, J., & Ronfeldt, D. (2001a). *Networks and netwars: The future of terror, crime, and militancy*. Santa Monica: RAND.

Arquilla, J. & Ronfeldt, D. R. (2001b). Networks, netwars, and the fight for the future. *First Monday, 6*(10), 1-25.

Arquilla, J., Ronfeldt, D., & Zanini, M. (1999). Networks, netwar and information-age terrorism. In I. O. Lesser, B. Hoffman, J. Arquilla, D. F. Ronfeldt, M. Zanini, & B. M. Jenkins (Eds.), *Countering the new terrorism* (pp. 39-88). Santa Monica: RAND.

Baraldi, C. (2006). New forms of intercultural communication in a globalized world. *The International Communication Gazette, 68*(1), 53-69.

Barber, B. R. (2003). *Jihad vs. McWorld: Terrorism's challenge to democracy*. London: Corgi.

Barley, S. (1983). Semiotics and the study of occupational and organizational cultures. *Administrative Science Quarterly, 28,* 398-413.

Barry, T.E., & Howard, D.J. (1990). A review and critique of the hierarchy of effects in advertising. *International Journal of Advertising, 9*(2), 121-35.

Baudrillard, J. (2002). *The spirit of terrorism and the requiem for the Twin Towers*. New York: Verso.

Begleiter, R.J. (2001). Whose media are we-notions of media and nationality challenged by the war on terrorism. *Brown Journal of World Affairs, 8*(2), 17-26.

Bendrath, R. (2003). The American cyber-angst and the real world. In R. Latham (Ed.), *Bombs and bandwidth: The emerging relationship between IT and security* (pp. 49-73). New York: The New Press.

Berinato, S. (2002, March 17). The truth about cyber-terrorism. *CIO Magazine, 1,* 10-21.

Bernstein, A., Iwanyk, B., (Producers) & Loncraine, R. (Director). (2006). *Firewall.* [Motion Picture]. United States: Warner Brothers.

Billig, M. (1995). *Banal Nationalism.* Thousand Oaks, CA: Sage.

Boardman, M. E. (2005). Known unknowns: The illusion of terrorism insurance. *The Georgetown Law Journal, 93*(3), 783-844.

Brown, D. (2006). A proposal for an international convention to regulate the use of information systems in armed conflict. *Harvard International Law Journal, 47*(1), 179-221.

Brownlie, I. (1963). *International law and the use of force by states*. Oxford: Clarendon Press.

Cassell, B. L. (2006, November 21). Criminal network: To catch crooks in cyberspace. *Wall Street Journal (Eastern Edition)*, p. A1.

Chandler, D. (2002). *Semiotics: The basics.* New York: Routledge.

Clem, A., Galwankar, S., & Buck, G. (2003). Health implications of cyber-terrorism. *Prehospital and Disaster Medicine, 18*(3), 272-275.

Conway, M. (2002). What is cyberterrorism? *Current History, 2,* 436-440.

Cowen, T. (2006). Terrorism as theater: Analysis and policy implications. *Public Choice, 128*(1), 233-244.

Cronin, A. K. (2006). How al-Qaida ends: The decline and demise of terrorist groups. *International Security 31*(1), 7-48.

Deal, C., Gage, A., & Schueneman, R. (2001). Viral contagia in cyberspace. *Military Review, 81*(2), 1-17.

Denning, D. E. (1999). *Cyberterrorism*. Georgetown University, DC: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives.

Denning, D. E. (2000). Hacktivism: An emerging threat to diplomacy. *Foreign Service Journal, 1*(1), 10-17.

Deutsch, J. M. (1996, June 25). *Statement before the US Senate Governmental Affairs Committee*. Washington, DC: Permanent Subcommittee on Investigations.

Deutsch, J. M. (1997). Terrorism. *Foreign Policy, 108*, 10-22.

Desouza, K. C. (2002). *Managing knowledge with artificial intelligence*. Westport, CT: Quorum Books.

Desouza, K. C., Chattaraj, A., & Kraft, G. D. (2003). Supply chain perspective to knowledge management: research propositions, *Journal of Knowledge Management, 7*(5), 129-138.

Desouza, K. C., & Hensgen, T. (2003). Technological forecasting and social change. *Science Direct*, *70*(4), 385-396.

Desouza, K. C., & Hensgen, T. (2007). Connectivity among terrorist groups: A two models business maturity approach. *Studies in Conflict & Terrorism, 30*, 593-613.

Dinstein, Y. (2004). *The conduct of hostilities under the law of international armed conflict.*

Cambridge: Cambridge University Press.

Docherty, T. (1993). *Postmodernism: A reader*. London: Harvester Wheatsheaf.

Dunlap, C. J. (1996). How we lost the high-tech war of 2007. *The Weekly Standard, 1*(19), p. 29.

Eco, U. (1976). *A theory of semiotics*. London: Macmillan.

Embar-Seddon, A. (2002). Cyberterrorism. *The American Behavioral Scientist, 45*, 1033-1043.

Erbschloe, M. (2001). *Information warfare: How to survive cyber attacks*. Boston: McGraw-Hill.

Filipe, J. (2000). An organizational semiotics model for multi-agent systems design. *Knowledge Engineering and Knowledge Management Methods, Models, and Tools, 1937*(302), 265-269.

Fottrell, M., (Producers) & Wiseman, L. (Director). (2007). *Live Free or Die Hard.* [Motion Picture]. United States: 20th Century Fox.

Fulghum, D. A. (2005). Aviation. *Week & Space Technology, 163*(16), p. 1.

George, A.L. (1959). *Propaganda analysis: A study of inferences made from Nazi propaganda in World War II.* Evanstan, IL: Row, Peterson & Co.

Glasser, S. B., & Coll, S. (2005). The web as weapon. *Washington Post*, p. A10.

Gordon, S., & Ford, R. (2002). Cyberterrorism? *Computers and Security, 21*(7), 636-647.

Gorge, M. (2007). Cyberterrorism: Hype or reality? *Computer Fraud & Security, 2*, 9-12.

Gray, J. (2003). *Al Qaeda and what it means to be modern*. London: Faber & Faber.

Gunaratna, R. (2005).The prospect of global terrorism. *Society, 42*(6), 31-35.

Gunaratna, R. (2006). The terror market. *Harvard International Review, 27*(4), 66-69.

Harmon, C. C. (2001). *Terrorism today*. London: Frank Cass Publishers.

Haugh, R. (2003). Cyber terror. *H&HN: Hospitals & Health Networks, 77*(6), p. 60.

Hensgen, T., Desouza, K., Evaristo, J. R., & Kraft, G. D. (2003a). Playing the "cyber terrorism game" towards a semiotic definition. *Human Systems Management, 22*(2), 51-61.

Hensgen, T., Desouza, K. C., & Kraft, G. D. (2003b). Games, signals, and processing in the context of crisis management. *Journal of Crisis and Contingencies Management, 11*(2), 67-77.

Hoffman, B. (2003). Al Qaeda, trends in terrorism, and future potentialities: An assessment. *Studies in Conflict and Terrorism, 26*, 427-440.

Hoopes, N. (2005). New focus on cyber-terrorism. *Christian Science Monitor, 97*(184), p. 1.

Iqbal, A. (2002, February 20). Site claims Bin Laden's message. *United Press International*. Retrieved October 17, 2008 http://www.firstmonday.org/ISSUES/issue7_11/conway/.

Jain, R. (2005). Cyber terrorism: A clear and present danger to civilized society? *Information Systems Education Journal, 3*(44), p. 3.

Jaishankar, K. (2008). Identity related crime in the cyberspace: Examining phishing and its impact. *International Journal of Cyber Criminology, 2*(1), 10-15.

Jameson, F. (1991). *Postmodernism, or the cultural logic of late capitalism*. Durham, NC: Duke University Press.

Jenkins, B. 1975. *International terrorism.* Los Angeles: Crescent Publication.

Jowett, G., & O'Donnell, V. (2006). *Propaganda and persuasion.* Thousand Oaks, CA: Sage.

Janczewski, L. J., & Colarik, A. M. (2005). *Managerial guide for handling cyber-terrorism and information warfare*. Hershey, PA: Idea Group Publishing.

Keen, S. (1991). *Faces of the enemy: Reflections of the hostile imagination.* UK: Harper Collins.

Kim, S., Scheufele, D. A., & Shanahan, J. E. (2002). Agenda-setting, priming, framing and second-levels in local politics. *Journalism and Mass Communication Quarterly, 79*(1), 7-25.

Kohlmann, E. F. (2006). The real online terrorist threat. *Foreign Affairs, 85*(5), 115-124.

Kontzer, T. (Sep 5, 2005). Collaboration helps nab cybercriminals. *InformationWeek, 9*, p. 5.

Krippendorff, K., Bock, M.A. (2008). *The content an analysis reader.* Thousand Oaks, CA: Sage.

Kress G. (1993). Against arbitrariness: The social production of the sign as a foundational issue in Critical Discourse Analysis. *Discourse and Society, 4*(2), 169-191.

Kress, G., & van Leeuwen, T. (2001). *Multimodal Discourse: The Modes and Media of Contemporary Communication.* Oxford: Hodder Arnold.

Kvale, S. (1996). *InterViews*. Thousand Oaks, CA: Sage.

Laqueur, W. (2006) *No end to war: Terrorism in the twenty-first century*. New York: Continuum.

Laru, J., & Järvelä, S. (2008). Social patterns in mobile technology mediated collaboration among members of the professional distance education community. *Educational Media International, 45*(1), 17-32.

Lasswell, H.D. (1971). *Propaganda technique in world war.* Cambridge, MA: MIT Press.

Lenzner, R., & Vardi, N. (2007). The next threat. *Forbes, 174*(5), 15-21.

Lewis, J. (2002). *Assessing the risks of cyberterrorism, cyber war, and other cyber threats*. Washington, D. C.: Center for Strategic and International Studies (CSIS).

Littlejohn, S. & Foss, K. (2008). *Theories of human communication* (9th Ed.). Belmont, CA: Thomson Higher Education.

Liu, K. (2000). *Semiotics in information systems engineering*, Cambridge: Cambridge University Press.

Lye, K. W., & Wing, J. M. (2005). Game strategies in network security. *International Journal of Information Security*, *5*(1), 1-10.

MacIntyre, A. (1984). *After virtue.* Notre Dame: University of Notre Dame Press.

Mathieu G. (2007). Cyberterrorism: Hype or reality? *Computer Fraud & Security, 2*, 9-12.

Matusitz, J. (2008a). Cyberterrorism: Postmodern state of chaos. *Information Security Journal: A Global Perspective, 17*(4), 179-187.

Matusitz, J. (2008b). Postmodernism and networks of cyberterrorists. *Journal of Digital Forensic Practice, 2*(1), 17-26.

McGirk, T. (1999, October 11). Wired for warfare. *Time International*, p. A11.

McKenna, B. (2005). FBI arrests young Turk and Moroccan for Zotob. *Infosecurity Today*, *2*(5). A4.

McQuail, D. (2000). *McQuail's mass communication theory*. Thousand Oaks, CA: Sage.

Meyer, J. (2001). Tearing down the facade: A critical look at the current law on targeting the will of the enemy and air fans doctrine. *A.F L. Rev. 51*(143), 168-171.

Miller, C., Matusitz, J., O'Hair, D., & Eckstein, J. (2008). The role of communication and the media in terrorism. In D. O'Hair, R. Heath, K. Ayotte, & G. R. Ledlow (Eds.), *Terrorism: Communication and rhetorical perspectives* (pp. 43-66). Cresskill, NJ: Hampton Press.

Misra, S. (2003) High-tech terror. *American City & County, 118*(6), p. 1.

O’Hair, D., & Heath, R. (2005). Conceptualizing communication and terrorism. In D. O’Hair, R. Heath, & J. Ledlow (Eds.), *Community preparedness, deterrence, and response to terrorism: Communication and terrorism* (pp. 1-12). Westport, CT: Praeger.

Paul, C. (2008). *Information operations: Doctrine and practice*. Westport CT: Praeger.

Peiree, C. T. (1955). Logic as semiotic: The theory of signs. In J. Buchler (Ed.), *Philosophical writings of Peirce*. New York: Dover Press.

Polderman, J. W., & Willems, J. C. (1997). *Introduction to mathematical systems theory: A behavioral approach*. Berlin: Springer Verlag.

Posner, R. A. (2005). Catastrophe: The dozen most significant catastrophic risks and what we can do about them. *Skeptic, 11*(3), 42-63.

Preimesberger, C. (2006). Plugging holes. *eWeek, 23*(35), 22-28.

Ramaprasad, A., & Rai, A. (1996) Envisioning management of information. *Omega: The International Journal of Management Science*, *24(*2) 179-193.

Reinard, J.C. (2001). *Introduction to communication research*. New York: McGraw-Hill.

Rheingold, H. (1993). *The virtual community: Homesteading on the electric frontier.* Reading, MA: Addison-Wesley.

Rockel, K. (2005). *Stedman’s guide to the HIPAA privacy rule*. Philadelphia: Lippincott Williams & Wilkins.

Rogers, M. (2003). The psychology of cyber-terrorism. In A. Silke (Ed), *Terrorist, victims, and society: Psychological perspectives on terrorism and its consequence* (pp. 72-92). London: John Wiley.

Schmitt, M. N. (2002). Wired warfare: Computer network attack and the *jus in bello*. *International Review of the Red Cross, 84*, 365-399.

Schneier, B. (2005). The Zotob storm, *IEEE Security and Privacy, 3*(6), 96.

Schweitzer, G. E. (2002). *A faceless enemy: The origins of modern terrorism*. Cambridge, MA: Perseus Publishing.

Shulman, M. R. (1999). Discrimination in the laws of information warfare. *Columbia Journal of Transnational Law, 37*, 939-967.

Skoll, G. (2007). Meanings of terrorism. *International Journal for the Semiotics of Law, 20*(2), 107-127.

Sloan, S. (1981). *A study in political violence: The Indonesian experience*. Norman, OK: University of Oklahoma Press.

Sloan, S. (2006). *Terrorism: The present threat in context*. Oxford: Berg Publishers.

Slone, M (2000). Response to media coverage of terrorism. *Journal of Conflict Resolution, 44*(4), 508-522.

Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge: Cambridge University Press.

Stamper, R (1996). Signs, norms, and information systems. In B. Holmqvist (Ed.), *Signs at work* (pp. 349-397). Berlin, Germany: Walter de Gruyte.

Subramanya, S. R., & Lakshminarasimhan, N. (2001). Computer viruses. *IEEE Potentials 20*(4), 16-19.

Talbot, D. (2005, January 27). Terror's server. *Technology Review, 1,* 46-52.

Tedeschi, B. (2003, January 27). Crime is soaring in cyberspace. *The New York Times,* p. A1.

Tricker, R.I. (1992). *The management of organizational knowledge*. Oxford: Blackwell

Tuman, J. S. (2003). *Communicating terror: The rhetorical dimensions of terrorism*. Thousand Oaks, CA: Sage.

Tzfati, Y & Weimann, G. (2002). www.terrorism.com: Terror on the Internet. *Studies in Conflict and Terrorism*, *25*(5) 317-332.

Verton, D. (2003). *Black ice: The invisible threat of cyber-terrorism*. New York: McGraw-Hill.

Weimann, G. (2004). *www.terror.net: How modern terrorism uses the Internet*. Washington, D.C.: United States Institute of Peace.

Weimann, G. (2005). Cyberterrorism: The sum of all fears? *Studies in Conflict & Terrorism, 48*(2), 129-149.

Weimann, G. (2006). *Terror on the Internet: The new arena, the new challenges*. Washington D.C.: USIP Press Books.

West, M. (1999). Online opportunities. *American Fitness, 17*(4), 63-68.

Wingfield, T. C. (2000). *The law of information conflict: National security law in cyberspace*. Aegis Research Corp, VA: Falls Church.

Wright, J. (1991). *Terrorist propaganda: The Red Army Faction and the Provisional IRA.* New York: St. Martin’s Press.

Wynne, J. (2002, February 14). White house advisor Richard Clarke briefs senate panel on cybersecurity. *Washington File*, p. A14.

Yonah A. (2000), Terrorism in the twenty-first century: Threats and responses. *DePaul Bus. L.J., 12*, 59-83.