Winter 2007

Knowledge and perceptions of "cyberterrorism"

Andrew J. Van Hoogenstyn
University of New Hampshire, Durham

KNOWLEDGE AND PERCEPTIONS OF "CYBERTERRORISM"

BY

ANDREW J. VAN HOOGENSTYN

BA, University of New Hampshire, 2006

THESIS

Submitted to the University of New Hampshire

in Partial Fulfillment of

the Requirements for the Degree of

Master of Arts

in

Justice Studies

December 2007

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

This thesis has been examined and approved.

Ellen S. Coh

Thesis Director, Ellen S. Cohn,
Professor of Psychology

Cesar J. Rebellon,
Assistant Professor of Sociology

Andrew M. Macpherson,
Research Assistant Professor of Justiceworks

12/13/07

Date

DEDICATION

I dedicate this thesis to my family. Your encouragement of my academic and athletic work has inspired me achieve great accomplishments. Thank you for being there for me through all the tough times. Thank you for all your love and support.

ACKNOWLEDGEMENTS

Thank you Dr. Ellen Cohn for your guidance, support and encouragement. You were of great assistance throughout the entire process of the completion of this thesis. I would also like to thank Dr. Cesar Rebellon and Andrew Macpherson for their assistance and guidance. Finally, I would like to thank the entire Justice Studies Department.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

KNOWLEDGE AND PERCEPTION OF "CYBERTERRORISM"

by

Andrew J. Van Hoogenstyn

University of New Hampshire, December 2007

While the threat of terrorists utilizing the Internet to execute a cyberterrorist attack is of prominent concern there exist great misconceptions and factual errors in the media as to the nature of this threat (Conway, 2002; Embar-Seddon, 2002; Weimann, 2005). This thesis examined media exposure, knowledge of cyberterrorism, fear of terrorism and perceived seriousness of cyberterrorist events in a sample of college students. Generally, participants had little knowledge of cyberterrorism. Women were found to be more fearful of terrorism and cyberterrorism than men. A positive relation was found between media consumption and fear of terrorism among women. Finally, fear of terrorism was positively related to perceived seriousness of cyberterrorist events.

CHAPTER I

INTRODUCTION

The Internet provides individuals and businesses around the world with a new medium to communicate and exchange ideas globally. However, the Internet also provides criminals with attractive opportunities to engage in computer crimes. Over the last two decades, the reported incidence of computer crimes has been on the rise (Dowland, Furnell, Illingworth & Reynolds, 1999). One potential threat that has received great attention in recent years is the use of the Internet to engage in terrorist acts. Since the September 11, 2001 terrorist attacks in which over 3,000 were killed, the prevention of terrorism has been a prime concern of the U.S government. (Pyszczynski, Solomon, & Greenberg, 2003).

Increasingly terrorism has been a topic of the media, specifically the use of the Internet by terrorists. The use of computers or networks in executing a terrorist attack is called "cyberterrorism." Unfortunately the media has often exaggerated and embellished the threat of cyberterrorism (Vegh, 2002; Wiemann, 2004). It is the purpose of this thesis to determine what general knowledge people have of cyberterrorism, how serious they perceive cyberterrorism to be and how fearful they are of terrorism. No research has addressed the issue of knowledge and perceptions of cyberterrorism; it is the goal of this thesis to determine whether common misconceptions of cyberterrorism exist that warrant further research. Specifically, what influences do the media have on knowledge and perceptions of cyberterrorism? Additionally, this thesis will examine the relation between fear of terrorism and perceived seriousness of cyberterrorism. Finally, sex differences will be examined in the perceptions of terrorism and cyberterrorism.

Psychological Effects of Terrorism

The attacks of September 11th had significant psychological effects on both those directly exposed and the general American population. During the attacks and at the one year anniversary, the general public was witness to dramatic and robust media attention. Some researchers have reported as much as a 50% increase in the prevalence of one or more anxiety disorders in the general population following terrorist attacks (Cohn et al., 2006). While these findings were tentative due to a small sample size, other studies have found similar results. A second study of full-time employed adults reported significantly greater depressive symptoms for the month following the attacks compared to before with symptoms quickly dissipating after a month (Knudsen, Roman, Johnson, & Ducharme, 2005). In a third study, 16% of adults in a nationally representative sample were found to be significantly bothered by one or more of five distress symptoms immediately following the attacks and over a month later. Those that reported persistent distress were more likely than others to have their daily activities disrupted by thoughts and concerns of terrorism (Stein, et al., 2004). Finally, it was found that proximity to the World Trade Center was related to the reported level of post traumatic stress symptoms (PTSS) and depressive symptoms in college students one year after the attacks (Blanchard, Rowell, Kuhn, Rogers, & Wittrock, 2005). It is clear that terrorist events such as the September 11th attacks had significant psychological consequences and for this reason the perceptions of terrorist attacks require further evaluation.

Defining Terrorism

This thesis will define terrorism according to the following criteria. Terrorism involves premeditated use of violence or the threat of violence to intimidate or coerce a government or an audience of civilians (Whittaker, 2004). The desired outcome will be achieved by instilling fear and insecurity in a population. Force and violence are carefully calculated and implemented against civilians and non-combatants. However, it is not just the threat of violence but the randomness of the attacks that instills fear in target populations. Terrorist goals are usually politically, socially, ideologically or religiously motivated (Whittaker, 2004) and attacks are commonly justified, either on religious or ideological grounds (Burns & Peterson, 2005). Terrorist acts are carried out by a sub-national group, clandestine agent or individuals (Whittaker, 2004). Finally attacks are perpetrated with the intent of attracting maximum media attention (Burns & Peterson, 2005).

Creating a definition of terrorism may seem straight forward. However, when considering the varying political agendas, it is difficult not to have a biased perspective. For example, Steater (1990) in an analysis of *Time Magazine* found the label “terrorist” was often reserved for anti-government left-wing extremists. This problem is illustrated best by the saying, "One man's terrorist is another man's freedom fighter" (Ash, 2002, p. 62). To attempt to differentiate between the two, it will be helpful to define a "freedom fighter". A freedom fighter conducts a campaign to liberate his/ her people from dictatorial oppression, or from an occupying power. The key difference between the terms “freedom fighter” and "terrorist" is the terrorist's deliberate use of violence towards non-combatants (Whittaker, 2004). It is possible for a freedom fighter to harm or kill a civilian inadvertently; however this would only be in the form of collateral damage.

Event Features of a Terrorist Attack

Recent research has focused on the perceived severity of specific features of terrorist events in an attempt to determine the most salient aspects of a terrorist attack. The following features of an attack were rated by respondents as the most salient (in descending order): type of the attack (e.g. bomb, fire arm, knife, etc.), suicide attacks, number of casualties, and the target of the attack (Jenkin, 2006). In addition, events that were perceived to be random attacks were reported to be more serious. When respondents were asked about future terrorist attacks, the type of weapon used and level of disruption were the two most salient features reported. However, respondents did not differ in their reactions to an actual attack compared to that of a threat of an attack. Finally, a relation between fear and communication was found, as individuals that were fearful after an attack were more apt to seek outside communication (Jenkin, 2006).

The features of a terrorist event have a significant effect on an individual's perception of the severity of an attack. In his work, Jenkin (2006) focused on more conventional terrorist scenarios including: biological attacks, bomb attacks, chemical attacks, firearm attacks and radiological attacks. However, recent attention by the media and our government has turned to the threat of cyber crimes, Internet crimes and cyberterrorism. It is the focus of this thesis to explore the realm of Internet crimes, most specifically, cyberterrorism.

Computer Attacks

Internet crime includes a variety of behaviors from sex offenses to identity theft; however this thesis will focus on the use of computers as weapons or as targets to carry out a terrorist attack. In a report to Congress, computer attacks were defined as "actions directed against computer systems to disrupt operations, change processing control, or corrupt stored data." (The Library of Congress, 2005, p. 6) As this thesis will be focusing on cyberterrorism, the primary foci will be on these kinds of attacks. Computer attacks include physical attacks, which use conventional weapons in the destruction of computer facilities or transmission lines. This includes electronic attacks, which use electromagnetic energy (most commonly in an electromagnetic pulse or EMP) to overload computer circuitry or to insert malicious code into microwave radio transmissions. Computer network attacks or "cyberattacks" include but are not limited to the use of malicious code as a weapon to infect computers by exploiting weaknesses in software, in system configuration, or in computer security practices (The Library of Congress, 2005).

Since the late 1990's cyberattacks have been increasing in both frequency and sophistication (Institute for Security Technology Studies, 2001). U.S. and allied military strikes and incidents have resulted in retaliatory cyberattacks against American infrastructure of economic, political or symbolic value. For example, following the collision of a U.S. spy plane and a Chinese fighter air craft in 2001, an Internet campaign of cyber attacks and web defacements broke out between countries. Cyberattacks may be perpetrated by hackers or thrill seekers, terrorist sympathizers and anti-U.S. hackers, nation-states or terrorist organizations (Institute for Security Technology Studies, 2001). Perpetrators may use computers to attack other computers in a number of ways including: email and other miscellaneous viruses, Trojans and backdoors, worms, time bombs, spyware, adware or stealware (Erbschloe, 2005). To date terrorists have only used the

Internet to formulate plans, communicate, raise money and spread propaganda (Lewis, 2003). It is the aim of this paper to examine the possibility that terrorists may begin to utilize the Internet in a new way, to aid in the execution of future terrorist attacks.

Defining Cyberterrorism

Congress defined cyberterrorism as, "the use of computers as weapons, or as targets, by politically motivated international or sub-national groups or clandestine agents who threaten or cause violence and fear in order to influence an audience or cause a government to change its policies" (The Library of Congress, 2005). Like terrorism, cyberterrorism involves the purposeful threat or use of violence to achieve a political or social goal. However, cyberterrorism is perpetrated through a different medium, computers. Thus, cyberterrorism includes the use of computers as weapons and computers as targets of conventional weapons or other computers.

One of the more comprehensive definitions of cyberterrorism put forth by Verton (2003) specifically addresses computers as weapons and as targets. According to Verton cyberterrorists (either a sub national foreign group or individual with a domestic political agenda) will use computer technology and the Internet to compromise a nation's electronic or physical infrastructure. Such an attack would result in the disruption of a critical service such as the Internet, electric power, 911 emergency systems, telephone service or banking to name a few (Verton, 2003, p. *xx*).

This thesis will define "cyberterrorism" as the use of the computers and networks to execute a terrorist attack. Computers may be used as weapons or as targets (The Library of Congress, 2005). The purpose of a cyberterrorist attack is to cripple or disrupt a nation's electronic and physical infrastructure (Verton, 2003). Such attacks are perpetrated by international or sub-national foreign terrorists or clandestine agents. Attacks include the threat or use of violence and fear. Finally, “cyberterrorist” attacks deliberately target non-combatants to influence an audience, attract maximum media attention, and bring about political or societal changes (Burns & Peterson, 2005; Whittaker, 2004).

To create a complete definition of cyberterrorism, it will be useful to define what is not included. First and foremost cyber or computer crime is not necessarily cyberterrorism. Cyber crime can be defined as the "the use of computers to facilitate or carry out a criminal offense." (Katyal, 2001, p. 1005) Cyber crime includes computers as the victim of an attack (e.g. unauthorized access, unauthorized destruction, or theft of information) and the use of computers to facilitate a crime (e.g. child pornography, copyright infringements, or white collar crimes). A cyberterrorist attack may include a cyber crime such as unauthorized access, but unauthorized access itself is not cyberterrorism. Thus, the execution of a cyberterrorist attack may entail different cyber crimes, but any one cyber crime is not necessarily an act of cyberterrorism (Katyal, 2001).

Terrorists may engage in a variety of activities on computers that are not classified as cyberterrorism. Among them are the use of the Internet by terrorists to spread propaganda, engage in fundraising, recruit personnel, communicate among terrorist cells or encrypt information (Conway, 2002; Embar-Seddon, 2002; Weimann, 2005). While some of these behaviors may be illegal, they are not in themselves acts of cyberterrorism.

Terrorists should not be confused with hackers. Hacking is defined as "activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software." (Weimann, 2005, p. 135) Hacktivists are politically motivated hackers that seek to disrupt and protest but not kill, maim or terrify, thus they are not classified as cyberterrorists (Weimann, 2005). Few criminal acts on the Internet are acts of terrorism and thus can not be classified as cyberterrorism; however as will be explained later, there is significant misunderstanding as to what cyber crimes constitute cyberterrorism.

Advantages of Cyberterrorism

Cyberterrorism has several advantages over traditional terrorist methods. As mentioned before, terrorists desire maximum media exposure, and recently the Internet and computer crimes have received significant attention. The Internet provides terrorists with a diverse set of global targets (Silke, 2003). If anonymity is desired computer attacks are difficult to detect or trace and attacks are easy to carry out (Embar-Seddon, 2002). Such attacks may have a significant impact as they target infrastructure vulnerabilities. By utilizing computers, terrorists may simultaneously attack with computers and conventional weapons. Of great importance, cyberterrorism has an added psychological threat as anyone can be a victim at any time. Unlike conventional terrorist attacks that generally target significant landmarks and symbols, cyberterrorists may target an entire region (Silke, 2003).

Cyberterrorism is also a “force multiplier”. In other words, cyberterrorist attacks increase the striking potential of a unit without requiring an increase in personnel. Cyberterrorism is a force multiplier in two ways; via mass media attention, attacks may appear significantly more destructive than they actually are and computer technologies can increase the striking power of conventional weapons (Embar-Seddon, 2002). With technology becoming more sophisticated, cyberterrorist attacks are only becoming a more attractive method for terrorist organizations and individuals; however, such an attack has not yet occurred.

Since the mid-1990's there have been a large number of terrorist incidents and cyberattacks but not one incident of a cyberterrorist attack. At the present time cyberterrorism may not be the preferred choice of terrorists for two reasons. Terrorist groups such as Al Qaeda prefer explosives due to their dramatic and instantaneous physical damage and psychological impact. Second, cyberterrorist scenarios involving critical infrastructure are unrealistic. Critical infrastructures do not always depend on a computer network accessible to the Internet and those that do are still under human control for vital mechanisms (Lewis, 2003). Not only is the U.S. infrastructure redundant but failures are common and we know how to fix them. For these reasons cyberattacks have not yet been executed by a terrorist group.

Common Misconceptions of Cyberterrorism

Despite hackers launching the majority of computer attacks, there exists great concern over cyberterrorism. There are four factors that have contributed to the fear of cyberterrorism. First, misinformation has led to greater fear; typically things that are not understood are feared. Second, the media exaggerates the threat and fails to distinguish between terrorists and hackers. Third, ignorance has led to the confusion between cyber crime and cyberterrorism. Finally, politicians use public anxiety of terrorism to advance their own agendas. Such fear can be economically rewarding; after September 11th, 2001 Congress received 4.5 billion dollars for infrastructure security (Weimenn, 2005).

Cyberterrorism is often over used, misused and misunderstood in the popular media (Embar-Seddon, 2002). The greatest misconception is the belief that cyberterrorism is commonly occurring; however a cyberterrorist attack has never occurred (Coway, 2002; Weimann, 2005). Since the attacks of September 11th, 2001 special attention has been focused on terrorism and cyber security. Unfortunately, experts often classify protesters, hackers, and hacktivists as cyberterrorists despite different motivations and outcomes. Newspapers often sensationalize accounts of cyber crimes and often lack factual basis. In addition, vague wording is often used when discussing the time, place or nature of cyberattacks (Vegh, 2002). Finally, both the government and media have focused on the risk of the use of encryption by terrorists, despite the fact that encryption is commonly used to protect legitimate communications.

Fear of the Internet, Technology and Cyberterrorism

These common misconceptions of cyberterrorism are coupled with an existing fear that many have in regards to the Internet and computer technology. Such fears are understandable as the Internet provides criminals complete anonymity and the means to commit crimes covertly, from distant locations. Additionally, worms and viruses run rampant on the Internet; the chance of contamination is great. Finally, there exists the fear of unchecked surveillance. The Internet has been described as the "wild wild West", in which, the four horsemen of the information apocalypse are terrorists, drug dealers, money launderers and child pornographers (Sandywell, 2006). It is no surprise that many people are both confused and in fear of computer crimes such as cyberterrorism.

Terror management theory may help to examine reactions to terrorist events, and more specifically, may aid in the understanding of the fear of cyberterrorism. Terror management theory states that a human awareness of annihilation is the "awareness that such threats are ubiquitous and will all eventually succeed: death will be our ultimate fate." (Pyszczynski, et al., 2003, p. 8). Terrorist attacks interrupt our means of managing natural terrors or our "psychological equanimity". This theory is based on the proposition that humans are creatures that seek to have meaning in a meaningful world and will devote considerable time in maintaining this faith. It is destructive acts such as terrorist attacks that compromise this faith, while as death becomes more salient, the quest for meaning becomes more intense (Pyszczynski, et al., 2003). It is this underlying fear of death and a loss of meaning that makes terrorism so disturbing psychologically. In addition to this, the ambiguous and threatening nature of cyberterrorism may only enhance this already salient fear of death.

Public Opinions of Cyber Crime

Widespread confusion in the media between cyber crimes and cyberterrorism begs the question, what knowledge does the general public have about cyberterrorism and what are the common beliefs and misconceptions? While little research is available on cyberterrorism, research has examined public awareness of computer crimes. British researchers Dowland, Furnell, Illingworth, and Reynolds (1999), surveyed individuals to determine public awareness and attitudes towards computer crimes and the influence the media had on their perceptions of these crimes. Eighty percent of the respondents believed computer crime to be a significant problem and found crimes with a clear analogy to real world crimes to be the most serious (sabotage, theft, etc.). Interestingly 71% of respondents believed hacking to be wrong; however 80% of respondents did not believe the invasion of privacy to be wrong. The media had a significant impact on respondents with many reporting that the media glorified computer crimes. A majority of respondents recalled news reports on computer crimes from years before. Finally, headlines from two major newspapers were sensational and misleading. In light of these misconceptions and the potential for a growing reluctance of the public to trust new computer technologies it was concluded that there exists a need for responsible reporting (Dowland, et al., 1999).

The Goal and Hypotheses of the Current Thesis

It is clear that computer and Internet crimes are clouded by uncertainty and fear, and cyberterrorism is no exception. While research has documented the psychological consequences of a conventional attack and assessed public awareness and opinions of computer crimes, little research has focused on cyberterrorism. While a cyberterrorist attack has never occurred, such attacks have been the subject of sensational media coverage, containing both misconceptions and misinformation (Vegh, 2002). It is the aim of this thesis to ascertain some preliminary insight into the knowledge individuals have about cyberterrorism and their perceptions as to how serious cyberterrorist attacks would be.

This thesis has three specific hypotheses. The first hypothesis is that greater media exposure will predict less knowledge of cyberterrorism. The second hypothesis is that fear of terrorism will predict greater perceived seriousness of cyberterrorism. The final hypothesis is that greater media exposure will predict greater perceived seriousness of cyberterrorism.

Previous research has assessed public opinions and knowledge of computer crimes, as well as the influence media consumption has had on their beliefs. Media consumption was found to have a significant impact, as respondents clearly remembered computer crimes from prior years. In addition, there exist contrary beliefs as to what constituted criminal behavior (Dowland et al., 1999). Research has not yet assessed people's knowledge and perceptions of cyberterrorism. It is evident that there exists great confusion in the media as to what constitutes cyberterrorism (Embar-Seddon, 2002). In addition, a significant quantity of research has documented the adverse psychological effects of conventional terrorist attacks. It is the purpose of this thesis to extend the research pertaining to terrorism and computer crimes to cyberterrorism.

To test these hypotheses a survey of college students was conducted. The survey assessed participants' media consumption. Fear of terrorism was measured using the Attitudes Toward Terrorism Scale (Jenkin & Cohn, 2001). Individuals' knowledge of cyberterrorism was assessed in a true/ false questionnaire. Finally, participants rated the seriousness of five cyberterrorist scenarios. This survey was designed to determine what effects the media has on the knowledge and perceived seriousness of cyberterrorism. Additionally, it measured whether there was a relation between fear of terrorism and perceived seriousness of cyberterrorism.

CHAPTER II

METHOD

Participants

Participants were 368 students (including 12 graduate students) from a public university. The sample reflected the expected demographics of a northern New England public university with the sample being 91% white (N = 335), 66% female (N = 244) and ages ranging from 17 to 25 (*M* = 19.59, *SD* = 1.70). Participants were recruited in three different ways. Some undergraduate and graduate students were recruited in summer classes. Other students were recruited during an introductory Justice Studies class during the fall semester with the permission of the professor. Finally, undergraduate psychology students were recruited from a fall semester subject pool. All students were given the option to participate in the voluntary survey. The survey took approximately 15-25 minutes. Some professors gave participants class credit in return for participation. Participants that did not receive class credit were given the option to be entered into a raffle for an iPod. The names of the students that chose to participate in the raffle were kept separate from the questionnaires to ensure confidentiality and anonymity. The winner of the raffle was randomly selected by a neutral third party.

Materials

Demographics. Participants were asked general demographic questions including: class standing, sex, age, religion, ethnicity, area of study, grade point average and political affiliation.

Attitudes Toward Terrorism Scale (ATTS). Participants were asked questions pertaining to their fear of terrorism and perceived risk of terrorism. The ATTS was developed by Jenkin and Cohn (2001) and consisted of 27 separate statements. Participants rated the 27 statements on a six point Likert Scale (1= "Strongly disagree" to 6= "Strongly agree"). These 27 statements ($\alpha = .94$) included statements designed to measure emotional fear of terrorism, (e.g. "When I see a low-flying plane, I worry that it might crash") and perceived risk of victimization (e.g. "I think that I live in a place that is a good target for terrorists") (Jenkin, 2006).

Knowledge of Cyberterrorism Scale. The Knowledge of Cyberterrorism Scale was developed to determine how knowledgeable participants were of the subject of cyberterrorism. Participants were asked 20 true/ false questions pertaining to cyberterrorism ($\alpha = .30$). The Knowledge of Cyberterrorism Scale had items designed to measure participants' classification of terrorist behaviors using computers, (e.g. "The use of computers by terrorist organizations to recruit members is not cyberterrorism"), categorization of specific types of attacks, (e.g. "Cyberterrorist attacks can include both a conventional attack and a computer attack"), and estimation of both the likelihood and success of such attacks (e.g. "Cyberterrorist attacks have been used by state-sponsored terrorists against the United States").

Perceived Seriousness of Cyberterrorism Scale. To determine how serious participants found potential cyberterrorist attacks to be, five hypothetical cyberterrorist attacks were developed from Verton's book, *Black Ice* (2003). Each cyberterrorist attack was described in a short scenario in no more than two sentences. In the Utility Center scenario, terrorists used computer viruses to tamper with and destroy a gas utility center. In the 911 Response scenario, terrorists used a computer worm to overload 911 response centers with cell phone calls. In the Hospital Records scenario, terrorists used computers to gain access and alter patient medical records. In the Commercial District scenario, terrorists used an electromagnetic pulse bomb to damage all electric circuitry in a commercial district. Finally, in the Internet Switching Center scenario, terrorists drove an explosive rigged truck into an Internet switching center to disable the Internet. (See Appendix B)

Participants were asked to rate each scenario on a scale of ten point increments from 0-100 according to their seriousness, (0= "not serious" to 100= "very serious"). After rating the scenarios, participants were given a manipulation check to ensure they had actually read the passages and not written a random response. Participants were asked to list three objects targeted and three methods the terrorists used in the five scenarios without referring back to the scenarios. Participants were excluded if their answers were incorrect or vague.

Media Exposure. To measure media consumption, participants were asked the amount of time and frequency with which they watched television, watched national news broadcasts, read newspapers and read news articles on the Internet (Bucolo & Cohn, 2007). For each media type, they were asked to indicate for each day of the week the frequency they consumed each media type on a five point Likert scale, (1= "never" to 5= "always") and to indicate how many minutes a day they consumed for each type of media. Participants were asked to rate the frequencies with which they watched legal/forensic dramas (e.g. CSI), legal/ crime reality shows (e.g. COPS), police dramas (e.g. NYPD Blue), and courtroom dramas (e.g. Law and Order). They rated each program on a ten point Likert Scale (1= "Never" to 10="Every Chance").

Procedure

All participants read and signed an informed consent form before beginning the survey. Participants who agreed to participate were instructed that the purpose of the research was to examine general knowledge of cyberterrorism, perceptions of terrorism and media consumption. They were asked not to leave any questions blank and to answer each question to the best of their ability. They were given at least thirty minutes to complete the survey. Upon completion of the survey, participants read a debriefing form, which provided them with the purpose and specific hypotheses of the experiment. After reading the debriefing, all participants who did not receive class credit were given the option to enter to win an iPod. Participants who entered the contest were asked to provide their name and email address with the assurance that all personal information would remain anonymous and in no way be linked to their survey.

CHAPTER III

RESULTS

Preliminary Analyses

Participants were excluded from the analysis if they failed the manipulation check following the cyberterrorist scenarios, left a portion of the survey blank, or answered a large portion of the survey with the same response regardless of the question being asked. In total 25 participants were excluded from all analyses because they failed to understand the task.

Ordering Effects. To determine if the order of the measures affected participants' responses two different survey orders (1, 2) were randomly given to participants. In both orders demographic questions were presented first. Order 1 presented the cyberterrorist scenarios last. Order 2 presented the cyberterrorist scenarios immediately following the demographic questions. (See Appendix B for survey order 1.)

To determine if the placement of the scenario measure with respect to the other measures affected participants' responses a mixed model MANOVA was conducted with survey order (scenarios last and scenarios first) as the independent variable and the five scenarios (Utility Center, 911 Response, Hospital Records, Commercial District and Internet Switching Center) as the dependent variables. The between subject effect for survey order was not significant ($F(1, 363) = 1.12, p = .29, \eta^2 = .00$). The placement of the scenarios with respect to the other measures did not affect participants' rating of the scenarios. (See Table 1)

Media Consumption. The minutes of media exposure reported from each day of the week were summed for minutes of news watched (α = .96), minutes of news read (α = .94) and minutes of Internet news read (α = .98). The resulting variables total minutes of news watched (*M* = 104.36, *SD* = 112.20), total minutes of news read (*M* = 53.05, *SD* = 72.12) and total minutes of Internet news read (*M* = 105.97, *SD* = 124.34) were used in the following analyses. Total minutes of news watched ranged from 0 to 630 minutes, total minutes of news read ranged from 0 to 420 minutes and total minutes of Internet news read ranged from 0 to 1320 minutes.

Knowledge of Cyberterrorism Scale. The 20 true/ false questions were coded (incorrect= 0, correct= 1) and summed to calculate a total knowledge score. The raw knowledge score was converted to a 100-point scale to create the variable total knowledge of cyberterrorism (TKC). Participants had little knowledge of cyberterrorism answering 34.35% (*SD* = 9.63%) of the questions correct. Total correct answers ranged from 10% to 75% of the twenty true/ false questions.

Perceived Seriousness of Cyberterrorism. For each participant seriousness rating summed across the five scenario scores (α = .83) were converted to a 100-point scale to create the variable, total seriousness of cyberterrorism (TSC) (*M* = 81.16, *SD* = 13.72). Generally participants perceived the five cyberterrorist scenarios to be serious in nature. Both the individual scenario scores and the total seriousness of cyberterrorism were used in the following analyses.

Factor Analysis Attitudes Toward Terrorism Scale (ATTS). A principal component factorial analysis with Varimax rotation was conducted on the 27 items of the

ATTS. (See Table 2) The analysis was limited to the first four components (all with eigenvalues greater than 1). Items over .50 were loaded onto one of the four components. The first component, general worry of a terrorist attack (GWTA) (*M* = 13.80, *SD* = 5.35), consisted of six items (α = .80) pertaining to the worry that the participant and other individuals were likely to be victims of a terrorist attack ("I believe that people I know live in areas that are likely terrorist targets"). The second component, travel worry of attack (TWA) (*M* = 19.23, *SD* = 6.09) consisted of six items (α = .84) pertaining to fear of a terrorist attack while traveling ("I think that when I travel I am at greater risk of terrorism."). The third component, worry of a biological or chemical attack (WBCA) (*M* = 16.03, *SD* = 6.18), consisted of five items (α = .80) pertaining to a personal worry of being the target of a biological or chemical terrorist attack ("I think that it is likely I will be the victim of a chemical attack"). The forth component, personal worry of attack (PWA) (*M* = 14.51, *SD* = 5.92), consisted of six items (α = .87) pertaining to the personal worry of being a victim of the next terrorist attack ("I have been kept awake at night worrying about being a part of the next big attack"). Items were reverse coded on the factors TWA and WBCA so that a higher score indicated greater fear of terrorism. GWTA was significantly correlated with both TWA and WBCA and TWA was significantly correlated with WBCA. See Table 3 for correlations.

Additionally, a total fear of terrorism score was calculated from the 27 items (α = .94) of the ATTS. All questions were recoded so the greater the score on each item the greater the reported fear. The total was summed and the raw score converted to a 100-point scale to form the variable total fear of terrorism (TFT) (*M* = 51.66, *SD* = 15.44).

Sex Differences in Fear of Terrorism. To determine whether sex differences existed a MANOVA was conducted with sex as an independent variable and TFT, GWTA, WBCA, PWA and TWA as dependent variables. A significant multivariate effect was found for sex, $\Lambda = .91$, ($F(5, 301) = 5.77, p < .001$). Significant between subjects effects for sex were found for TFT ($F(1, 305) = 17.67, p < .001$), TWA ($F(1, 305) = 20.06, p < .001$) WBCA ($F(1, 305) = 9.91, p < .01$), and PWA ($F(1, 305) = 20.30, p < .001$). GWTA was not significantly different ($F(1, 305) = 3.03, p = .08$). Women reported being more afraid than men on four out of five measures of fear of terrorism. (See Table 4)

Primary Analyses

Predicting Knowledge of Cyberterrorism. The first hypothesis was that media exposure would be negatively related to knowledge of cyberterrorism. A linear regression analysis was conducted with total minutes of news watched, total minutes of news read, total minutes of Internet news read, frequency of legal/ forensic dramas watched, frequency of legal/ crime realities watched, frequency of police dramas watched and frequency of political commentaries watched as the independent variables and total knowledge of cyberterrorism as the dependent variable. The overall regression was not significant ($F\ (7, 320) = 1.18, p = 0.31, R^2 = .03$, *adj.* $R^2 = .00$). (See Table 5) Media exposure did not predict knowledge of cyberterrorism. See Table 6 for correlations.

Predicting Perceived Seriousness of Cyberterrorism from Fear of Terrorism. Second, it was hypothesized that greater fear of terrorism would predict greater perceived seriousness of cyberterrorist scenarios. Five multiple regressions were conducted for each cyberterrorist scenario with GWTA, TWA, WBCA and PWA from the ATTS entered as the independent variables and the five individual scenario seriousness rating as the dependent variables. The overall regression was significant for the Utility Center scenario (*F* (4, 308) = 2.69, *p* = .03, R^2 = .03, *adj.* R^2 = .02), however none of the predictors were significant. The overall regression was significant for the 911 Response scenario (*F* (4, 308) = 3.63, *p* < .01, R^2 = .05, *adj.* R^2 =.03), PWA was a significant predictor. The overall regression was not significant for the Hospital Records scenario (*F* (4, 308) = 1.64, *p* = .17, R^2 = .02, *adj.* R^2 = .01). The overall regression was significant for the Commercial District scenario (*F* (4, 308) = 3.99, *p* < .01, R^2 = .05, *adj.* R^2 = .04), but none of the predictors were significant. The overall regression was significant for the Internet Switching Center scenario (*F* (4, 308) = 2.59, *p* = .04, R^2 = .03, *adj.* R^2 = .02), but again none of the predictors were significant. The high degree of collinearity between the fear of terrorism variables (GWTA, TWA, WBCA, PWA) can account for a lack of significant predictors despite the significant overall regressions. See Table 7 for unstandardized and standardized beta weights and Table 8 for correlations.

Predicting Perceived Seriousness of Cyberterrorism from Media Exposure.

Finally, it was hypothesized that greater media exposure would predict greater perceived seriousness of cyberterrorist scenarios. Three linear regressions were run, two separate regressions for men and women and a third including both men and women. In all three regressions total minutes of news watched, total minutes of news read, total minutes of Internet news read and frequency of legal/ forensic dramas watched were the independent variables and total perceived seriousness of cyberterrorist scenarios was the dependent variable. The overall regression was not significant for men (*F*(4, 113) = 1.58, *p* = .18, R^2 = .05, R^2 *adj.* = .02), women (*F*(4, 228) = 1.89, *p* = .11, R^2 = .03, R^2 *adj.* = .02), or both men and women ($F(4, 346) = 1.74$ $p = .14$, $R^2 = .02$, R^2 *adj.* = .01). (See Table 9)

Three more linear regressions were run for men, women and both men and women with total minutes of news watched, total minutes of news read, total minutes of Internet news read, frequency of legal/ forensic dramas watched and total fear of terrorism as the independent variables and total perceived seriousness of cyberterrorist scenarios as the dependent variable. The overall regression was not significant for men, $F(5, 88) = 31.26, p = .29$, $R^2 = .07$, *adj.* $R^2 = .01$). The overall regression was significant for women ($F(5, 193) = 3.41, p < .01$, $R^2 = .08$, *adj.* $R^2 = .06$), significant predictors included total minutes of news read and total fear of terrorism. Perceived seriousness of cyberterrorism was negatively related to news read and positively related to fear of terrorism among women. The overall regression was significant for both men and women ($F(5, 287) = 3.91, p < .01$, $R^2 = .06$, *adj.* $R^2 = .05$), total fear of terrorism was a significant predictor. Fear of terrorism was positively related to perceived seriousness of cyberterrorism. (See Table 10)

Because it was found that women were more fearful than men on several measures of fear of terrorism an analysis was run to determine if there existed sex differences in perceived seriousness of cyberterrorism. A mixed model MANCOVA was conducted with sex as an independent variable, total minutes of news watched, total minutes of news read, total minutes of Internet news read and frequency of forensic dramas watched as the covariates and the five seriousness ratings of the cyberterrorist scenarios as the dependent variables. Only total minutes of news read ($\Lambda = .97$, F (4, 342) = 2.55, $p = .04$, $\eta^2 = .02$) was a significant covariate. None of the other covariates were found to be significant: total minutes of news watched ($\Lambda = .97$, (F (4, 342) = 2.29,

$p = .06$, $\eta^2 = .03$), total minutes of Internet news read ($\Lambda = .99$, $F\,(4, 342) = 1.14$, $p = .34$, $\eta^2 = .01$), and frequency of forensic dramas watched ($\Lambda = .99$, $F\,(4, 342) = .78$, $p = .54$, $\eta^2 = .01$). A significant multivariate effect for sex was found, ($\Lambda = .95$, $F\,(4, 342) = 4.79$, $p = .001$, $\eta^2 = .05$). Sex had a significant effect on the five seriousness ratings of the cyberterrorist scenarios. The between subjects sex effect approached significance, ($F(1, 345) = 3.60$, $p = .059$, $\eta^2 = .01$) Follow up independent samples t-tests found women rated the Utility Center ($t(1, 366) = -2.76$, $p < .01$), 911 Response ($t(1, 366) = -3.18$, $p < .01$) and Hospital Records ($t(1, 365) = -3.60$, $p < .001$) scenarios to be more serious than men. There were no differences between the Commercial District ($t(1, 364) = .86$, $p = .39$) and Internet Switching Center scenarios ($t(1, 366) = .64$, $p = .52$). A significant between subjects effect was found for total minutes of news read, ($F(1, 345) = 3.79$, $p = .05$, $\eta^2 = .01$). (See Table 11)

Additional Analysis

Predicting Fear of Terrorism. An additional analysis was conducted to determine if fear of terrorism could be predicted by knowledge of cyberterrorism, media exposure and sex. Regression analyses were performed separately for men and women with total minutes of news watched, total minutes of news read, total minutes of Internet news read, frequency of legal/ forensic dramas watched and total knowledge of cyberterrorism as the independent variables and total fear of terrorism as the dependent variable. The overall regression was non-significant for men, ($F\,(5, 81) = .61$, $p = .69$, $R^2 = .04$, *adj.* $R^2 = -.02$) (See Table 16). However, for women the overall regression was significant ($F\,(5, 186) = 5.31$, $p < .001$, $R^2 = .13$, *adj.* $R^2 = .10$), significant predictors included total minutes of news watched, total minutes of news read, frequency of legal/ forensic dramas watched and total knowledge of cyberterrorism. (See Table 12) For women, fear of terrorism was negatively related to knowledge of cyberterrorism and exposure to print news and positively related to exposure to television news broadcasts and legal/ forensic dramas. See Table 13 for correlations.

A second regression was run with sex (dummy coded), total minutes of news watched, total minutes of news read, total minutes of Internet news read, frequency of legal/ forensic dramas watched, frequency of legal/crime dramas watched, frequency of crime reality shows watched, frequency of political commentaries watched and total knowledge of cyberterrorism as independent variables and total fear of terrorism as the dependent variable. The overall regression was significant, (F (9, 268) = 3.87, p < .001, R^2 = .12, *adj.* R^2 = .09). Significant predictors of fear of terrorism included sex and total minutes of news read. Again, there was a negative relation between minutes of news read and total fear of terrorism. See table 13 for correlations and Table 14 for standardized and unstandardized beta weights.

CHAPTER IV

DISCUSSION AND CONCLUSION

The media often misuses and overuses the term "cyberterrorism" (Embar-Seddon, 2002) in vague, sensationalized accounts (Vegh, 2002). On this basis it was hypothesized that greater exposure to media would be related to greater misconceptions of cyberterrorism. Thus, it was expected that greater media consumption would be related to less knowledge of cyberterrorism. No relation was found but this is not surprising as the majority of respondents had very little knowledge of cyberterrorism, answering only 34% of the twenty true/ false questions correctly.

The lack of knowledge about cyberterrorism may be related to misleading and sensationalized media coverage of cyberterrorism (Ballard, Hornick, McKenzie, 2002; Conway, 2002; Vegh, 2002). The lack of knowledge may also be due to a scarcity of available factual information pertaining to cyberterrorism. Again, this makes sense as there appears to be great confusion and ignorance when it comes to details of cyberterrorism (Weimenn, 2005).

It was hypothesized that fear of terrorism would predict perceived seriousness of cyberterrorism. This hypothesis was supported as fear of terrorism was positively related to perceived seriousness of cyberterrorist scenarios. It is not surprising that individuals that are more fearful of terrorism would find cyberterrorism to be more serious.

Again, on the basis that cyberterrorism is sensationalized in the media (Vegh,

2002) it was hypothesized that greater media exposure would be related to greater perceived seriousness of cyberterrorism. No relation was found between the media measures and the perceived seriousness of cyberterrorism. However, media exposure and fear of terrorism were found to be related to perceived seriousness of cyberterrorism among women and among men and women combined. Among women perceived seriousness of cyberterrorism was negatively related to exposure to news broadcasts and was positively related to fear of terrorism. It may be that media exposure can predict perceived seriousness of cyberterrorism but only when fear of terrorism is accounted for.

This thesis found a significant sex effect as women were more fearful of terrorism and rated cyberterrorist scenarios to be more serious than men. The greater fear among women is confirmed by the literature as women have been found to judge a variety of events involving the threat of physical injury to be more harmful than men. Additionally, women believe there to be a higher probability that they would experience harmful events compared to men (Fetchenhauer & Buunk, 2005). This thesis shows that the threats of terrorism and cyberterrorism are no exception as women were more fearful of terrorism than men and rated cyberterrorist events to be more seriousness than men.

Finally, for women it was found that fear of terrorism was negatively related to knowledge of cyberterrorism and positively related to exposure to television news broadcasts and legal/ forensic dramas. As would be expected less knowledge is associated with greater fear of terrorism. Typically, things that are poorly understood are more likely to be feared (Weimenn, 2005). Crime on the Internet is a worry of many. The Internet provides criminals with the perfect opportunity to target individuals anonymously without fear of detection (Sandywell, 2006). Cyberterrorism is one of many possibilities the Internet provides terrorists and as this thesis shows it is a poorly understood possibility. Additionally, as was expected greater exposure to television media was associated with greater fear of terrorism.

This preliminary research demonstrates the need for more accurate information as to the nature of the threat of cyberterrorism. Why is there such little knowledge of cyberterrorism and why did participants rate the scenarios to be so serious? While participants were only moderately fearful of terrorism it still begs the question, where do these fears come from and what are the psychological, social and political repercussions of such fears?

The media is one of the major influences upon public opinion. For example, fear of crime may be better explained by the media than by the actual crime rate. In a recent study in Norway, it was found that reading tabloid headlines was associated with greater avoidance behavior and worry of victimization (Smolej & Kivivuori, 2006). While it could not be concluded that this was a causal relation, it is clear that the media's portrayal of crime is related to consumers' fear of crime and victimization.

Terrorism and terrorist events have long since been a popular focus of the media. Similar to crime, terrorism is also over-emphasized in the media. Despite a consistent pattern of international terrorism, post-Cold War media reported increasing levels of international terrorism (Enders & Sandler, 1999). Additionally, newspapers focus the majority of their attention toward the more horrific terrorist events. These cases that do receive the most print provide an opportunity to address policy and social issues. For example, after the 1993 terrorist bombings of the World Trade Center the *New York Times* highlighted the issues of automobile searches and access to explosive materials

(Chermak & Gruenewald, 2006).

It is clear that the media does not present the issue of terrorism without bias. Steater (1990) in his analysis of *Time Magazine* found that terrorist events in countries allied with the U.S. received little media attention. On the other hand, domestic terrorist events received great attention (Chermak & Gruenwald, 2006). Thus, it could be possible media coverage is reinforcing the threat of domestic terrorist events, making the possibility of being a victim of a cyberterrorist attack seem more likely.

Terrorism is also a popular subject in Hollywood movies. Recurring themes are patriotism, excessive violence and guns, glorification of technology, the masculine hero and exotic alien threats. The terrorists are unrealistically portrayed as purely evil, irrational and excessively violent while the hero is modeled after a James Bond or Rambo, saving the world from weapons of mass destruction. By depicting terrorists as such, it may wrongly justify the torturing of terrorists (Boggs & Pollard, 2006). Popular media helps to distort reality reinforcing fear, anxiety and paranoia in the general public and rationalizing simplistic solutions to complicated situations.

Differences in the presentation of terrorist incidents on television and in newspapers translate to differences in emotional responses by media consumers. While television could explain viewers' emotional response newspapers could not (Cho, Boyle, Keum, Shevy, McLeod, Shah, et al., 2003). Despite these differences both forms of media left consumers believing the incident was important, a solution desirable and that both the media and public attention were important (Weimann, 1990).

In the current thesis different forms of media exposure were related to different responses among women. While watching news broadcasts and legal forensic dramas was positively related to fear of terrorism, reading news was negatively related to be fear of terrorism and perceived seriousness of cyberterrorist scenarios. As previous literature suggests, different forms of media exposure are related to different emotional responses (Cho et al, 2003).

Altheide (2004) argues that the media has transformed terrorism from an event to a condition. A content analysis of news accounts, advertisements and political and military actions following the September 11th attacks found simplistic explanations of the events, who was to blame and what was to be done. Terrorism was used generally to include all enemies of the U.S. Most importantly was the use of the fear of terrorism to promote patriotism and the support of the war on terror, a never ending war with no specific enemy.

In a later analysis by Altheide (2006) of newspaper content before and after the September 11th attacks a dramatic increase in linking the words "fear" and "victim" to "terrorism" was found. By keeping the explanations of the events simple and fears applicable to everyday life the media was able to expand the situation to involve all Americans. This "politics of fear" was found to be a central theme of media coverage of the attacks. For these reasons, the media is an important factor in the representation of significant events and plays a vital role in shaping public opinions.

Debrix (2001) argues similarly that the threat of cyberterrorism is part of the bigger theme of "common anxiety in an age of uncertainty" (p. 153). Without the media, this threat of cyberterrorism would have never become an imminent public emergency. Debrix reminds us how convincing the media was during the Y2K phenomena. The warnings of computer meltdowns were without merit as the new millennia passed without incident. He argues this is how the media portrays cyberterrorism, an uncertain danger that requires preventative emergency measures.

In the current thesis, a relation was found between fear of terrorism and fear of cyberterrorism. Among women fear of terrorism was negatively related to knowledge of cyberterrorism and positively related to total minutes of news watched and the frequency of legal/ forensic dramas watched. It is clear that both media exposure and fear of the unknown is contributing to the fear of terrorism and perceived seriousness of cyberterrorism among women.

This thesis did not find any significant effects for fear of terrorism or cyberterrorism among men. This may be due to the small sample size of men. However, the lack of significant findings for men may be because they are generally less fearful. Males are less fearful of violent events so it is not surprising they would be less fearful of terrorism and perceive cyberterrorism to be less serious. It may be that the measures used were not sensitive enough to detect differences in fear among males. Future research should find a larger sample of men and utilize a more sensitive measure of fear.

There are several other limitations that should be addressed in further research. This thesis asked participants to judge how serious cyberterrorist scenarios were. Generally participants rated the scenarios quite serious, creating a ceiling effect. A baseline or control may have been helpful in determining how serious participants believed a cyberterrorist event to be relative to other crimes. Another important question to ask is how likely does one believe such an event will actually take place. It may be that participants judge all cyberterrorist events to be serious but find them very unlikely to occur.

Participants had very little knowledge of cyberterrorism. While this study utilized a true/ false measure, it might be helpful to try a different method when measuring knowledge. Individuals could be asked to provide a written definition of cyberterrorism to measure knowledge.

This thesis measured media exposure in two ways, minutes of consumption and frequency of consumption. While there measures are effective for determining the types and quantity of media consumed, it did not provide any information as to the actual media content to which participants were exposed. The greater exposure women had to news broadcasts and legal/ forensic dramas, the greater their fear of terrorism, but what specific shows were they watching? A content analysis for cyberterrorism or other related terms in different media sources could further our understanding of the context in which cyberterrorism is presented in the media. For example, in a newspaper article, how frequently is the term used, where is it located within the article (headline, text, figure), within what context is the term used and where is the article located in the newspaper? Such analysis could specifically determine how the media is biased, factually incorrect or sensationalizing the threat of cyberterrorism.

A second way to measure media exposure would be to specifically ask about exposure to terrorism and cyberterrorism in the media. This approach was taken in a study of crime news in Norway in which participants were asked what media types were important sources of crime news (Smolej & Kivivuori, 2006). A similar approach to studying terrorism could be taken. This could be especially helpful for studying terms that occur infrequently in the media, as may be the case with the term “cyberterrorism”.

Another direction for future research addressing cyberterrorism and media exposure is to examine a broader range of media sources. For example, this thesis did not ask about video game consumption. It may be that fear of terrorism and perceived seriousness of cyberterrorism is related to an alternate media source such as computer games among men. Again, it may be easiest to identify media sources of cyberterrorism by simply asking individuals to form a list.

Further research could utilize a similar paradigm to that of Jenkin's (2006) to determine what features of a cyberterrorist attack are most severe. The cyberterrorist scenarios used in the current thesis made no mention of the terrorist group responsible, casualties, or of suicide bombers. By making the scenarios more specific, it could be determined what unique features of a cyberterrorist attack are most feared by the general public.

Finally, taking into account proximal location is another important question that could be addressed in future research. Proximity to the World Trade Center has been found to be related to greater incidence of depressive symptoms in college students (Blanchard et al., 2005). Additionally, inhabitants of large cities may be more likely to worry about terrorism than those in rural areas. This has been found to be the case for fear of crime (Smolej & Kivivuori, 2006).

The current thesis underlines the importance of the psychological implications of a terrorist attack. How do terrorist attacks such as September 11th affect the individual? A three year longitudinal study following the September 11th attacks found forward thinking (e.g. coping by emergency planning) was associated with greater fear of future terrorist attacks and psychological distress. Additionally, television watching immediate following the attacks was associated with fear of future terrorism (Holman & Roxane, 2006). The current study found women's fear of terrorism was related to media exposure. It is clear that terrorist events are associated with future fears of terrorist attacks, which is one of the goals of terrorism.

Individuals' fear of future terrorist attacks has both political and social implications. The purpose of terrorism is to threaten to use or use violence to intimidate a government or an audience of civilians to make political, social, ideological or religious changes (Whittaker, 2004). In most cases terrorist events are designed to attract maximum media attention (Burns & Peterson, 2005). Thus, it is possible that the media is actually empowering the terrorists, spreading their message to a wider audience or even rationalizing their behaviors (Weimann, 1990). However, others claim the media focus only on the violence, portraying terrorists as irrational psychopaths and cold blooded killers (Steater, 1990). Either way, it is important to know how the media is portraying terrorism and potential cyberterrorist attacks and to identify responses such coverage will elicit. We want to avoid causing unnecessary psychological distress.

Cyberterrorism is presented in the media and among some experts as the next great threat to the U.S. and is sometimes referred to as the "Digital Pearl Harbor" (Lewis 2003; Vegh, 2002; Weimann, 2005). Cyberattacks by hackers and terrorists' use of the Internet to advance their cause (e.g. recruitment) are mistakenly classified as cyberterrorism (Vegh, 2002). Contributing to the misconceptions, cyberterrorism is often used as a policy issue for politicians (Weimann, 2005) and to advance social issues by the media (Chermak & Gruenewald, 2006). Cyberterrorism has several psychological and tactical advantages to that of a conventional attack (Embar-Seddon, 2002; Silke, 2003). However, despite the multitude of cyber attacks and conventional terrorist attacks over the last decade there has been no single incident of a terrorist group utilizing a cyber or network attack that could classify as cyberterrorism (Conway, 2002; Lewis 2003; Weimann, 2005).

This thesis found a relation between media exposure and fear of terrorism, and perceived seriousness of cyberterrorism. The media is shaping individuals' perceptions of the threat of cyberterrorism. Additionally, there is a general lack of knowledge pertaining to the idea of "cyberterrorism". For these reasons it of the utmost importance that the media accurately reflect the true threat of cyberterrorism.

The current thesis has several important policy recommendations for decision makers. For the time being terrorist prefer the immediate carnage that traditional weapons provide and appear to be reluctant to try cyberattacks. Still, terrorists are utilizing the Internet. The literature suggests that the real threat lies in the protection of information security (Lewis, 2003). This is why our decision makers should avoid focusing their efforts on "cyberterrorism" and address the issues of network and information security on the Internet. Less emphasis should be placed on the threat of the loan hacker and more attention paid to the alienated insider. Why contribute unnecessarily to the fear of cyberterrorism and ignore the more immediate threat to information security. Accurate portrayals of the threat of terrorism, cyberattacks and network security by experts and the media will allow decision makers to focus on the more immediate threats and avoid misrepresenting the less realistic possibility of cyberterrorism.

LIST OF REFERENCES

Ash, T.G. (2002). Is there a good terrorist? In C.W., Kegley. Jr. (Ed.)., *The New Global Terrorism: Characteristics, Causes, and Controls.* (pp. 60-70) Prentice Hall.

Altheide, D. (2004) Consuming terrorism. *Symbolic Interaction, 27,* 289-308.

Altheide, D. (2006) Terrorism and the politics of fear. *Cultural Studies Critical Methodologies, 6,* 415-439.

Ballard, J., Hornick, J., & McKenzie, D. (2002). Technological facilitation of terrorism. *American Behavioral Scientist, 45,* 989-1016.

Blanchard, E., Rowell, D., Rogers, R., & Wittrock, D. (2005). Posttraumatic stress and depressive symptoms in a college population one year after the September 11 attacks: the effects of proximity. *Behavioral Research and Therapy, 43,* 143-150.

Boggs, C. & Pollard, T. (2006) Hollywood and the spectacle of terrorism. *New Political Science, 3,* 335-351.

Bucolo, D., & Cohn, E. (2007). *The CSI Effect? The association between legal attitudes watching crime dramas.* A poster presentation at the 19th annual Association of Psychological Science Convention. Washington, D.C.

Burns, V., & Peterson, D. (2005). *Terrorism A Documentary and Reference Guide.* Connecticut: Greenwood Press.

Cho, J., Boyle, M., Keum, H., Shevy, M., McLeod, D., Shah, D., et al. (2003) Media, terrorism, and emotional differences in media context and public reactions to the September 11th terrorist attacks. *Journal of Broadcasting & Electronic Media, 47,* 309-327.

Cohn, P., Kasen, S., Chen, H., Gordon, K., Berenson, K., Brook, J., et al. (2006). Current affairs and the public psyche: American anxiety in the post 9/11 world. *Social Psychiatry Epidemiology, 41,* 251-260.

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

Debrix, F. (2001) Cyberterror and media-induced fears: The production of emergency culture. *Strategies, 14,* 2001.

Dowland, P., Furell, S., Illingworth, H., & Reynolds, P. (1999). Computer crime and abuse: A survey of public attitudes and awareness. *Computers & Security, 18*, 715-726.

Erbschloe, I. (2005). *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*. Massachusetts: Elsevier Butterworth-Heinemann.

Embar-Seddon, A. (2002). Are we under siege? *American Behavioral Scientist, 45*, 1033-1043.

Enders, W., & Sandler, T. (1999) Transnational terrorism in the post-Cold War era. *International Studies Quarterly, 43*, 145-167.

Fetchenhauer, D., & Buunk, B. (2005) How to explain gender differences in fear of crime: Towards an evolutionary approach. *Sexuality, Evolution and Gender, 7*, 95-113.

Holman, A., & Silver, R. (2005) Future-oriented thinking and adjustment in a nationwide longitudinal study following the September 11th terrorist attacks. *Motivation and Emotion, 29*, 389-?.

Institute for Security Technology Studies at Dartmouth College. (2001). *Cyber Attacks During the War on Terrorism: A Predictive Analysis.* Hanover, Vermont: Vatis, M.

Jenkin, C. (2006). *Responses to terrorism scenarios: Event features, individual characteristics, and subjective evaluations* Unpublished doctoral dissertation, University of New Hampshire, 2006.

Katyal, N. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review, 149*, 1003-1115.

Knudsen, H., Roman, P., Johnson, J., & Ducharme, L. (2005) A changed American? The effects of September 11th on depressive symptoms and alcohol consumption. *Journal of Health and Social Behavior, 46*, 260-273.

Lewis, J. (2003) Cyber terror: Missing in action. *Knowledge, Technology, & Policy, 16*, 34-41.

Mirka, S., & Kivivuori, J. (2006) The relation between crime news and fear of violence. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 7*, 211-227.

Proceeding from Joint Economic Committee and Congress of the United States: *Wired World: Cyber Security and the U.S. Economy.* (2001). Washington D.C.: U.S. Government Printing Office.

Pyszczynski, T., Solomon, S., & Greenberg, J. (2003). *In the Wake of 9/11 The*

Psychology of Terror. Washington D.C.: American Psychological Association.

Sandywell, B. (2006). Monsters in cyberspace, cyberphobia and cultural panic in the information age. *Information, Communication & Society*, *9*, 39-61.

Silke, A. (Ed.). (2003). *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences*. New Jersey: John Wiley & Sons.

Smolej, M., & Kivivuori, J. (2006) The relation between crime news and fear of violence. *Journal of Scandinavian Studies in Criminology & Crime Prevention, 7*, 211-227.

Stein, B., Elliott, M., Jaycoxx, L., Collins, R., Berry, A., Klein, D., et al. (2004) A national longitudinal study of the psychological consequences of the September 11, 2001 terrorist attacks : reactions, impairment, and help-seeking. *Psychiatry*, *67*, 105-117.

Steuter, E. (1990) Understanding the media/terrorism relationship: An analysis of ideology and the news in Time Magazine. *Political Communication and Persuasion, 7,* 257-278.

The Library of Congress. (2005). *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (Order Code RL32114). Congressional Research Office: Library of Congress.

Vegh, S. (2002). Hacktivists or cyberterrorists? The changing media discourse on hacking. *First Monday*, *7*. Retrieved February 21, 2007, from http://www.firstmonday.org/.

Verton, D. (2003). *Black Ice: The Invisible Threat of Cyberterrorism*. California: McGraw-Hill Companies.

Weimann, G. (1990). 'Redefinition of image': the impact of mass-mediated terrorism. *International Journal of Public Opinion Research*, *2*, 16-29..

Weimann, G. (2005). Cyberterrorism: the sum of all fears? *Studies in Crime & Terrorism*, *28*, 129-149.

Whittaker, D. (2004). *Terrorists and Terrorism in the Contemporary World*. New York: Routledge.

Table 1

Test Order Means and Standard Deviations for Cyberterrorist Scenarios

Measures	Order 1	Order 2	Total
Cyberterrorist Scenarios			
Utility Center	81.01 (19.37)	84.10 (15.18)	82.63 (17.37)
911 Response	85.54 (16.84)	84.37 (18.00)	84.93 (17.44)
Hospital Records	86.27 (18.23)	89.59 (15.08)	88.00 (16.74)
Commercial District	78.46 (20.41)	79.00 (16.83)	78.74 (18.61)
Internet Switching Station	70.57 (19.96)	72.42 (18.41)	71.53 (19.17)

Table 2

Factor Analysis of Attitudes Toward Terrorism Scale

	ATTS Factors			
	GWTA	TWA	BCA	PWA
	Loadings			
I think that people I know are likely victims of contaminated mail.	**.766**	.143	.156	.011
I believed that I will be the victim terrorism using conventional weapons.	**.728**	.097	.186	.248
I believe that people know live in areas that are likely terrorist targets.	**.653**	.151	.067	.055
I think it likely that someone I know will be the victim of a nuclear or radioactive terrorist attack.	**.650**	.170	.166	.264
I think it likely that I will be the victim of a nuclear or radioactive terrorist attack.	**.586**	-.013	.175	.294
I believe that I am likely to be a victim of a terrorist attack.	**.566**	.062	.253	.337
I do worry about terrorism when I travel.*	.054	**.767**	.304	.078
I do think that what I travel I am at greater risk of terrorism.*	-.005	**.766**	.240	-.004
I think that my friends and family are at risk of terrorism when they travel.	.247	**.689**	.177	.322
I am afraid for people who fly across the country because of the threat of hijackings	.148	**.606**	.107	.422
I do worry about people I know being attacked by terrorists.	.203	**.537**	.483	.126
I worry about U.S. citizens becoming victims of biological terrorist attacks.	.328	**.516**	.148	.372
I think it likely that I will be exposed to a biological terrorist attack.*	.202	-.049	**.712**	.144
I always worry that my mail might be contaminated.*	.076	.198	**.689**	.020
I worry about becoming a victim of a chemical attack.*	.160	.198	**.683**	.188
I do worry that terrorists may release biological weapons in my area.*	.219	.301	**.625**	.318
I think that it is likely that I will be the victim of a chemical attack.*	.426	.069	**.570**	.266

Table 2 Continued

I do worry about in mail carriers becoming infected with anthrax.*	.286	.318	.488	.067
I am concerned that terrorist will attack using nuclear or radioactive weapons.*	.039	.279	.465	.156
I think it likely that a friend or relative will be a victim of a chemical attack.*	.439	.206	.441	.101
I have been kept awake at night worrying about being a part of the next big attack.	.066	.029	.119	**.751**
I am scared that terrorists may be planning an attack near my home.	.261	.138	.307	**.692**
I worry about being in an area where terrorists may use nuclear or radioactive weapons.	.315	.253	.323	**.593**
I am afraid of becoming a victim of a terrorist attack.	.281	.323	.198	**.574**
I worry about when and where the next big will take place.	.316	.456	.174	**.517**
I worry about people I know becoming victims of a chemical attack.	.388	.409	.256	**.511**
When I see a low flying plane I worry it might crash.	.158	.456	-.083	.478

Note: * Item reverse coded.

GWTA is general worry of terrorist attack; WBCA is worry of a biological or chemical attack; PWA is personal worry of a terrorist attack; TWA is travel worry of a terrorist attack.

Table 3

Zero Order correlations Between Fear of Terrorism Measures and Total Perceived Seriousness of Cyberterrorism

Variables	GWTA	TWA	WBCA	PWA	TSC
1. General Worry of Attack (GWTA)	-	.40*	.54*	.60*	.17*
2. Travel Worry of Attack (TWA)		-	.56*	.58*	.14*
3. Biological/ Chemical Worry of Attack (WBCA)			-	.59*	.18*
4. Personal Worry of Attack (PWA)				-	.18*
5. Total Perceived Seriousness of Cyberterrorism					-

Note: * $p < .01$

GWTA is general worry of terrorist attack; WBCA is worry of a biological or chemical attack; PWA is personal worry of a terrorist attack; TWA is travel worry of a terrorist attack; TSC is total perceived seriousness of cyberterrorism.

Table 4

Sex Fear Rating Means and Standard Deviations for Fear of Terrorism Measures

	Sex		
Variables	Men	Women	Total
Total Fear of Terrorism	46.33** (14.98)	54.06** (15.04)	51.59 (15.42)
General Worry of a Terrorist Attack	13.02 (5.80)	14.18 (5.28)	13.80 (5.47)
Travel Worry of a Terrorist Attack	17.04** (6.14)	20.33** (5.93)	19.28 (6.18)
Worry of a Biological or Chemical Attack	14.43* (6.16)	16.81* (6.15)	16.05 (6.24)
Personal Worry of an Attack	12.39 ** (5.19)	15.58** (6.04)	14.56 (5.96)

Note: ** $p < .001$, * $p < .01$

Table 5

Unstandardized and Standardized Coefficients for Standard Multiple Regression Predicting Knowledge of Cyberterrorism

Predictor Variables	b	β	*t*
Total Minutes News Watched	-.01	-.05	-.86
Total Minutes News Read	.02	.12	1.92
Total Minutes Internet News Read	.00	-.02	-.40
Frequency Watched Police Dramas	-.08	-.02	-.37
Frequency Watched Legal/ Forensic Drama	.10	.05	.82
Frequency Watched Legal/ Crime Reality	-.35	-.09	-1.49
Frequency Watched Political Commentary	.18	.06	.87

Table 6

Correlations Between Perceived Seriousness and Knowledge of Cyberterrorism and All Media Predictors

Measures	Utility	911	Hospital	District	Internet	Sex	TKC
Tot. Freq. TV Watched	-.01	-.02	-.03	.04	-.03	-.20**	-.02
Tot. Min. TV Watched	-.06	-.09	-.08	.04	-.08	-.23**	-.06
Tot. Freq. News Watched	-.03	-.05	-.05	.10	.00	-.14*	-.04
Tot. Min. New Watched	-.11*	-.11*	-.07	.05	-.05	-.14**	-.02
Tot. Freq. News Read	-.07	-.19**	-.15*	-.04	-.03	-.19**	.08
Tot. Min News Read	-.05	-.22**	-.15*	-.05	-.08	-.15**	.11
Tot. Freq. Internet News Read	.04	-.08	-.07	.02	.04	-.20**	.03
Tot. Min. Internet News Read	.00	-.12*	-.05	.00	-.06	-.26**	.01
Freq. Legal/ Forensic Drama	.01	.07	.00	.03	-.01	.15**	.03
Freq. Legal/ Crime Reality	.04	.00	-.03	.01	.01	-.14**	-.07
Freq. Police Drama	.06	.05	.02	.05	-.01	.08	-.03
Freq. Political Commentary	-.04	-.14*	-.18**	-.02	-.01	-.30**	-.04

Note: ** $p < .01$, *$p < .05$*

Utility is the utility center scenario; 911 is the 911 response scenario; Hospital is the hospital records scenario; District is the commercial district scenario; Internet is the Internet switching center scenario; TKC is total knowledge of cyberterrorism.

Table 7

Unstandardized and Standardized Coefficients for Standard Multiple Regressions Predicting Total Perceived Seriousness of Cyberterrorism From Fear of Terrorism

Measures	Scenario									
Predictors	Utility		911		Hospital		Comm.		Internet	
	b	β	b	β	b	β	b	β	b	β
GWTA	-.05	-.02	-.15	-.05	-.11	-.04	.50	.14	.17	.05
TWA	.18	.06	-.09	-.03	.16	.06	-.03	-.01	.16	.05
BCWA	.30	.11	.26	.09	-.04	-.01	.32	.10	.36	.11
PWA	.17	.06	.57*	.20*	.36	.13	.05	.02	.03	.01

Note: * $p < .05$

Hospital is the hospital records scenario; 911 is the 911 response scenario, Hospital is the hospital records scenario; Comm. is the commercial district scenario, Internet is the internet switching center scenario; GWTA is general worry of terrorist attack; WBCA is worry of a biological or chemical attack; PWA is personal worry of a terrorist attack; TWA is travel worry of a terrorist attack; TFT is total fear of terrorism.

Table 8

Correlations Between Fear of Terrorism Measures and Fear of Cyberterrorism

Measures	Fear of Terrorism Measures				
	GWTA	TWA	WBCA	PWA	TFT
Total Perceived Seriousness of Cyberterrorism	.17**	.14**	.18**	.18**	.23**
Scenarios					
Utility Center	.11	.14**	.17**	.14**	.19**
911 Response	.11	.10	.13*	.17**	.18**
Hospital Records	.07	.08	.05	.12*	.13*
Commercial District	.21**	.11	.18**	.15**	.20**
Internet Switching Center	.15**	.12*	.17**	.12*	.18**

Note: ** *p* < .01, **p* < .05*

GWTA is general worry of terrorist attack; WBCA is worry of a biological or chemical attack; PWA is personal worry of a terrorist attack; TWA is travel worry of a terrorist attack; TFT is total fear of terrorism.

Table 9

Unstandardized and Standardized Coefficients for Standard Multiple Regressions Predicting Total Perceived Seriousness of Cyberterrorism From Media Exposure

Variables	Sex					
	Men		Women		Both	
Predictors	b	β	b	β	b	β
Total Minutes of News Watched	-.03	-.23	.01	.11	.00	-.03
Total Minutes of News Read	.00	.02	-.04	-.19	-.02	-.12
Total Minutes of Internet News Read	.00	.03	.01	.08	.00	.00
Freq. of Legal Forensic Dramas Watched	-.03	-.01	.08	.04	.11	.04

Note: * $p < .05$

Table 10

Unstandardized and Standardized Coefficients for Standard Multiple Regressions Predicting Total Perceived Seriousness of Cyberterrorism From Media Exposure and Total Fear of Terrorism

Variables	Sex					
	Men		Women		Both	
Predictors	b	β	b	β	b	β
Total Minutes of News Watched	-.02	-.16	.01	.10	.00	.00
Total Minutes of News Read	.01	.05	-.04	-.17*	-.02	-.08
Total Minutes of Internet News Read	.00	-.01	.01	.09	.00	.00
Freq. of Legal Forensic Dramas Watched	-.33	-.06	.05	.01	-.01	.00
Total Fear of Terrorism	.21	.21	.19	.21*	.21	.23*

Note: * $p < .05$

Table 11

Men and Women Mean Seriousness Ratings and Standard Deviations for the Five Cyberterrorist Scenarios

Variables	Sex		
	Men	Women	Total
Scenarios			
Utility Center	78.39* (19.44)	84.46* (16.14)	82.42 (17.53)
911 Response	80.51* (19.99)	87.17* (15.77)	84.93 (17.56)
Hospital Records	82.97** (20.06)	90.34** (14.52)	87.86 (16.92)
Commercial Center	79.41 (18.73)	78.34 (18.45)	78.72 (18.53)
Internet Switching Center	72.20 (19.96)	71.29 (18.69)	71.60 (19.10)

Note: ** $p < .001$, * $p < .01$

Table 12

Unstandardized and Standardized Coefficients for Standard Multiple Regression Predicting Fear of Terrorism for Men and Women

Variables	Sex			
	Men		Women	
Predictors	b	β	b	β
Total Minutes of News Watched	-.02	-.11	.03*	.18*
Total Minutes of News Read	.00	-.01	-.04*	-.17*
Total Minutes of Internet News Read	.01	.11	-.01	-.07
Freq. of Legal Forensic Dramas Watched	.90	.16	.92*	.17*
Total Knowledge of Cyberterrorism	.09	.06	-.30*	-.18*

Note: * $p < .05$

Table 13

Correlations Between Fear of Terrorism Measures and All Predictions

	Fear of Terrorism Measures				
Media Measures	GWTA	TWA	WBCA	PWA	TFT
Tot. Freq. TV Watched	.03	.01	.03	-.04	.01
Tot. Min. TV Watched	-.07	-.05	-.06	-.11	-.09
Tot. Freq. News Watched	.20**	.06	.08	.10	.12*
Tot. Min. New Watched	.12*	.01	.07	.09	.07
Tot. Freq. News Read	.01	-.15**	-.06	-.08	-.11
Tot. Min News Read	-.02	-.19**	-.09	-.09	-.14*
Tot. Freq. Internet News Read	.04	-.12*	-.09	-.07	-.09
Tot. Min. Internet News Read	.02	-.11*	-.11*	-.11	-.10
Freq. Legal/ Forensic Dramas	.07	.05	.08	.11*	.18**
Freq. Legal/ Crime Reality	.05	.04	.11*	.09	.10
Freq. Police Drama	.13*	.03	.20**	.15**	.16**
Freq. Political Commentary	.00	-.13*	-.06	-.11*	-.10*
Knowledge of Cyberterrorism					
Total Knowledge of Cyberterrorism	-.08	-.08	-.10	-.06	-.10

Note: ** *p* < .01, **p* < .05*

GWTA is general worry of a terrorist attack; WBCA is worry of a chemical or biological attack; PWA is personal worry of an attack; TWA is travel worry of attack; TFT is total fear of terrorism.

Table 14

Unstandardized and Standardized Coefficients for Standard Multiple Regression Predicting Fear of Terrorism

Predictor Variables	b	β	*t*
Sex	6.64	.20	3.10**
Total Minutes News Watched	.01	.09	1.47
Total Minutes News Read	-.03	-.14	-2.10*
Total Minutes Internet News Read	.00	-.01	-.17
Freq. Legal/ Forensic Drama Watched	.54	.10	1.31
Freq. Legal/ Crime Drama Watched	.30	.05	.76
Freq. Police Drama Watched	.35	.06	.88
Freq. Political Commentary Drama Watched	.03	.01	.08
Total Knowledge of Cyberterrorism	-.12	-.08	-1.46

Note: ** $p < .01$, * $p < .05$

APPENDICES

APPENDIX A

IRB APPROVAL LETTER

University *of* New Hampshire

Research Conduct and Compliance Services, Office of Sponsored Research
Service Building, 51 College Road, Durham, NH 03824-3585
Fax: 603-862-3564

22-May-2007

VanHoogenstyn, Andrew
Psychology
8747 GSS (MUB)
PO Box 2217
Windham, ME 04062

IRB #: 4001
Study: Knowledge and Perceptions of Cyberterrorism
Approval Date: 21-May-2007

The Institutional Review Board for the Protection of Human Subjects in Research (IRB) has reviewed and approved the protocol for your study as Exempt as described in Title 45, Code of Federal Regulations (CFR), Part 46, Subsection 101(b). Approval is granted to conduct your study as described in your protocol.

Researchers who conduct studies involving human subjects have responsibilities as outlined in the attached document, *Responsibilities of Directors of Research Studies Involving Human Subjects.* (This document is also available at http://www.unh.edu/osr/compliance/irb.html.) Please read this document carefully before commencing your work involving human subjects.

Upon completion of your study, please complete the enclosed pink Exempt Study Final Report form and return it to this office along with a report of your findings.

If you have questions or concerns about your study or this approval, please feel free to contact me at 603-862-2003 or Julie.simpson@unh.edu. Please refer to the IRB # above in all correspondence related to this study. The IRB wishes you success with your research.

For the IRB,

Julie F Simpson

Julie F. Simpson
Manager

cc: File
Cohn, Ellen

APPENDIX B

CYBERTERRORIST SCENARIOS

Scenario Name	Description
Utility Centers	Terrorists use computers to illegally access natural gas utility control centers. Using computer viruses and worms, terrorists inject false commands, closing valves resulting in an explosion which destroys the utility centers.
911 Response	Terrorists use computers to spread a worm (computer virus) that infects every unprotected cell phone causing them to all dial 911 simultaneously jamming all incoming calls.
Hospital Records	Terrorists use computers to illegally access and alter hospital patient records online. As a result patients within the region receive incorrect medical treatment and blood transfusions.
Commercial District	Terrorists detonate an electromagnetic pulse bomb, damaging all electric circuitry (including computers and other electric circuit devices) in a commercial district.
Internet Switching Center	Terrorists drive a dynamite rigged fuel truck into a critical Internet switching center destroying it. The center was used by major Internet service providers to share data across networks. The center accounts for as much as 40% of Internet traffic.

APPENDIX C

KNOWLEDGE AND PERCEPTIONS OF CYBERTERRORISM SURVEY ORDER 1

First, we would like you to tell us a little about your background. For each question below, please **circle** or **fill in** the answer that is correct.

1. What class year are you?

   1. Freshmen
   2. Sophomore
   3. Junior
   4. Senior
   5. Graduate Student

2. What is your sex?

   1. Male
   2. Female

3. How old are you?

_______________ years old
(Please fill in)

4. What is your religion?
   1. Agnostic
   2. Atheist
   3. Buddhist
   4. Catholic
   5. Christian
   6. Greek Orthodox
   7. Jewish
   8. Protestant
   9. Muslim
   10. Hindu
   11. Other _______________________

(If "other," please fill in)

5. What is your main racial background?

   1. African American
   2. Native American (Indian)
   3. Asian American
   4. Caucasian (White)
   5. Hispanic American
   6. Other ________________________

6. What is your field of study?

   1. Social Sciences (Psychology, Sociology, etc.)
   2. Sciences (Biology, chemistry, etc.)
   3. English
   4. History
   5. Engineering
   6. Math/ Physics
   7. Business
   8. Computer Science
   9. Other ____________________

7. What is your approximate cumulative GPA.

   1. 4.00
   2. 3.99-3.50
   3. 3.49-3.00
   4. 2.99-2.50
   5. 2.49-2.00
   6. 1.99-1.50
   7. 1.49-1.00
   8. below 1.00

8. What is your political affiliation?

   1. Republican
   2. Democrat
   3. Independent
   4. Other

Below are a series of questions about your exposure to different media sources. Please answer to the best of your knowledge. For each item circle one answer only.

1. Please indicate the **frequency with which you watch television each day.** Use the following scale: (1) I never watch TV on that day to (5) I always watch TV on that day.

	Never				Always
Monday	1	2	3	4	5
Tuesday	1	2	3	4	5
Wednesday	1	2	3	4	5
Thursday	1	2	3	4	5
Friday	1	2	3	4	5
Saturday	1	2	3	4	5
Sunday	1	2	3	4	5

2. Please estimate how **many minutes a day** you **watch television** on each of the following days.

Minutes

Monday ______

Tuesday ______

Wednesday ______

Thursday ______

Friday ______

Saturday ______

Sunday ______

3. When **you do watch television**, how often do you watch the **following types of television programs** using the following scale: (1) I never watch that type of program to (10) I watch that type of program every chance I get.

	Never								Every Chance	
Legal/Forensic Dramas (e.g. Bones, CSI, NCSI, CSI: Miami, CSI:NY, Criminal Intent)	1	2	3	4	5	6	7	8	9	10
Legal/Crime Reality Shows (e.g. COPS, 911, Judge Judy, Court TV)	1	2	3	4	5	6	7	8	9	10
Police Dramas (e.g. NYPD Blue, The Shield, Without a Trace, Cold Case, Closer)	1	2	3	4	5	6	7	8	9	10
Political Commentary (e.g. Daily Report, Colbert Report)	1	2	3	4	5	6	7	8	9	10

1. Please indicate the **frequency** with which **you watch national news (e.g. Foxnews, CNN, Nightly News) or local broadcast news.** Use the following scale: (1) I never watch national news on that day to (5) I always watch national news on that day.

	Never				Always
Monday	1	2	3	4	5
Tuesday	1	2	3	4	5
Wednesday	1	2	3	4	5
Thursday	1	2	3	4	5
Friday	1	2	3	4	5
Saturday	1	2	3	4	5
Sunday	1	2	3	4	5

2. Please estimate **how many minutes a day** you watch **national news (e.g. Foxnews, CNN, Nightly News) or local broadcast news** on the following days.

Minutes

Monday ______

Tuesday ______

Wednesday ______

Thursday ______

Friday ______

Saturday ______

Sunday ______

1. Please indicate the frequency with which **you read a national newspaper (e.g. USA Today, NY Times, Wall Street Journal) or local newspaper (e.g. TNH, Foster Daily Democrat)**. Use the following scale: (1) I never read national/ local newspapers on that day to (5) I always read national/ local newspapers on that day.

	Never				Always
Monday	1	2	3	4	5
Tuesday	1	2	3	4	5
Wednesday	1	2	3	4	5
Thursday	1	2	3	4	5
Friday	1	2	3	4	5
Saturday	1	2	3	4	5
Sunday	1	2	3	4	5

2. Please estimate how many minutes a day **you read a national newspaper (e.g. USA Today, NY Times, Wall Street Journal) or local newspaper (e.g. TNH, Foster Daily Democrat)** on the following days.

Minutes

Monday ______

Tuesday ______

Wednesday ______

Thursday ______

Friday ______

Saturday ______

Sunday ______

1. Please indicate the **frequency** with which **you read news articles on the Internet or get your news from websites (e.g. cnn.com)**. Use the following scale: (1) I never read news articles on the Internet or get my news from websites on that day to (5) I always read news articles on the Internet or get my news from websites on that day.

	Never				Always
Monday	1	2	3	4	5
Tuesday	1	2	3	4	5
Wednesday	1	2	3	4	5
Thursday	1	2	3	4	5
Friday	1	2	3	4	5
Saturday	1	2	3	4	5
Sunday	1	2	3	4	5

2. Please estimate **how many minutes a day you read news articles on the Internet, or get your news from websites (e.g. cnn.com)**. on the following days.

Minutes

Monday ______

Tuesday ______

Wednesday ______

Thursday ______

Friday ______

Saturday ______

Sunday ______

How many hours a week do you spend on the Internet? ___________________

Below are a series of questions about your Internet use. Please answer the questions according the following scale, for each activity circle one answer only:

How often do you engage in the following activity?

Never	Rarely	Sometimes	Often	Very Often
0	1	2	3	4

How often do you engage in the following activities?

Activity	Never	Rarely	Sometimes	Often	Very Often
1. E-mail	0	1	2	3	4
2. Chat	0	1	2	3	4
3. Newsgroups	0	1	2	3	4
4. Online Games	0	1	2	3	4
5. Sex Sites	0	1	2	3	4
6. Shopping	0	1	2	3	4
7. Download/ Listening to Mus	0	1	2	3	4

How often do you engage in the following activities?

Activity	Never	Rarely	Sometimes	Often	Very Often
1. Search the library website fo references.	0	1	2	3	4
2. Contact University Staff via e-mail for information.	0	1	2	3	4
3. Contact external experts via e-mail for information.	0	1	2	3	4
4. Download relevant material from course web pages	0	1	2	3	4
5. Use the World Wide Web fo searching relevant material	0	1	2	3	4
6. Post questions to newsgroup and message boards.	0	1	2	3	4

Please indicate if the following statements are True or False to the best of your ability.

	True	False
1. ...Cyberterrorist attacks frequently occur.	T	F
2. ...The use of computers by terrorist organizations to recruit members is not considered cyberterrorism.	T	F
3. ...The use of computers by terrorist organizations to raise funds for future campaigns is not considered cyberterrorism.	T	F
4. ...The use of computers by terrorist organizations to spread propaganda is considered cyberterrorism.	T	F
5. ...The use of computers by terrorist organizations to communicate plans for future attacks to other terrorist groups is considered cyberterrorism.	T	F
6. ...Any attempt to access secure Internet sites without authorization (or permission) is not considered cyberterrorism.	T	F
7. ...Any attempt to access secure Internet sites without authorization (or permission) to destroy information without permission is considered cyberterrorism.	T	F
8. ...Politically motivated hackers (individuals that gain access to secure Internet sites without permission) are considered cyberterrorists.	T	F
9. ...The privates sector (includes power grids, water supply, natural gas, and communications networks) are not vulnerable to a cyberterrorist attack.	T	F
10. ...The use of steganography (or hidden messages in emails or pictures), to communicate future terrorist attacks while avoiding the detection of the authorities is not an act of cyberterrorism.	T	F
11. ...Terrorists do not yet have the human capital (personnel) to carry out a cyberterrorist attack.	T	F
12. ...Terrorists currently do not have the resources (money & equipment) to carry out a cyberterrorist attack.	T	F
13. ...The U.S. infrastructure (gas, water, electric, communication networks, government security agencies, & military) is vulnerable to cyberterrorist attacks.	T	F
14. ...Web defacements (or the unauthorized altering of a website without the knowledge of the creator) are considered an act of cyberterrorism.	T	F
15. ...The word 'cyberterrorism' has been clearly defined.	T	F
16. ...Attacks by terrorist organizations conducted without the use of a computer could be considered cyberterrorism.	T	F
17. ...The physical destruction of computers by terrorist organizations resulting in disruption of the infrastructure (gas, water, electric, communication networks, government security agencies, & military) is not cyberterrorism.	T	F

18. ...Attacks by terrorists using computers must result in bodily injury, death or significant destruction or disruption to be considered a cyberterrorist attack.	T	F
19. ...Cyberterrorist attacks can include both a conventional attack and a computer attack.	T	F
20. ...Cyberterrorist attacks have been used by state-sponsored terrorists against the United States.	T	F

Please indicate the extent to which you agree with each statement using the following scale, for each question circle one answer only:

1 Completely Disagree	2 Somewhat Disagree	3 Slightly Disagree	4 Slightly Agree	5 Somewhat Agree	6 Completely Agree

Statement						
1. ... I have been kept awake at night worrying about being a part of the next big attack.	1	2	3	4	5	6
2. ... I am not concerned that terrorists will attack using nuclear or radioactive weapons.	1	2	3	4	5	6
3. ... I am scared that terrorists may be planning an attack near my home.	1	2	3	4	5	6
4. ... I don't worry about becoming a victim of a chemical attack.	1	2	3	4	5	6
5. ... I am afraid of becoming a victim of a terrorist attack.	1	2	3	4	5	6
6. ... I never worry that my mail might be contaminated.	1	2	3	4	5	6
7. ... I worry about being in an area where terrorists may use nuclear or radioactive weapons.	1	2	3	4	5	6
8. ... I don't worry that terrorists may release biological weapons in my area.	1	2	3	4	5	6
9. ... I do not think that when I travel I am at greater risk of terrorism.	1	2	3	4	5	6
10. ... I don't worry about terrorism when I travel.	1	2	3	4	5	6
11. ... When I see a low-flying plane, I worry that it might crash.	1	2	3	4	5	6
12. ... I don't worry about people I know being attacked by terrorists.	1	2	3	4	5	6
13. ... I am afraid for people who fly across the country because of the threat of hijacking.	1	2	3	4	5	6
14. ... I worry about U.S. citizens becoming victims of biological terrorist attacks.	1	2	3	4	5	6
15. ... I don't worry about the mail carriers becoming infected with anthrax.	1	2	3	4	5	6
16. ... I worry about when and where the next big attack will take place.	1	2	3	4	5	6
17. ... I worry about people I know becoming victims of a chemical attack.	1	2	3	4	5	6
18. ... I think that it is unlikely that I will be the victim of a chemical attack.	1	2	3	4	5	6
19. ... I think it likely that I will be the victim of a nuclear or radioactive terrorist attack.	1	2	3	4	5	6

20. … I believe that I am likely to be a victim of a terrorist attack.						
21. … I think it unlikely that I will be exposed to a biological terrorist attack.	1	2	3	4	5	6
22. … I believe that I will be the victim of terrorism using conventional weapons.	1	2	3	4	5	6
23. … I think that people I know are likely victims of contaminated mail.	1	2	3	4	5	6
24. … I believe that people I know live in areas that are likely terrorist targets.	1	2	3	4	5	6

25. … I think it unlikely that a friend or relative will be a victim of a chemical attack.	1	2	3	4	5	6
26. … I think that my friends and family are at risk of terrorism when they travel.	1	2	3	4	5	6
27. … I think it likely that someone I know will be the victim of a nuclear or radioactive terrorist attack.	1	2	3	4	5	6

Please indicate if you have engaged in any of the following behaviors. For each answer circle yes or no.

Behavior		
28. … I have taken action to reduce my risk of becoming a victim of terrorism.	Yes	No
29. … I fly less because of terrorist hijackings.	Yes	No
30. … I have a terrorist emergency supply kit.	Yes	No
31. … I have a plan in place in case of terrorist attack.	Yes	No
32. … I have discussed my personal risk of terrorism with a friend or family member.	Yes	No
33. … I have encouraged others to take steps to stay safe from terrorism.	Yes	No

Please read the following scenarios and determine how serious each event would be. Please rate each scenario according to the following scale, for each question circle one answer only:

Not Serious										**Very Serious**
0	10	20	30	40	50	60	70	80	90	100

<table>
<tr><td colspan="11">Terrorists use computers to illegally access natural gas utility control centers. Using computer viruses and worms, terrorists inject false commands, closing valves resulting in an explosion which destroys the utility centers.</td></tr>
<tr><td>Not Serious</td><td colspan="9">How Serious is the above scenario? Circle one:</td><td>Very Serious</td></tr>
<tr><td>0</td><td>10</td><td>20</td><td>30</td><td>40</td><td>50</td><td>60</td><td>70</td><td>80</td><td>90</td><td>100</td></tr>
</table>

<table>
<tr><td colspan="11">Terrorists use computers to spread a worm (computer virus) that infects every unprotected cell phone causing them to all dial 911 simultaneously jamming all incoming calls.</td></tr>
<tr><td>Not Serious</td><td colspan="9">How Serious is the above scenario? Circle one:</td><td>Very Serious</td></tr>
<tr><td>0</td><td>10</td><td>20</td><td>30</td><td>40</td><td>50</td><td>60</td><td>70</td><td>80</td><td>90</td><td>100</td></tr>
</table>

<table>
<tr><td colspan="11">Terrorists use computers to illegally access and alter hospital patient records online. As a result patients within the region receive incorrect medical treatment and blood transfusions.</td></tr>
<tr><td>Not Serious</td><td colspan="9">How Serious is the above scenario? Circle one:</td><td>Very Serious</td></tr>
<tr><td>0</td><td>10</td><td>20</td><td>30</td><td>40</td><td>50</td><td>60</td><td>70</td><td>80</td><td>90</td><td>100</td></tr>
</table>

<table>
<tr><td colspan="11">Terrorists detonate an electromagnetic pulse bomb, damaging all electric circuitry (including computers and other electric circuit devices) in a commercial district.</td></tr>
<tr><td>Not Serious</td><td colspan="9">How Serious is the above scenario? Circle one:</td><td>Very Serious</td></tr>
<tr><td>0</td><td>10</td><td>20</td><td>30</td><td>40</td><td>50</td><td>60</td><td>70</td><td>80</td><td>90</td><td>100</td></tr>
</table>

<table>
<tr><td colspan="11">Terrorists drive a dynamite rigged fuel truck into a critical Internet switching center destroying it. The center was used by major Internet service providers to share data across networks. The center accounts for as much as 40% of Internet traffic.</td></tr>
<tr><td>Not Serious</td><td colspan="9">How Serious is the above scenario? Circle one:</td><td>Very Serious</td></tr>
<tr><td>0</td><td>10</td><td>20</td><td>30</td><td>40</td><td>50</td><td>60</td><td>70</td><td>80</td><td>90</td><td>100</td></tr>
</table>

Now without looking back please list three targets and three methods that were used in the previous five scenarios.

Targets:

1 ______________________________

2 ______________________________

3 ______________________________

Methods:

1 ______________________________

2 ______________________________

3 ______________________________