UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

CYBERTERRORISM: A POSTMODERN VIEW OF NETWORKS OF TERROR AND HOW COMPUTER SECURITY EXPERTS AND LAW ENFORCEMENT OFFICIALS FIGHT THEM

A Dissertation

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

degree of

Doctor of Philosophy

By

JONATHAN A. MATUSITZ
Norman, Oklahoma
2006

UMI Number: 3207541

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

CYBERTERRORISM: A POSTMODERN VIEW OF NETWORKS
OF TERROR AND HOW COMPUTER SECURITY EXPERTS
AND LAW ENFORCEMENT OFFICIALS FIGHT THEM

A Dissertation APPROVED FOR THE
DEPARTMENT OF COMMUNICATION

BY

_____
Dr. Eric M. Kramer

_____
Dr. H. Dan O'Hair

_____
Dr. Todd L. Sandel

_____
Dr. Patrick C. Meirick

_____
Dr. Edward J. Perkins

ACKNOWLEDGEMENTS

First and foremost, I dedicate this product of months of academic work to my doctoral advisor, Dr. Eric Kramer. Without his wisdom, direction, and valuable pieces of advice, this dissertation would not have been what it is today. Dr. Kramer has greatly exceeded the role of advisor in my four years of doctoral experience. This is what an ambitious graduate student needs. Equally supportive is my mother, Anne Matusitz. Her emotional assistance has contributed to the success of my life. Her fortitude, serenity, and attentiveness have made me a much stronger individual.

I would like to thank Dr. Jin Brown and Dr. Pamela McWherter, both of whom teach at the University of Alaska Fairbanks. Dr. Brown was my advisor and Dr. McWherter was one of my major professors. They truly made me the qualitative scholar that I have become today. I am very thankful to Dr. Dan O'Hair for his support, thoughtful recommendations, and humor. I also express gratitude to Dr. Sandel for giving me suggestions on how to improve the quality of the data analysis in this doctoral dissertation. In addition, Dr. Meirick and Dr. Perkins, I thank you for your patience and for reading this long dissertation.

Finally, I am grateful to those fellow graduate students in the Department of Communication at the University of Oklahoma who have strongly supported me. I want to thank you, too, Gerald-Mark Breen, for your faith in me and your encouragement to "not let completed papers sleep on my computer, but to send them off to peer-reviewed journals." And it works. Now, I keep the pipeline running.

Thank you all.

TABLE OF CONTENTS

ABSTRACT

The purpose of this study is to investigate how cyberterrorists create networks in order to engage in malicious activities against the Internet and computers. The purpose of the study is also to understand how computer security labs (i.e., in universities) and various agencies (that is, law enforcement agencies such as police departments and the FBI) create joint networks in their fight against cyberterrorists. This idea of analyzing the social networks of two opposing sides rests on the premise that it takes networks to fight networks. The ultimate goal is to show that, because of the postmodern nature of the Internet, the fight between networks of cyberterrorists and networks of computer security experts (and law enforcement officials) is a postmodern fight. Two theories are used in this study: social network theory and game theory.

This study employed qualitative methodology and data were collected via in-depth conversational (face-to-face) interviewing. Twenty-seven computer security experts and law enforcement officials were interviewed. Overall, this study found that cyberterrorists tend not to work alone. Rather, they team up with others through social networks. It was also found that it takes networks to fight networks. As such, it is necessary for experts and officials to combine efforts, through networking, in order to combat, let alone understand, cyberterrorist networks. Of equal relevance is the fact that law enforcement agents and computer security experts do not always engage in battle with cyberterrorists. They sometimes try to interact with them in order to obtain more information about their networks (and vice versa). Finally, four themes were identified from the participants' accounts: (1) postmodern state of chaos, (2) social engineering, (3) know thy enemy, and (4) the enemy of my enemy is my friend.

CYBERTERRORISM: A POSTMODERN VIEW OF NETWORKS OF TERROR AND HOW COMPUTER SECURITY EXPERTS AND LAW ENFORCEMENT OFFICIALS FIGHT THEM

Chapter I

Introduction

The year 2006 has seen the release of a blockbuster, *Firewall*, starring Harrison Ford. This is the story of a computer security specialist whose job is to protect a Seattle bank's financial holdings from the relentless threat of cyberterrorists and sophisticated Internet hackers. In this movie, Harrison Ford uses a complex network of tracers, access codes, and firewalls (Diones, 2006). What this also means is that pop culture no longer celebrates cyberterrorism as generally innocuous. Television and print journalists have been portraying cyberterrorism as a realistic threat to computers and the Internet (Krapp, 2005). Indeed, as our lives rely heavily on the Internet, the attempt for cyberterrorists to spread terror is easy as the Internet is one of their means to wreak havoc. Government agencies, banks, universities, and many goods and service providers today use the Internet as their integral way to conduct daily operations (Lye & Wing, 2005). Not only is it very easy to connect to the Internet; the Internet has also brought revolutionary changes to humanity. One of these greatest changes has been the ever-expanding connectivity worldwide. In many respects, this has been a bonus for human communication (Dunnigan, 2003). Now, the expansion of communication and the transfer of knowledge throughout the world occur at a rate never achieved before (Matusitz, 2005a). However, there also has been a sinister side to this achievement. Individuals or groups can take advantage of the ease, flexibility, and anonymity afforded

by cyberspace to threaten citizens, specific groups, organizations, communities and entire countries (Clem, Galwankar, & Buck, 2003). This threat is represented through the rapid spread of computer viruses, worms, Trojan horses, and other malicious software programs to cripple entire network systems. As humans become more dependent on the plethora of opportunities available on the Internet, the potential exists for much more devastating consequences of this "sinister side" of the Internet; the biggest of these consequences may come from cyberterrorism (Clem, Galwankar, & Buck, 2003).

Broadly defined, cyberterrorism is the use of new communication technologies to attack computer systems (Dunnigan, 2003). Cyberterrorism is a real threat and it is growing. It could be a destructive weapon of mass destruction and could harm the American economy in the process (McConnell, 2004). The reason is that the number of cyber attackers with the tools and resources to use computers against the United States is rising. The United States is the biggest target for cyberterrorists. As a result, large-scale computer attacks on the U.S. critical infrastructure and economy would be devastating (Kouri, 2005). A report by the General Accounting Office, an internal government watchdog, found soft spots in the computer network that could allow cyberterrorists to severely disrupt national defense or critical public operations or steal sensitive data (Williams, 2001). In fact, by eliminating certain data networks, cyberterrorists could cripple everything from telecommunications and power grids to hospitals and banking (Cha, 2001). The same cyberterrorists frequently attempt to break into corporate computers or contaminate a satellite with viruses that could dismantle it or change its orbit (Stone, 2001). According to Clem, Galwankar, and Buck (2003),

> in the near future, it may be possible to harness the connectivity of the Internet to disable certain key computer systems and cause similar amounts of damage at much less risk to the attacker. For example, if a group wanted to disable an emergency medical services (EMS) dispatch center, it would be easier and less risky for the attacker to destroy it with explosives or to disable its computer systems with a computer virus (p. 272).

In line with these contentions, cyber attacks against vital services, such as water and electrical supply systems, are another major area of concern. Hospitals and their surroundings heavily rely on water and can subsist for very limited periods without water (Clem, Galwankar, & Buck, 2003). Although most American hospitals have back-up generators that run when electrical supply systems fail, communities still remain highly vulnerable. By the same token, the longer a community remains without power, the more likely the people will suffer food and medication spoilage because of a loss of refrigeration and because of deaths due to medical equipment failure (Clem, Galwankar, & Buck, 2003).

A very perilous attack that cyberterrorists could launch would be one against the Internet. The Internet is a mushrooming network that consists of billions of nodes and is burgeoning at a rapid rate. It includes private-home users, businesses of all sizes, universities, as well as federal, state, and local government agencies. Cyberterrorists can take advantage of a technique already perfected by hackers called a distributed denial of service (DOS) attack. DOS would contribute to the country's increasing vulnerability as the American critical infrastructures become ever more reliant on the Internet (Kouri, 2005). Paul Virilio (2000) already evoked the alarming likelihood of the collapse of the

Internet caused by a major technological "event" through DOS attacks, but also cyber attacks, worms, and computer viruses.

Of equal concern is the fact that cyberterrorists also network among each other; they form networked enterprises for malicious activities against the computer world (Kouri, 2005). They use the Internet to communicate with each other and, among the many Internet sites where they can convene, the chat room is the one they use the most (Zepp, 1999). For cyberterrorists, a chat room is like a hub in the network; it is a central location on the Internet that has a large number of highly connected nodes. Cyberterrorists work in an "all-channel" type of network (Bavelas, 1950; Leavitt, 1951), that is, a network where all dispersed nodes can be interlinked for simultaneous dissemination of information and instant coordination (Barabasi, 2002). As a network of terror, a cyberterrorist network is of the postmodern type[1], where no leadership is needed, where no leader exists, where no center exists, and where communication is even more flexible than one can ever imagine (Matusitz & O'Hair, in press).

Fortunately, cybersecurity, an area of information technology and law enforcement, has flourished tremendously for the past couple of years (Moore, 2005). In response to cyberterrorism, and faced with the fear that networks of terror may become endless because of the ubiquity and flexibility of the Internet, federal government agencies, industries, and other organizations have applied a variety of security measures (Clem, Galwankar, & Buck, 2003). One of these security measures is the development of social networks of cyber defense. It is common knowledge that federal agencies have top-secret networks (Webb, 2001); on a daily basis, they strive to ward off acts of

[1] The idea that cyberterrorist networks are postmodern was suggested by Dr. Eric Kramer, my advisor, during the multitude of conversations that I had with him.

cyberterrorism through these top-secret networks (Webb, 2001). For instance, the Federal Bureau of Investigation has created a Cyber Division to manage and direct a program that identifies cyber threats (Kouri, 2005). The FBI frequently networks with computer security experts (and vice versa) who have highly specialized computer-based skills (Kouri, 2005). Some of these computer security experts are instructors, and even undergraduate students, working in university cyber forensics labs.

Cyberterrorism is a serious issue that pertains to us all. It must be carefully studied in order to understand how its networks can be effectively countered by networks of computer security experts and law enforcement officials. The ability to identify cyber attackers is now enabled from highly sophisticated specialists (Dunnigan, 2003). Computer security has become one of the main pillars for survival to organizations such as businesses, banks, and governments (Clem, Galwankar, & Buck, 2003). For this reason, it proves very important to not only study what cyberterrorists can do to a computer or Internet system, but, above all, to investigate how networks of cyberterrorists operate and how cyber forensics teams and various law enforcement agencies create networks with each other in order to combat networks of terror.

Purpose of Study

This is a study about a growing communication phenomenon: social networks. In doing so, I explored the subfields of organizational communication and new communication technology. The purpose of this study is to investigate how cyberterrorists create networks in order to engage in malicious activities against the Internet and computers. The purpose of my study is also to understand how computer security labs (i.e., in universities) and various agencies (that is, law enforcement agencies

such as police departments and the Federal Bureau of Investigation) create joint networks in their fight against cyberterrorists. This idea of analyzing the social networks of two opposing sides rests on the premise that it takes networks to fight networks (Arquilla & Rondfelt, 2001). The ultimate goal is to show that, because of the postmodern nature of the Internet, the fight between networks of cyberterrorists and networks of computer security experts (and law enforcement officials) is a postmodern fight.

Although I touched on technical aspects such as firewalls and anti-virus software programs, the heart of this study pertains to the social aspect of the networks of the two opposing sides mentioned above. The goal is to see how they network, what types of communication patterns they use, why they need to network, and so on. I focused my research on computer technology labs at five universities – the University of Oklahoma, Purdue University, the University of North Texas, the University of Central Florida, and the University of Tulsa – because these labs have computer experts who have created cyber forensics teams that network with law enforcement agencies in their fight against cyberterrorists. I also focused my research on law enforcement agencies. It is important to know that many police departments today have computer security experts who are trained to identify cyberterrorists. For the past couple of years, federal agencies such as the Federal Bureau of Investigation have created cybersecurity teams working collaboratively with university cyber forensics labs and other organizations (McGinn, Raymond, & Joseph, 2002).

Research Questions

The participants were computer security experts and law enforcement officials. Among law enforcement officials were local police officers, members of the FBI, the

CIA, the National White Collar Crime Center, and other important organizations. Computer (or cyber) forensics experts work, for the most part, in universities. Twenty-seven participants (n=27) in total were selected. Twenty-seven participants might seem to be an insufficient number for such a long study, but the participants were all primary sources. Participants in this field of study are uncommon and difficult to convince to participate in a major study. Many of them said that they had never been interviewed before. As such, the data in this study are primary. The reason all those participants were selected lies in the fact that they have adequate knowledge and expertise to enlighten me, through their direct experiences with both computer security and cyberterrorist incidents, on all the various topics that pertain to my research questions. These computer experts have created cyber forensics teams that network with law enforcement agencies in their fight against cyberterrorists. They have a very good idea of how networks of cyberterrorists work. For all these reasons, they are ideal participants in my study. There is a very detailed section of the methods section in Chapter 3. Below are the following questions to guide my research.

RQ1: What do computer security experts' and law enforcement officials' accounts reveal about networks of cyberterrorists?

RQ2: What do computer security experts' and law enforcement officials' accounts reveal about their own networks?

RQ3: How can the conflict and interaction between cyberterrorists and computer security experts (and law enforcement officials) be explained through the use of both social network theory and game theory?

RQ4: What are the themes that emerged across the participants' accounts?

In order to answer **RQ1** and **RQ2**, I analyzed the accounts – based on social network theory – provided by the participants through their answers to all the interview questions (as well as the possible probing questions). In order to answer **RQ3**, I analyzed the data from both the social network theory and game theory perspectives. The arrangement for this interpretation of data was structured in three different parts. Each was independent from one another. The first part was exclusively a social network theory approach; the second part was exclusively a game theory approach; and the third part was an intersection of the two approaches. As the point is made at the end of the literature review in this dissertation, the intersection of the two theories is appropriate to the novel characteristics of the Internet. Finally, in order to answer **RQ4**, I looked for common themes that emerged across the participants' accounts. The list of interview questions is to be found in the interview protocol (see Appendix B on the last two pages of this dissertation).

Methodological Approach

The research employed qualitative methodology and data were collected via in-depth conversational (face-to-face) interviewing. One of the reasons the methodology was qualitative lies in the fact that a certain number of the participants were highly secure people who refused to fill out surveys. According to them, one of the conditions to answer my questions was to see the researcher face to face. In fact, before I interviewed an FBI agent in the Southwest, I had to go through a scanner and a metal detector. I was not allowed to bring a tape-recorder either. I had to take notes for hours. This process had to be repeated for a couple of other participants as well. The method of in-depth conversational (face-to-face) interviewing followed the procedures described by Kvale

(1996). Kvale (1996) calls for seven stages in the interview process: *thematizing*, *designing*, *interviewing*, *transcribing*, *analyzing*, *verifying*, and *reporting*. Analysis of the accounts is an omnipresent process throughout the research. While the qualitative researcher needs to know how to assess qualitative interview findings, it is also important that he or she understands that methods of improving research validity must be taken into account. An explanation of why the qualitative interviewing method is suitable for this study is given at the end of the methods chapter (Chapter III).

Social Network Theory and Game Theory

We already know that this study uses two theoretical approaches in the analysis of networks of cyberterrorists as well as networks of computer security experts and law enforcement officials: social network theory and game theory. This will be described in detail later. For right now, let us focus on a brief description of the two theories. In the context of cyberterrorism, social network theory implies that cyberterrorists operate in an "all-channel" type of network (Bavelas, 1950; Leavitt, 1951), that is, a network where all dispersed nodes (cyberterrorists) can be interlinked for simultaneous dissemination of information and instant coordination (Barabasi, 2002). This is precisely how the Internet chat room works: simultaneous dissemination of information and immediate coordination. Likewise, computer security experts and law enforcement officials also need to network in an "all-channel" type of network, via computers and new communication technologies. Recall that it takes networks to fight networks.

Game theory is the second theory used in this research. Game theory studies how individuals behave when they are placed in situations that require them to interact with other individuals. Game theory is about power and control. It rests on the premise that

each player "must first know the decision of the other agents before knowing which decision is best for himself or herself" (Jehle & Reny, 2001, p. 267). As applied to cyberterrorism, cyber attackers like to commit malicious acts where they believe it will help change the course of actions that are used to prevent these attackers from reaching their goals. Any action that causes damage to a computer network will give a sense of victory to these cyberterrorists (i.e., self-glorification as the "enemy" suffers, and so on). On the other hand, the response from the computer administrators against a cyberterrorist action is twofold: retaliation (offensive) or conciliation (collaborative). Ironically, collaboration between the attackers and the defenders can contribute to the shrinking of the cyberterrorist network by reducing the number of members who were part of their [the cyberterrorists'] network. What happens is that the computer network can make it appear that the conciliation was not the result of the actions taken by the cyberterrorists. Consequently, some of the members may feel that the cyberterrorist attacks in question have not carried the impact they had hoped.

Rationale for Conducting this Study

This section explains the rationale for conducting this study. Cyberterrorism is an act of terror that is waged on the Internet; many of us are potential targets of cyber attacks, which happen on a daily basis. Cyberterrorism is the sort of fear that can land in any home connected to the Internet. Therefore, millions of Internet users have something to worry about (Dunnigan, 2003). The fight against cyberterrorism requires law enforcement agencies and other groups to develop strategies, guidelines, and protocols – through solid networks – for sharing information about computer vulnerabilities and

cyber attacks (Peterson, 2002). Our daily lives depend on the outcomes of such joint efforts. Therefore, this study pertains to all of us.

This Study Breaks New Ground

This study breaks new ground. Most studies on cyberterrorism and its effects on Internet and computer networks have been conducted in the disciplines of business, management information systems, and information technology (i.e., Brynjolfsson & Mendelson, 1993; Klein & Myers, 1999). Yet, questions such as, "What are networks of cyberterrorists?" "How to defend against networks of cyberterrorists?" and "What are networks between cyber forensics labs and law enforcement agencies?" have been barely or inadequately answered from a communication perspective. Besides, no qualitative research has ever been conducted on the analysis of networks between computer security labs (i.e., in universities) and various agencies (that is, law enforcement agencies such as police departments and the Federal Bureau of Investigation) in their fight against cyberterrorists.

Likewise, no investigation of cyberterrorist networks from a qualitative standpoint has been published. This analysis of the "social aspect" of computer security helps readers, laypersons, and society in general better understand what a cyberthreat is, how networks of terror form and function, and how computer security labs and various agencies work together. One theory about terrorism is that the next big terrorist threat, among others, will happen within our computer systems.

New Theoretical Approaches

Although social network theory has been vastly applied to the study of terrorism (see Arquilla & Ronfeldt, 2001), it has been rarely applied to the analysis of

cyberterrorism (see Matusitz & O'Hair). In this study, the readers will notice that cyberterrorists are sometimes labeled as "nodes" in the network, with hubs being their central locations (i.e., Internet chat rooms). The theory will hopefully contribute to the study of networks in cyberspace and be further applicable in the context of organizational communication and new communication technology.

In line with these contentions, to date, no cyber forensics experts or law enforcement professionals have advocated using principles based on game theory to try to model or predict the probability of a cyberterrorist attack. Therefore, they will find value in reading this study because they have never taken their experience and knowledge of cyberterrorism, the Internet, and computer security into the theoretical framework that are used in this study. The fact is that cyberterrorism is an area of investigation where practical application of game theory is essential. Game theory explains that, if a computer security expert wants to stay equal to, or one step ahead of, a cyberterrorist, state-of-the-art expertise in defensive and offensive computer-related strategies is required. Protection of computer and Internet assets is critical in today's corporate, military, academic, local, and national environments. For this reason, it is crucial to understand how networks of cyberterrorists form in order to keep our systems operative and secure. Game theory offers an array of powerful strategies for aiding understanding in the domain of cyberterrorism.

A third and final point is that game theory is applied to social networks as I am attempting to show that the two theories intersect. This intersection of the two theories is primarily explained at the end of the literature review and allows me to perform a more complete analysis. The next three divisions of this section justify why this study is

important for the subfield of organizational communication, for the subfield of new communication technology, and for the field of communication at large.

Importance for the Subfield of Organizational Communication

This study is important for the subfield of organizational communication for two main reasons. First, it improves the understanding of organizational communication overall. In fact, today is a very good time to explore perceived problems for research in organizational communication, especially in consideration of the substantial number of reported problems of information security systems in organizations (Lee, 2001). As the nature of cyberterrorism as well as Internet and network security is still being debated, and despite the fact that organizations, businesses, or even private-home PC owners might suffer from cyberterrorist attacks, particular attention to the identification of relevant actors in the organizational network of both cyberterrorists and computer security experts and law enforcement agents is important.

Second, this study does not only increase the understanding of Internet and computer-related networks; it also increases awareness of the importance of interorganizational communication. The big challenge is to understand how cyberterrorist networks form, how they operate to carry out attacks, and how they can be dismantled. Equally challenging is to determine how networks of computer security experts and law enforcement agents function in all respects. If their networks are strong, they are able to identify, resist, and maybe thwart networks of cyberterrorists. The ultimate goal is to purge cyber attackers from our systems. After all, the goal is to improve society as a whole, is it not? Given that many present-day organizations are increasingly using computer technology, greater security will smooth the progress of the work of IT security

analysts, managers, and other vital members of organizations in their attempts to strengthen the exchange of information and knowledge quality. For all these reasons, this study likely advances the subfield of organizational communication.

Importance for the Subfield of New Communication Technology

In line with these arguments, this study corroborates the idea that terrorist networks doubtlessly co-evolve with technological innovation. Information technology has the capability to radically alter the very notion of communication (Brynjolfsson & Mendelson, 1993). Since very poor or inadequate research on the importance of the role of the Internet and the World Wide Web in the creation and organization of both cyberterrorist networks and networks of computer security experts and law enforcement agents has been conducted so far, this study contributes tremendously to the subfield of new communication technology. Today, the introduction of computer and information technology brings unique changes in the way humans, whether good or bad, communicate with one another (Dewett & Jones, 2001; Park & Yun, 2004).

In addition, a unique application of game theory to a phenomenon related to new communication technology allows readers to understand the extent to which the interactions between the cyberterrorist and the computer security agent are to be viewed as a postmodern two-player game. As opposed to conventional combat techniques, conflict in cyberspace allows for the use of grand strategies aiming at fast and easy disintegration of the respective enemy. Not only can the cyberterrorist make multiple, simultaneous moves (as if he or she were composed of multiple selves), but, also, both the cyberterrorist and his or her opponent can make multiple, simultaneous moves coincidentally. In this world of new communication technologies, time and space are so

flexible that they allow for change and fluidity, so much so that the cyberterrorist's resources may change drastically and very fast; he or she can acquire new tools, new weapons, new techniques, and new strategies within seconds. Any computer network that is unable to handle that is at a serious disadvantage. In cyberterrorism, where new opportunities for attack are rapidly, effortlessly, and repeatedly introduced, online learning of these opportunities for increasing the chances of achieving the expected desires and outcomes is a good strategy. This is where game theory perfectly fits in the subfields of new media and communication and technology.

Importance for the Discipline of Communication at Large

Finally, my research questions offer a unique contribution to the discipline of communication at large because they are a glance at the future. Computer security represents a fairly new topic in qualitative research. Therefore, the research questions will establish a long research agenda on the topic because it is situated in a time of significant change: many twenty-first century organizations operate and survive in networks run by cutting-edge computer technology. Consequently, their viability is based upon information and communication technologies (ICT), which are a constituent element of organizational form. As such, my research questions can broaden the horizons of the communication discipline by allowing scholars to move effortlessly across several subfields of the communication discipline. Most of the study pertains to organizational communication. Yet, as we have seen, the subfields of new media and communication technology also fit very well in this study because the issue at hand deals with human interaction in cyberspace and the protection of computer and information systems.

Recall what was just said: the context of qualitative research with regard to computer security is relatively new. As Klein and Myers (1999) put it, examining a phenomenon related to information systems from a qualitative perspective improves "the quality of future interpretive field research in information systems (especially that of a hermeneutic nature)" (p. 70). As explained at the end of the methods chapter (Chapter III), the use of qualitative interviewing for investigating my research questions is an appropriate method for analyzing untapped areas in computer security. I asked the participants to recount from their personal experiences so that they could supplement the qualitative analysis and give me a sense of the impact that information technology has on various Internet-related activities and social network practices. More importantly, no problem to date has been adequately or amply investigated as to what cyberterrorist networks are and how cyber forensics experts and law enforcement agents network among each other in order to fight these networks. Therefore, my research questions will be of interest to communication scholars from various subfields because these questions will enable them to take unique angles for investigating the nature of Internet and computer security networks by gathering data in the context of organizational communication and new communication technology.

Chapter II

Literature Review

This very extensive literature review is essential for understanding the goal of this study. The first fifteen pages or so deal exclusively with cyberterrorism: the origins of the word, what it means today, its legal definition, who the cyberterrorists are and where they mostly come from, the tools that they use, the tools that law enforcement agents use against them, what good cases of cyberterrorism can prove that it does happen, and what social networks of cyberterrorists look like. The second part of this literature review deals with social network theory: its definition, its main components (i.e., nodes, hubs), its origins (in the social sciences), its roots in systems theory, and its applications to the Internet, to the threat to Internet and computer security, and to cyberterrorist networks. The third part of this literature review is a comparative analysis between terrorist networks in Antiquity and cyberterrorist networks today. The goal of this comparative analysis is to demonstrate that although they resemble one another in some ways, they also differ in many other ways. One major difference is that cyberterrorist networks are postmodern types of network, where no leadership is needed, no center exists, and where communication is very flexible.

This leads to the fourth part of the literature review: postmodernism and networks of cyberterrorists. This section describes postmodernism and discusses the application of postmodernism to cyberspace with respect to (1) Baudrillard's hyperreal/real continuum, (2) the fragmentation, fluidity, and decentralization of the self as a result thereof, (3) cyberterrorism *per se*, (4) the organizational challenges of cyberterrorist networks faced by cybersecurity and law enforcement agents, and (5) the absence of leadership in

cyberterrorist networks. The fifth part of the literature review deals with a postmodern theory of terrorism in cyberspace: game theory. This section begins with an explanation of the rationale for using game theory in this study, its origins, and a full description of the theory. Then, the literature proceeds to describe the role of communication in game theory and its applications to terrorism. What comes next is a description of the application of the theory to cyberterrorism and how game theory and social network theory can be intermingled to investigate cyberterrorism. The sixth part of this literature review is an important premise in this study: it takes networks to fight networks. As such, this section explains the importance of cyber forensics in networks fighting networks, the social networks between law enforcement agencies and cyber forensics labs, and the crucial role of university cyber forensics labs as well as the role of informal networks. The last part of this literature review deals with the ethical dilemmas (for cybersecurity experts) in this whole course of action. An issue that could be dealt with after this study is completed is the following: is computerized surveillance acceptable from an ethical standpoint, even if the objective is to benefit society as a whole?

Cyberterrorism

Cyberterrorism, what a strange word. Believe it or not, few people know what it means. And when they think they know what it means, they usually get it wrong. It might be interesting for the readers to describe cyberterrorism from various angles. Let us start with a brief description of the origin of the word.

Cyberterrorism: Origin of the Word

Cyberterrorism is the use of electronic networks, and computer technology, as a weapon (Dunnigan, 2003). Attacks through the Internet need to have a terrorist

component in order to be labeled "cyberterrorism." From an historical standpoint, the word "cyberterrorism" was born in the late 1980s when Collin, a senior research fellow at the Institute for Security and Intelligence (ISI) in California (Collin, 1996), coined this hot techno-phrase by blending two linguistic elements: cyberspace and terrorism.

Difficulty of Defining Cyberterrorism

Today, almost two decades later, cyberterrorism remains difficult to define because this term does not have a clear, widely accepted definition. Part of the reason is that there is some controversy in the definition of cyberterrorism itself: the word consists of "cyber" – a definition for which most people would agree on – and "terrorism" – which, since 1793, has had over two hundred definitions (Schmid, 1984). "Cyber" is anything related to computers, computerized items (both real and imagined), and/or automated systems (both in terms of hardware and software). On the other hand, one man's terrorist is another man's freedom fighter. No wonder why even top scholars in the field of communication and information technology cannot agree on one single definition of cyberterrorism. An e-mail bomb can be an act of pure hacking for some, while it can be an act of cyberterrorism for others.

To solve this problem, for the purpose of this study, I have chosen a definition that I stick to throughout the entire dissertation. Yet, I believe it is important to see how other scholars have defined cyberterrorism and its related terms. Let us begin to see what the definition of a "cyberthreat" is. Cyberthreats fall into two distinct classes: (1) traditional criminal activities facilitated by computers and the Internet, such as theft of intellectual property, online sexual exploitation of children, and Internet fraud; and (2) threats affecting national security (after Internet technology emerged), such as

cyberterrorism and computer-aided terrorism (Kouri, 2005). Based on this definition, several terms have to be differentiated, some of which are "cybercrime" [which refers to the first definition of cyberthreat] and "cyberterrorism" [which refers to the second one].

Cybercrime Different from Cyberterrorism

Scholars have also compared cyberterrorism with cybercrime. Cybercrime and cyberterrorism are both acts of wrongdoing in the cyberworld (Britz, 2004). However, there is a difference between the two. The difference pertains to the motives behind the cyber attacks. Cybercrime is an unlawful or criminal act where computer technology is either a tool or a target (or both) (Britz, 2004). It is a fairly new field of criminological inquiry that comes from the area of criminal justice and it encompasses computer crime or computer-related crime (Carter & Katz 1996) and Internet crime (Wall, 2001). A cybercriminal, in essence, is a criminal who uses computers and/or the Internet to communicate, raise money, recruit new members willing to break the law, and commit other crimes. According to Archick (2003), a cybercriminal offense includes money laundering, as well "fraud and forgery, child pornography, copyright infringements, and security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability" (p. 2). Cyberterrorism deserves a more detailed definition and will be explained in detail later. Briefly described, cyberterrorism is the premeditated use of disruptive activities or the threat of using disruptive activities in the cyberworld. A cyberterrorist act always has motives that can be social, ideological, religious, political, or of similar intentions. Another objective of the cyberterrorist can be intimidating any person or group in furtherance of those motives (Dunnigan, 2003).

With respect to this brief definition of cyberterrorism, it is crucial not to forget the meaning of the word "premeditation." A cyberterrorist act is always premeditated. However, a cybercriminal act does not have to be premeditated to be called "cybercrime." A computer-whiz college student may break into a computer system for various reasons, and these reasons are not necessary intentional or premeditated. If caught, the computer-whiz college student will still be considered a cybercriminal and will probably go to jail, especially if the act was committed in a country that has cybercriminal laws, such as the United States and many European nations (see Archick, 2003). Yet, the cybercriminal will not be found guilty of cyberterrorism if his or her act is not recognized as an act belonging to one of the categories described as cyberterrorism (as it is explained later in the sub-section entitled *Legal Definition of Cyberterrorism*). In addition, cyberterrorism is typically more massive and destructive than cybercrime (Clem, Galwankar, & Buck, 2003).

Hacktivism Different from Cyberterrorism

Scholars have highlighted the importance of hacktivism as well. Hacktivism is electronic civil disobedience or Internet activism. Hacktivism consists of writing codes in order to promote political ideology (Milone, 2003). Hacktivists are cyber protesters; they have political motives and believe that proper use of code will have powerful effects (Dunnigan, 2003). However, they are not cyberterrorists because they do not cause harm to information systems, Web sites, and other computer-related materials. In other words, hacktivists do not engage in defacing Web sites, launching computer viruses, sending worms, or using malicious computer tools. If they do – and since they have political motives – then they become cyberterrorists.

Computer-Assisted Terrorism Different from Cyberterrorism

Cyberterrorism is not the same as computer-assisted terrorism (Lenzner & Vardi, 2004). Computer technology and/or the Internet can be used by terrorists (i.e., al-Qaeda members) to assist conventional forms of terrorism such as suicide bombings. They can use Web sites to simply communicate, receive orders from their commanders, obtain important information, carry out missions, propagate their messages, or recruit supporters. In a similar vein, the use of email as a medium to communicate information regarding massive-scale terrorist attacks does not constitute cyberterrorism. For instance, some experts on terrorism believe that each of the four groups of hijackers on September 11th, 2001 did not know each of the other groups, but they had communicated with a central "commander" through the Internet. The "commander" might have been a sort of "go-between" or gatekeeper" between those four groups and might have used e-mail (or a Web site) to exchange information, procure and channel funding, and organize and order the launching of the attacks against the Twin Towers in New York City and the Pentagon.

Computer-assisted terrorism does not constitute cyberterrorism (Lenzner & Vardi, 2004). Computer-assisted, just like "techno-terrorism," refers to the abundant use of computer technology by terrorists as it adds to their conventional operations. Cyberterrorism, on the other hand, pertains to attacks on information systems, on a nation's computer systems, computer-generated infrastructures, and so on. The following sub-section defines cyberterrorism in detail.

What Is Cyberterrorism?

The word "cyberterrorism" has been described in different ways and from different angles (Matusitz & O'Hair, in press). One of the definitions of cyberterrorism

tells us that it is the intentional use of threatening and disruptive actions against computers, networks, and the Internet in order to cause harm or further ideological, political, or similar objectives, or to intimidate any person in furtherance of such objectives (Arquilla, Rondfeltd, & Zanini, 1999; Conway, 2002). A similar definition of cyberterrorism is that it is "aimed at coercing a population or its government to accede to certain political or social objectives" (Clem, Galwankar, & Buck, 2003, p. 272). For the purpose of this study, I chose the definition below to show the boundary lines. So, below are the main characteristics of cyberterrorist acts (see Dunnigan, 2003; Verton, 1999):

a) hacking into a top-secret federal computer system and stealing data for ideological, religious, political, or social reasons, or the threat thereof;

b) damaging files for the reasons mentioned in *a*, or the threat thereof;

c) changing information in order to destroy infrastructure targets, or the threat thereof;

d) causing a disruption in the federal computer network as an act of retaliation, or the threat thereof;

e) destroying the actual machinery of the information infrastructure, or the threat thereof;

f) hacking into the controls of a nuclear power plant or a facility that handles hazardous materials, or the threat thereof;

g) breaching dams through electronic computer systems (as a bomber would), or the threat thereof;

h) disrupting monetary systems for the reasons mentioned in *a*, or the threat thereof;

i) damaging the mass media for the reasons mentioned in *a*, or the threat thereof;

j) shutting down power grids for the reasons mentioned in *a*, or the threat thereof;

k) disseminating false information for agency purposes, or the threat thereof;

l) sabotaging operations, via computer technology, or the threat thereof;

m) threatening to divulge confidential information or system weaknesses;

n) causing a fatal incident by changing the prescription dosage through the hacking of a computer system, or the threat thereof;

o) defacing Web sites for the purpose of spreading terrorist propaganda and for the reasons mentioned in *a*, or the threat thereof;

p) coercing a government or a political faction, via computer technology, to modify, add, or subtract existing laws or rules;

q) attacking a national, racial, religious, linguistic, or any social group or community, via computer technology, or the threat thereof.

From all these characteristics of cyberterrorism, it follows that a cyberterrorist act is a cyber attack that endangers life, has the potential to inflict bodily harm, places the public or any section of the public in fear, affects unfavorably the harmony between different national, religious, racial, linguistic, or any social groups or communities, coerces or intimidates the government established by law, and so on. This brings up the question of whether or not a hacker is a cyberterrorist.

Are Hackers Cyberterrorists?

A computer-whiz kid seeking glory and who cripples the entire computer system of a university is not a cyberterrorist if (1) the act of hacking is not premeditated and (2) the act of hacking does not pertain to any of the seventeen characteristics of

cyberterrorism mentioned in the previous sub-section. As a result, the term "hacker" does not necessarily imply that he or she is a cyberterrorist. Hackers delve into systems or networks but do not destroy them. Note that, under the U.S. Congress approved law called "Act 2001" (Archick, 2003), if the damage caused by the computer-whiz kid is significant, then he or she might be still get some punishment. No matter what, a cyberterrorist is an intentional, malicious hacker. Hackers with malicious intent are cyberterrorists who use computer systems to achieve their goals (Vegh, 2002). If the hacker just tries to delve into computers with no intention to harm computers, then he or she is plainly a "hacker." In fact, hacking can be a good tool for understanding the threats and vulnerabilities of a user's computer. The key is to understand that the tools of the cyberterrorist are the tools of the hacker just applied with different motivations.

Cyberterrorism: A Communicative and Semiotic Perspective

In addition to this, there is a very important distinction to be made between hacking and cyberterrorism. Hackers delve into systems or networks but do not destroy them; they do not even communicate their intention to do so. Cyberterrorism, on the other hand, just like terrorism, is inherently a communicative process (O'Hair & Heath, 2005). Cyberterrorism can be promoted via the Internet, a public communication channel. As such, it is publicized and perpetuated through new media communication. Therefore, it is essentially through semiotics and the exploitation of new media that cyberterrorists find success in accomplishing their primary goals. Semiotics is the study of signs (Berger, 1989; Luskin, 1996; Nöth, 1995; Sebeok, 1994). A sign communicates something that stands for something else, or that can be made to represent or symbolize something else (Berger, 1989). A sign system is embedded in the construction of meaning in a process of

symbolizing the world that takes place outside of human awareness. According to semioticians, we do not face a "simple" objective reality. Instead, what we see are signs and symbols within a communication context, where the communication of messages is considered essential to the construction of meaning (Fiske, 1982). From this vantage point, meaning is not absolute; it is not a static concept. On the contrary, it is an active process that is subject to continuous transformation. Besides, verbal communication is not the only medium that conveys meaning. Semiotics also deals with nonverbal communication (Benford, 1998).

So, cyberterrorism is a semiotic act that is a message, a symbol, and a new media image. Our modern western world is immersed within images, signs, and symbols (Miller et al., in press). It is no surprise, then, that there is a powerful semiotic dimension to cyberterrorism. Indeed, it can involve sending images of fear. For instance, as will be explained later, in 1998 cyberterrorists sent a massive flood of e-mails to the Sri Lankan embassy's main Web server with messages that read "We are the Internet Black Tigers and we are doing this to disrupt your communications." The intent was not only to crash the computer systems of the embassy – and they succeeded (Denning, 2000) – the motive was also to send a semiotic message that evoked fear. Likewise, cyberterrorism is a semiotic gesture because it aims at creating not only fear, but also *signs* of fear. It is important to consider that, on the whole, cyberterrorist attacks are not successful. Although, theoretically, cyberterrorists could take down the whole U.S. West Coast if they managed to cripple a few massive power grids, in reality they create fewer casualties than is expected by the magnitude of the news they elicit. What it implies is that such acts leave compelling signs and images permanently anchored in our minds (Miller et al., in

press). For example, the movie *Firewall*, starring Harrison Ford, is a product of this. In the movie, the messages conveyed by cyberterrorist attacks of all sorts have an impact on Harrison Ford because those messages create interference and anxiety in the form of potent psychological noises in his (and his family's) daily life.

Just like terrorism is primarily a process of communication between terrorists and target audiences (Tuman, 2003), an important goal of cyberterrorists is to send a powerful signal, whose meaning is intended to frighten and coerce. Based on the seventeen characteristics of cyberterrorism mentioned earlier, cyberterrorism serves another semiotic function when it communicates a violent political meaning that symbolizes more of an ideological statement than a massive material threat. As we will see later, in 2002, a group of cyberterrorists, known as the World Fantabulous Defacers (WFD), hacked into the official Web site of Israeli Prime Minister Ariel Sharon and defaced it. As a title, they wrote, "The Face of the World's Biggest Murderer." At the bottom of the Web site, they left a message with the signature of the group. The WFD's hacking into Sharon's official Web site stands out as one example of a cyberterrorist group that was in a position to do far more damage and perhaps cause a national crisis in Israel (Verton, 2003a). By gaining such visibility – and sometimes they can infiltrate hundreds of thousands of computers – cyberterrorists are able to spread terror and evoke fear.

Finally, what is also very semiotic is the relationship between cyberterrorism and new media such as the Internet and information technologies. Without these, cyberterrorism is an ill-fated task. Cyberterrorism news is made to order for the specific requirements of new media. Farnen (1990) already noted this when describing terrorism. As he remarked, "terrorism is different, dramatic, and potentially violent. It frequently

develops over a period of time, occurs in exotic locations, offers a clear confrontation, involves bizarre characters, and is politically noteworthy. Finally, it is of concern to the public" (p. 111). The exploitation of communication technologies by cyberterrorists is a fundamental element of the semiotic cyber struggle. In order to trigger economic chaos, lose of faith (on the part of certain businesses) to do transactions online, and massive overreaction from the public, cyberterrorists count on those communication technologies to stir up the target population by using images which, once produced, can be evoked again later and reused to new effect. Now that we have seen the communicative and semiotic perspective of cyberterrorism, let us digress for a moment and focus on its legal perspective.

Cyberterrorism: A Legal Perspective

A little after the 9/11 attacks in New York and Washington, the U.S. Congress approved a new antiterrorist law called "Act 2001" (Archick, 2003). "Act 2001" included cyberterrorism as part of the legislative jargon and classified different types of cyberterorrism and wreaking losses to protected computer systems of citizens, juridical persons, and federal and state departments (including offices that coordinate national defense and ensure national security). Archick (2003) briefly describes those different forms of cyberterrorism. According to Archick, a cyberterrorist act is a cyber attack on critical infrastructure facilities, financial institutions, or government systems that are premeditated and motivated by the goal to (1) intimidate or coerce a government, the civilian population, or any segment thereof and to (2) further political, social, or ideological objectives.

The Filipino author of the "I Love You" virus, a hacking achievement that caused over $10 billion in damage around the world (*New York Times*, June 13, 2000), was never prosecuted because in 2000, when this 23-year old male student sent his devastating hybrid virus, no applicable laws on cyberterrorism existed in the Philippines. So far, the Filipino hacker has not revealed any malicious intentions to send that virus. Even if according to BBC news, in an article entitled "Love Bug Revenge Theory" (published in May 10, 2000), the police believe that the Filipino hacker had the personal objective of retaliating against computer systems after his Master's thesis was rejected, and even if for the American Computer Economic Group, the "I Love You" virus has been the most damaging act of cyberterrorism ever witnessed to date, the "I Love You" virus cannot be considered a cyberterrorist act because we do not know the intent of the Filipino hacker. Although the hacker's virus infected and compromised computer systems including that of the Pentagon, governmental establishments, parliaments, and corporations worldwide (Wehrfritz & Vitisca, 2000), we do not know if the hacker's objective was political, social, or ideological. It might have been an accident. The fact that no cyberlaws existed in the Phillipines in 2000 is a reflection of the clash between the old and the new in many legislative systems. As Ziff (2005) points out,

> police officers and other government agents commonly seize and search computers during criminal investigations. When reviewing the search of a properly seized computer for compliance with the Fourth Amendment, courts face the complicated task of applying constitutional protections from the eighteenth century to today's computerized world (p. 841).

If the Filipino hacker were to send that virus today and if he were caught in the process by either European or American authorities, he would face legal imprisonment for two reasons. First, this virus today would constitute a cyberterrorist act, based on the definition given in the first paragraph. Second, he would be considered a cyberterrorist by both the U.S. Congress and the Council of Europe's Convention (which is composed of 33 countries, including the United States). The 2001 treaty of the Council of Europe's Convention is the first international treaty designed to harmonize laws on cyberterrorism, "improving investigative abilities and boosting international cooperation" (Archick, 2003, p. 1). What this boils down to saying is that, from a legal standpoint, times have changed since the "I Love You" virus harmed so many computer-based infrastructures in 2000. Today, not only is there a legal definition of cyberterrorism ratified by many developed countries, but, also, international laws have been approved to identify, combat, and punish cyberterrorism.

Cyberterrorists Come from All over the World

The literature has shown that many cyberterrorists come from five different geographical areas: (1) North America, (2) Western Europe, (3) the Eastern block and the ex-Soviet Union, (4) Far-East Asia (mainly China, Korea, and Taiwan), and (5) the Middle-East.

The first major group of cyberterrorists is to be found in North America. In 1994, a cyberterrorist broke into the computers of an Arizona water facility, the Salt River Project in the Phoenix area. The person behind the attack was only 27 (Washington Post, 2002). Likewise, in March 2000, a computer virus was believed to have targeted the

Houston 911 system for massive disruption. The damage could have been unprecedented (Verton, 2003a).

The second major group of cyberterrorists is composed of computer users from Western Europe. During the late 1980s, a hacker group in Germany sold information to the ex-Soviet KGB. The German group accessed the information by hacking into computer systems in Departments of Energy and Defense, defense contractors, and NASA (Stohl, 1989). Had they succeeded, the damage would have been colossal. In another example, during the Persian Gulf War, a group of Dutch cyberterrorists who had penetrated the Department of Defense systems attempted to sell their services to the Iraqis (General Accounting Office, 1991).

The third major group of cyberterrorists is composed of Eastern Europeans and citizens of the ex-Soviet Union. The threat of networked cyberterrorism appears to have originated in the former communist countries of Eastern Europe (Kouri, 2005). In a similar vein, it has been reported that many ex-members of the former Soviet KGB are computer-savvy and have a solid background in the black arts of espionage (Center for Strategic and International Studies, 1998), which poses an enormous concern to energy systems, electric sectors, and power operations. Experts are particularly worried about highly qualified computer specialists from the former Soviet Union (Matusitz & O'Hair, in press). Paying for the services of ex-Soviet hacker groups could disrupt the management and control systems since they have been well trained in cyberterrorism. Furthermore, it might the case that hacker groups that despise the United States decide to independently perpetrate attacks on American targets.

The fourth major group of cyberterrorists is composed of computer users from Far-East Asia (Dunnigan, 2003). We already know the story of the hacker from the Philippines. Briefly describing a major cyberterrorist incident, in 1998 the Sri Lankan government got a bitter flavor of cyberterrorism when a flood of e-mails was sent to the embassy's main Web server with messages reading "We are the Internet Black Tigers and we are doing this to disrupt your communications." The e-mail bombing crashed the computer systems of the embassy (Denning, 2000). The Internet Black Tigers are Sri Lankan members of a specialized faction of the Liberation Tigers of Tamil Eelam (LTTE). Their intent is to harm the Sri Lankan government, whether through conventional terrorist acts or through cyberterrorist acts (Vidanage, 2006).

The last major group of cyberterrorists is composed of computer users from the Middle East. According to Dunnigan (2003), there have been many malicious hackers from the Middle East who have attempted to destroy Web sites of American power plants. When they cannot strike power plants, they put zombies (see next sub-section) in thousands of homes PCs and launch Denial-of-Service attacks (see next sub-section) on military, commercial, and government Web sites, of which the consequences would be deleterious.

What Tools Do Cyberterrorists Like to Use?

More astoundingly, examples of cyberterror on computers and the Internet are as simple as malicious software such as computer viruses, trojan horses, vampires, logic bombs, computer network worms, and DOS attacks.

Virus: a computer virus is a software program that can copy itself (Schwartau, 2000). By self-replicating, it is oftentimes capable to cause massive harm to files or other

programs on the same computer. A virus "attaches itself to a legitimate program or document (for example, a Microsoft macro virus is embedded in word processing or spreadsheet files)" (Schwartau, 2000, p. 8). Yet, a virus cannot propagate to another computer without human intervention. A computer virus acts in a way that resembles a biological virus: it proliferates by putting itself into living cells. Not all viruses that target our computer systems are harmful; some are in fact innocuous. Sadly, though, we rarely see those (Dunnigan, 2003). And to show how devastating a computer virus can be, it might be interesting to remind ourselves of the cyberterrorist attempt against the Houston 911 system for widespread disruption. Fortunately, the attempt to send a computer virus failed. Had the virus been successfully activated, it would have had a ripple effect (the possibility was that each infected computer propagated over 2,500 computers simultaneously). It would also have erased the infected computer's hard drive on the nineteenth of the month, creating in effect a massive DOS attack against the 911 emergency system (Verton, 2003a).

Trojan horse: a Trojan horse is not a virus; yet, a virus might include a Trojan horse (Schwartau, 2000). A Trojan horse is a software application where users are misled into installing a program that is replete with infected documents. This program is to be downloaded, for instance, through clever e-mails. To make the trick even more realistic, such e-mails sometimes appear to come from friends or colleagues. In other words, a Trojan horse is masqueraded as another legitimate program (Dunnigan, 2003). The goal of the cyberterrorist is to damage the victim's computer or files (Mitnick & Simon, 2002). According to an article entitled "Britain Warns of Trojan Horse Computer Attacks" (2005), central government computers have been the most usual targets of

Trojan horses. Corporations and individuals are also at risk, based on a warning given by the British National Infrastructure Security Coordination Center (NISCC). The aim of cyberterrorists appears to be covert gathering and sending of commercially or economically valuable information. In many cases, as Mitnick and Simon (2002) put it, "the reason this technique [sending a Trojan horse] is so effective is that it follows the theory of killing two birds with one stone: The ability to propagate to other unsuspecting victims, and the appearance that it originated from a trusted person" (p. 96).

Worm: a worm is a type of virus that slowly moves around from computer to computer and, then, slows things down. A worm tends to eat through and at resources (Schwartau, 2000), and does not attach itself to other programs (Dunnigan, 2003).

Logic bomb: it is a hidden software program in a computer system that is executed when certain conditions are met. At that point, what follows is that the program does something usually bad (Dunnigan, 2003). A logic bomb is an unauthorized computer code, sometimes sent by email. When activated, it looks for specific conditions or specific states of the system which triggers the perpetration of a destructive act of sabotage, deletes or corrupts data, and has other harmful effects.

DOS attack: DOS stands for denial-of-service attack; it is an attack against a computer system or network, causing a loss of service to users, usually the loss of connectivity and services by overwhelming the bandwidth of the target's network or congesting the computer-related resources of the target's system (Schwartau, 2000). DOS attacks "flood servers with so many incoming messages that the server can do nothing else but try and deal with the flood" (Dunnigan, 2003, p. 209).

Zombie: sometimes called "bot" or "robot," a zombie is a system that has been taken over using Remote Control Software. In many cases, a zombie is used to send spam or to attack remote servers with an overwhelming amount of traffic. It also enables the cyberterrorist to have easy access to the intruded computer, to launch attacks from that computer, to delve into password-protected chat rooms, and get into the storage for the invader's files (Dunnigan, 2003). A zombie, however, is more likely to be discovered and cleaned out if stored in professionally run Web sites (Dunnigan, 2003).

Vampire: a worm or a virus of which the sole purpose is to run so profusely that the infected computer cannot do anything else. To be more precise, after the vampire starts running, it begins to replicate itself, to such an extent that the victim's server is so active running hundreds of copies of the vampire that it can do nothing else (Dunnigan, 2003). As one can imagine, vampires pose a threat to Internet software and, when activated, they constitute a chance for the cyberterrorists to strike.

The importance of listing and defining those cyberweapons lies in the very fact that they can be used by nasty individuals "to shut down computers, destroy data, and damage the nation's power plants, factories, fuel supplies, communications systems, and even parts of the armed forces" (Dunnigan, 2003, p. 5). Now, it might be interesting to know what tools can be used for protection against cyberterrorism.

What Are the Tools against Cyberterrorism?

Computer security experts say that, although the first targets of cyber attacks tend to be government agencies, organizations and businesses that have not established security measures to protect their systems are also fair game. Some of the tools used against cyberterrorism are firewalls and anti-virus software programs.

Firewall: a computer system with special security precautions. Located between the Internet and a local network, it performs the role of a gateway to prohibit unauthorized or seemingly dangerous material from entering the network and to keep external nodes from accessing, say, an organization's confidential data. Major Web sites and corporate computer systems have protected themselves with firewalls because they have the funds and motivations to do so. For instance, American power plants have well-protected Internet operations and are well equipped to detect malicious intruders. Yet, they still have soft spots. According to an article entitled "Britain Warns of Trojan Horse Computer Attacks" (2005), firewalls do not give complete protection, and there is no complete mitigation for computers connected to the Internet.

Anti-virus software: a software program that examines the computer memory and disk drives for malicious code. The program modifies the user if a virus is present, and will clean and delete infected files or directories.

Other Cases of Cyberterrorism

In an earlier section, we saw that the fourth group of cyberterrorists is to be found in Far-East Asia. Thornburgh et al. (2005) tell us about a Chinese group of cyberterrorists called Titan Rain that stole U.S. secrets. Those cyberterrorists are voracious, never hesitating to destroy any parasitic file they could find coming in their way, attempting to penetrate secure computer networks at the American most sensitive military bases, defense contractors, and aerospace companies. According to the same Thornburgh et al. (2005), those Chinese cyberterrorists work for the government in mainland China and have a political goal. Their cyber attacks come from just three routers that seem to be the first connection point from a local network to the Internet. A TIME investigation into the

case reveals how the Titan Rain attacks were uncovered, why they are considered a significant threat now under investigation by the Pentagon, the FBI and the Department of Homeland Security, and why the U.S. government has yet to stop them (Thornburgh et al., 2005).

In the U.S. military, Titan Rain is creating fears. In fact, Titan Rain has the ability to cause widespread havoc as hundreds of computer systems in the Department of Defense have been penetrated by insidious programs such as Trojan horses. Not only could Titan Rain control the DOD hosts, but they could also use the DOD hosts in malicious activity (Thornburgh et al., 2005). The possibility also exists for the perpetrators to shut down each host. Allied nations such as Britain, Canada, Australia, and New Zealand have also been targeted by the Chinese cyberterrorists (Thornburgh et al., 2005).

Social Networks of Cyberterrorists

Although cyberterrorists tend to work alone, they sometimes feel the need to team up with others. In many cases, the now networked cyber attackers claim they are fighting a worthy cause. A few cyberterrorist groups are noticeable as being the "elite," as they have done some of the major attacks around (Zepp, 1999). When cyberterrorists network, they network with other factions through various channels of communication. This method reinforces the needs of the community of cyberterrorists without the necessity of creating a large-scale single organization, like a massive conventional terrorist organization. So, cyberterrorists have become involved in Internet social networks (McKenzie, 2004). Some cyberterrorist groups like to act as cybersurrogate groups in order to help other cyberterrorists – who are really in need of help (i.e., regarding the

design of certain malicious software programs, etc.) – increase their chances of striking the right node or hub in the Internet or computer network. This has been proved easy and advantageous (Schwartau, 1996).

Social Network Theory

This section is an extensive analysis of social network theory, the study of the connections between individuals or organizations, forming what we call "social networks." A "social network can be defined as a set of nodes or actors (persons or organizations) linked by social relationships or ties of a specified type. A tie or relation between two actors has both strength and content" (Castilla et al., 2000, p. 219). The study of social networks is important because it helps us better understand how and why cyberterrorists interact with each other through networks, and how the design of the network itself, especially in this day and age where technology plays a central role, can alter their interactions. This section starts with a definition, description, historical explanation, and identification of the basic tenets of social network theory. Then, it provides a synopsis of its role and scope in the social sciences and how the theory has become what it is today. As such, particularly examined are its origins rooted in Hegel's systems theory (Beiser, 1993; Kojeve, 1969). Systems theory stresses the idea that every single element in a system or organism is inseparably interconnected with its environment in dynamic webs of relationships. In other words, a system is more than the sum of its parts.

The end of this section focuses on the applications of social network theory to the Internet. In brief, the Internet is composed of an extremely large network of nodes that link computer systems worldwide, allowing them to send and receive information

(Dorogovtsev & Mendes, 2003). The section also describes how the theory applies to the threats to Internet and computer security. The main idea here is that the Internet is a scale-free network, which means that its nodes, the number of links on Web pages, the connection among users, and even emails are scale-free. A scale-free network is characterized by an uneven distribution of connectedness. While many nodes in the network are random (that is, they have a random pattern of connections), a few nodes act as hubs that have many connections (Matlis, 2002). The danger to this is that, because the Internet is a scale-free network, it is able to survive attacks or failures of its high number of insignificant nodes (called "random" nodes), but it is very vulnerable to targeted cyber attacks (Albert, Jeong, & Barabasi, 2000; Ball, 2000) against its most important nodes. The reason lies in the fact that these nodes are so powerful that they act as very connected hubs as they connect a great number of Web servers. Barabasi's explanation of the Internet network shows us that stopping a malicious software program from propagating requires that we focus on protecting those hubs (Albert, Jeong, & Barabasi, 2000). Finally, this section discusses social network theory as applied to the Internet, to the threats to Internet and computer security, and to cyberterrorist networks.

Social Network Theory: Definition

Social network theory is the mapping and understanding of social networks. The theory has grown considerably in this day and age since advanced computing technology has opened the door for new research. It is also a branch of social science that applies to a wide range of human organizations, from small groups of people to entire nations. As such, social network theory is the study of the connections between individuals (Degenne & Forse, 1999; Freeman, 1981; Lipnack & Stamps, 1986; Scott, 1991; Scott, 2000;

Wasserman & Faust, 1994; Wellman & Berkowitz, 1988) or organizations (Nohria & Eccles, 1992), forming what we call "social networks." Social network theory involves relationships that explain the emergence, success, and dissolution of communication networks among individuals or organizations. These networks should be paid attention to because they reflect how humans amass the different types of support that they need, such as financial, political, and moral support among cyberterrorists.

In the same train of thought, social network theory has shown that many intriguing properties of complex systems lie in their patterns of interaction (Sassen, 1992). In fact, all patterns of interaction can be portrayed as networks (Barabasi, 2002; Buchanan, 2002; Strogatz, 2003; Watts, 1999a, Watts, 1999b). Then, it is no surprise that social network theory is applied to society, college classes, financial markets, ecospheres, friendships, romantic liaisons, marriages, and… hacker groups. Indeed, as we will see, networks also shape processes of terror and violence.

What Are Social Networks?

A social network refers to a group of objects, entities, or people – sometimes called *nodes* – and the relationships between these objects, entities, or people. In most social networks, the objects refer to persons or groups (Lipnack & Stamps, 1986; Scott, 1991; Scott, 2000; Wasserman & Faust, 1994; Wellman & Berkowitz, 1988). For Castilla et al. (2000), a "social network can be defined as a set of nodes or actors (persons or organizations) linked by social relationships or ties of a specified type. A tie or relation between two actors has both strength and content" (p. 219). Social networks can have sub-networks (like hybrids). As such, they can be a combination of networks within networks (as simply said, networks of networks), with numerous nodes linked in various

ways, like in a spider's web. It is also fair to say that a social network is a collection of connected "points" generally designed to be resilient through redundancy. It can be one terminal, connected to the Internet, or one expert communicating with another expert in a common network devoted to a shared problem (Monge & Contractor, 2001, 2003). The design of a particular network also determines its resilience, its flexibility, its capacity to expand, and its vulnerability (Buchanan, 2002). The study of social networks, then, is important because it helps us better understand how and why we interact with each other, and how the design of the network itself, especially in this day and age where technology plays a central role, can alter this interaction.

As Castells (1996) puts it, "networks constitute the new social morphology of our societies, and the diffusion of networking logic substantially modifies the operation and outcomes in processes of production, experience, power, and culture" (p. 469). An analogy can be made here with Prigogine's (1969) concept of dissipative systems. A dissipative system is an open system characterized by the natural and unstructured appearance of a complex, sometimes chaotic, structure. The first phenomenological issue of a dissipative system is the realization that a "closed" physical system does not exist (Cahill & Kinger, 2000). From this vantage point, the interaction of a system with the outside world may become the beginning for the formation of a new dynamic state of matter for the system. So is a network; it is a dissipative structure that requires a continuous flow of matter and energy to maintain its state (Stengers & Prigogine, 1997). A network is an emergent structure that arises in a self-organizing system. Such a structure is dissipative in nature because it serves to dissipate energy in the system (Stengers & Prigogine, 1997).

The concept of "social network" is mostly associated with industrial society. Yet, it is interesting to know that as an organizational form it is an ancient practice. For instance, maritime trading networks were common in islands of ancient Greece and the islands that now constitute Indonesia (Landa, 1994). Later, in the Middle Ages, Christian religious scholars, who lived in isolated monasteries of Western Europe, organized an effective form of interaction through distributed social networks. Similarly, in the 11th century Maghrebi traders used networks of information exchange (Greif, 1994). Historians also record that families, ethnic diaspora groups, and communities around the world can all be seen as variants of social networks (Yarbrough & Yarbrough, 1999). Today, social networks are omnipresent (Buchanan, 2002). Whether they bind computers, economies, or hackers together, social networks are everywhere in the real world. In fact, the network appears to be an innovative form of organization – long after tribes, hierarchies, and markets – that comes into its own to put a new frame to society, and in so doing, the nature of conflict and cooperation (Arquilla & Ronfeldt, 2001).

In line with these contentions, while some social networks are hierarchical, like the church structure during medieval times and in some parts of the world today, other social networks are "unbounded or bounded clusters of organizations that ... are nonhierarchical collectives of legally separate units" (Alter & Hage, 1993, p. 46). From this, it follows that a network can be organized on a non-hierarchical basis (World Health Organization, 1998). In fact, a network is more nimble and flexible than a hierarchy; it is more adaptable to changing circumstances. A network can differ in its formality, size, goals, and durability any time. Some networks are not fixed; they can be very malleable (Barabasi, 2002; Buchanan, 2002). It is often an unplanned, emergent system whose ties

end up being unevenly distributed, with some areas of the network sparsely connected. As such, a (social) network can take on many different forms (Provan & Milward, 1995). For instance, one form is the chain or line network (Bavelas, 1950; Leavitt, 1951), where information moves in a sequential manner through a series of nodes. Another form is the wheel or star network is a set of links with the lowest degree of shared centrality (Leavitt, 1951). A third example is the hub network where there are a number of direct connections to a router or manager node and where exchange among actor nodes must pass through a central node (Lott & Taylor, 2005); this is typical of networks of terrorist groups that do not base their acts on cyber-technology. A fourth example is the all-channel network (Bavelas, 1950; Leavitt, 1951), where any actor in the network is connected to any other actor. The all-channel is collaborative, quick, and effective, but can be difficult to maintain due to the significant need of exchange of information required. Nevertheless, it is the network of the information age and, when organized by cyberterrorists, it can be very effective (can launch multiple, repeated attacks from different points), very difficult to identify, and very difficult to destroy in its entirety (nodes are redundant).

Nodes: Essential to Social Networks

As mentioned in this previous section, a network is simply a collection of connected objects or actors called nodes. If these nodes are highly connected, they act as hubs; they do not have many connections, they are random nodes (Johnson, 2000). In social networks, a node is an individual communicating with other individuals for a common purpose (Monge & Contractor, 2001, 2003). In fact, according to social network theory, all humans are simply nodes in a network of rapidly expanding networks

(Barabasi, 2002). For a social network theorist, a complex human system should be seen as an interconnected system of nodes (people and groups) and ties (relations, connectivity, and flows). A tie concerns the ability to facilitate communication between nodes and is a measure of efficiency (Monge & Contractor, 2001, 2003).

More importantly, nodes (as trivial and innocent as they look) in a social network can also be very powerful, for three reasons. First, the high number of nodes in a social network makes it a non-homogeneous entity. As such, there is a role for individual agency and (far) less dependence on leadership. Secondly, it is worth mentioning Metcalfe's Law, coined by Robert Metcalfe (1993). According to this law, the power of a network is equal to the square of the number of nodes that it contains: an enterprise with ten nodes or intersections is not ten times stronger but a hundred times more effective than an enterprise with just one. In other words, the value of a network grows by the square of the size of the network (Metcalfe, 1993). A third reason why nodes can be powerful is that they can take one of three different forms. Some nodes are actors (Johnson, 2000), that is, people who do things and who have all kinds of skills or expertise (Barabasi, 2002). Other nodes are the directors – people with the highest power, or at least who do have power, and who are highly charismatic, influential, and motivating. Those directors also act as gateways and impact the flow of information and activity.

Now that we have a definition of social network theory as well as a description of social networks and an explanation what their nodes represent, it is worth concentrating on the origins of the theory in order to understand the current scope of the theory and

why it applies particularly well to the context of cyberterrorism. The origins of social network theory are rooted in the social sciences and in systems theory.

Origins of Social Network Theory

This section gives a description of the origins of social network theory in the social sciences and the roots of the theory in systems theory. Systems theory is Hegel's theory of interconnections among all the parts of a system.

Social Network Theory in the Social Sciences

Social network theory is an important academic specialty pursued by a number of anthropologists, sociologists, and organizational communication theorists (Ronfeldt, 2000). Their view is that all social relationships can and should be analyzed as social networks. In other words, they should be considered sets of actors (nodes) and ties (links) whose relationships form a pattern (Nohria & Eccles, 1992; Wasserman & Faust, 1994; Wellman & Berkowitz, 1997). In fact, for a social network theorist, almost any set of nodes (actors) that have ties adds up to a network. It is not surprising, then, that the abstract notion of a network is bound to play a role in the social sciences in the same way that the concept of Euclidean space and its generalizations played a role in physics (Lorrain, 1975).

Historically, social network theory became significant in the social sciences with the release of anthropologist A. R. Radcliffe-Brown's (1940) seminal article entitled "On Social Structures," and with the works of sociologists like Moreno (1934), who have been studying social networks systematically for more than five decades in an attempt to develop sociograms and directed graphs to chart the ties among different individuals in groups or in particular contexts (what gradually became known as a "networks"). One of

the reasons social network theory has become popular in the social sciences lies in the fact that scholars have attempted to map the connections among individuals (Groom, 1977). Thereby, one can evaluate the social capital of that individual. Social capital refers to the network position of a node (or person) and consists of the potential to depend on the resources contained by members of the network. Scholars in the social sciences also believe that the more mappings among people in a social network, the more growth. Growth is contingent upon the knowledge, influence, and power the original person will control. Social networks can help sociologists identify all sorts of groups: ethnic groups, tribes, groups of friends, cliques, and so on. As such, people will stay in a group where they know they can share equal power with their peers (Bonachich, 2001). This is one of the premises of social identity theory.

Social network theory has also extended its scope in organizational communication. In fact, although many writers in the social sciences have discussed social networks, one of the most well-known social network researchers is Peter Monge, an expert on organization communication (Littlejohn, 1992). Monge (1987) has demonstrated that networks are groups connected to one another by communication ties. Organization is characterized by a number of structures, each being contingent upon those communication ties within the organization (Littlejohn, 1992; Shafritz & Ott, 1996; Stohl, 1995). Other scholars in organizational communication also study what are called organization-sets (Shafritz & Ott, 1996). They have observed that networks often come in several basic shapes (or topologies): notably the all-channel or fully connected or full-matrix networks, where everyone is connected to and can communicate directly with everyone else (Evan, 1972). In the same train of thought, social network theory has been

seriously taken into consideration by organizational communication scholars who emphasize the importance of knowledge networks in global organizations and their relationships with IT-based organizations. Organizational researchers have designed computer models that test hypotheses about networks and information diffusion, changes in people's knowledge and interaction networks, and the dynamics of networks of cultural influence.

Finally, in international relations, the concept of network has been embraced by functionalists and integration theorists, and in the "cobweb" theory of world order of Burton (1972).

Social Network Theory Rooted in Systems Theory

Social network theory is among the dynamic large-scale theories of social systems (Berlinski, 1976; Hejl, 1984; Luhmann, 1982, 1995; Zeeuw, 1992) that emerged from Hegel's systems theory (Beiser, 1993; Kojève, 1969). Georg Hegel (1770-1831) was a German idealist philosopher (Lukács, 1975) who suggested a holistic approach to understanding the dynamic interrelationship of parts to a whole. Hegel's goal was to explain historical development as a dynamic process (Kojève, 1969). The main core of his theory was the system rather than the individual in isolation. As such, Hegel looked at society as a set of organizational and behavioral pattern structures that a system learned to select from the complex choices presented to it without full information as to the outcome (Beiser, 1993). In this train of thought, society came to make sense out of its options, as it came to learn from the outcomes. From this, it follows that the system develops means of self-analysis (Weinberg, 1975) to generate parts (or subsystems) that interact with all this complexity, and means to interact with these interactions. The main

premises of systems theory, then, are that a system is the sum of all its parts plus the effects of interrelation and interdependency among those parts – thus, a system is more than the mere sum of its parts – that the whole determines the nature of the parts (Lilienfeld, 1978; Weinberg, 1975), and that the parts cannot be isolated from the whole. Later, Marx and Darwin used Hegel's theory in their work. Systems theory was strengthened and corroborated by biologist Ludwig von Bertalanffy as the basis for the field of study known as "general systems theory" (Bertalanffy, 1962, 1968). Instead of reducing a biological system, such as a plant or animal, to parts (organs or cells), systems theory posits that each component is related to other parts. The entire system functions as a whole, but each part (or subsystem) is identified by the unique activity that occurs within it. Consequently, Bertalanffy's "general systems theory" influenced and impacted postliminary attempts to model system needs of organizations on those of all living systems (e.g., Miller, 1978).

Today, systems theory has become an interdisciplinary study of the organization of phenomena: living things, objects, nodes, organizations, and, of course, people. It investigates both the principles common to all complex entities, and the (usually mathematical) models that can be used to describe them. Research using systems theory constitutes a wide range of possibilities of breaking down an organizational structure or process (Cortes, Przeworski, & Sprague, 1974). Subsequent, similar theories have demonstrated various ways of powerful counterintuitive dynamic effects of system structure, and in the past decades, the technical capacities of computer modeling have given rise to a powerful explosion of simulations of complex system dynamics (Collins, Hanneman, & Mordt, 1995; Bar-Yam, 1988). It is acknowledged among many scientists

and researchers that a system is composed of four things. First, a system consists of objects – the parts, elements, or variables within the system – that can be physical or abstract. Or both, depending on the nature of the system. Second, a system consists of attributes – the qualities or properties of the system and its objects. Third, a system has interrelationships among its objects. Fourth, a system exists in a particular setting, an environment. In fact, a system is a set of things that affect one another within a particular environment and form a larger pattern that is different from any of the parts. By extension, two types of system have been described in systems theory: the closed system and the open system. The closed system does not interact with its environment. It does not receive information and is likely to disappear. An open system, however, receives information, is organized, interacts dynamically with its environment, and adjusts to its surrounding systems (Midgley, 2003).

In the same train of thought, another German thinker, Luhmann (1982) saw social systems as "autopoietic" (Bailey, 1997; Bednarz, 1988; Benseler, Hejl, & Kock, 1980; Zeeuw, 1992; Zeleny, 1981), that is, based on self-organization, something implying that all regulation in such systems is itself regulated and all controls are themselves controlled (Mingers, 1994). A system exercises control and achieves self-regulation in order to maintain stable states and adjust to its environment. In other words, it reaches the point of homeostasis (Luhmann, 1982, 1995). It becomes well ordered while it survives, and, because it attains its goals in many ways, it demonstrates the need for balance/homeostasis, change and adaptability (morphogenesis) and equifinality (Luhmann, 1982, 1995).

Finally, for the past few decades, as a result of the introduction of systems theory into social sciences, new terms have entered their vocabulary. Supporters of systems theory speak of systems, feedbacks and circular loops, cybernetic loops (Wiener, 1961), information retrieval, and, of course, networks. Since, for a system to function, there must be interaction among its parts, then networks do not exist without interconnection among individuals; by the same token, these individuals cannot be understood in isolation from the whole (Banathy, 1996). In this day and age, networks of terror are like that; they form a complex system of communications that has differentiated itself horizontally into a network of interconnected social subsystems. Within the framework of systems theory, it is of interest to investigate a cyberterrorist network by analyzing its key components.

Social Network Theory and the Internet

The rationale for describing systems theory in the previous section lies in the fact that the complex structures and growth patterns of the Internet appear to resemble those of complex living systems, among which are the metabolic networks that operate inside cells and the social networks that constitute societies (Albert, Jeong, & Barabasi, 2000). This section describes social network theory as applied to (1) the Internet, (2) the threats to Internet and computer security, and (3) cyberterrorist networks.

Social Network Theory Applied to the Internet

How does social network theory apply to the Internet? In a few words, the Internet is composed of an extremely large network of nodes that link computer systems worldwide, allowing them to send and receive information (Dorogovtsev & Mendes, 2003). The networks of emails and many Web sites, for instance, have the unique structure of what we call “scale-free” networks (also known as “small world” networks).

Scale-free networks are characterized by their centrally located, highly connected hubs, which considerably influences the way the Internet operates (Dorogovtsev & Mendes, 2003).

The great advantage for the Internet to have a scale-free distribution is that navigation and communication online are extremely fast. In contrast, it takes much longer, with many more hops, to travel or communicate across networks that are not scale-free (Albert, Jeong, & Barabasi, 2000). Furthermore, because the Internet is a scale-free network, the number of nodes with a specified number of connections automatically decreases as that number of nodes increases (Keller, 2005). Many nodes are linked to the network by way of just one connection: fewer have two, even fewer have three, and so down the line. As opposed to an exponential network, in the Internet network, there remain small but significant numbers of nodes that have many connections (Albert, Jeong, & Barabasi, 2000). Consequently, the Internet is characterized by an uneven distribution of connectedness. Instead of the nodes of the Internet network having a random pattern of connections, some nodes act as very connected hubs, which significantly influence how the Internet network operates, while many other nodes do not (Keller, 2005).

Social Network Theory Applied to the Threats to Internet and Computer Security

We have seen that the Internet enables the formation of scale-free networks (Keller, 2005) and that it is a gigantic network of nodes that link computer systems worldwide, allowing them to exchange information (Dorogovtsev & Mendes, 2003). What this sub-section accentuates is how social network theory can be applied to the dangers posed by cyberterrorists to Internet and computer security. The Internet has many

nodes, and the majority of these nodes are so insignificant that the system will still survive if these nodes can crash. Basically, these nodes are like drops in the ocean. They are called "random" nodes. If truth be told, a very small percentage of Internet nodes are down at any given time (Albert, Jeong, & Barabasi, 2000). What this means is that the Internet can cope with up to 80% of all random node failures. Indeed, a scale-free network can absorb random node failures up to 80% of its small nodes before it dismantles. The reason for this is the non-homogeneity of the nodes on the Internet network; in many cases, failures are likely to occur on relatively small nodes (Faloutsos, Faloutsos, & Faloutsos, 1999; Matlis, 2002). With their very connected nodes, which are statistically unlikely to fail under random conditions, connectivity in the network is maintained. It takes quite a lot of random failure before the hubs are wiped out, and only then does the network stop working (Matlis, 2002).

However, a major problem is that some of these Internet nodes, although few in numbers, are not random; rather, they are so powerful that they connect a great number of Web servers. These nodes act as very connected hubs, that is, as places of convergence in the network or as central connections to all devices in the network. When cyberterrorists know how to disrupt these nodes, the Internet will essentially be broken down into isolated parts (Ball, 2000). Failure of random nodes might have extremely little impact on a scale-free network's connectivity or survival, but cyber attacks on network hubs will not only completely destroy the Internet; they will also make the Internet unusable until repaired. Cyber attacks can be terminal as cyberterrorists would mainly target the routers and servers that provide the most connections to the rest of the network. Connectivity is maintained by a few highly connected nodes, that is, hubs. The destruction of only 5-15%

of these hubs will effectively disable the Internet (Faloutsos, Faloutsos, & Faloutsos, 1999; Matlis, 2002). Albert, Jeong, and Barabasi (2000) claim that the destruction of just 4% of these hubs will destroy the Internet. No matter what the exact figure is, the percentage is still small and should these hubs be targeted, they will make the Internet break into many isolated fragments.

As one can see, a cyber attack, in which node failures are not random but are the result of deliberate harm, if directed at hubs, will make the Internet fail catastrophically (Matlis, 2002). Eliminate the very connected nodes and the scale-free network will stop functioning. What this all boils down to saying is that with respect to cyber attacks the critical infrastructures, whether the nodes on the network are randomly distributed or are scale-free makes a huge difference (Matlis, 2002). Yet, if the cyberterrorist is more than an amateur, and if he or she is armed with a map of a scale-free network, he or she could strategically focus their cyber attack(s) on the few very connected nodes. Destroying just a few of these could knock out virtually all flow of or access to information for other Web users, which, in turn, would disintegrate the webs rapidly into isolated fragments (Ball, 2000). This is the Achilles' heel of the Internet (Albert, Jeong, & Barabasi, 2000). For this reason, protection against cyberterrorism needs to be concentrated on making key nodes or hubs invulnerable (Ball, 2000).

Truly, a full understanding that the scale-free network that makes up the Internet is fragile is vital to Internet security. The Internet is simply too vulnerable to attacks that use malicious software programs. The same Albert, Jeong, and Barabasi (2000) present us with a clever analogy when they claim that the network of nodes of the Internet can be compared to the network of airports in the United States. Most American airports are

small and would not disrupt the system too much if they were shut down. Yet, airports in cities like New York, Los Angeles, or Atlanta are so indispensable to the country that closing them would disastrously affect traffic (Albert, Jeong, & Barabasi, 2000).

Now, social network theory can be applied in exactly the same way to computer security. In the United States, most nuclear, water, electric, gas, telephone, data, transportation, and distribution systems are scale-free networks just like the Internet and they rely heavily on computer systems. This also means that, in order to function, they must be very dependent on highly connected nodes or hubs. Cyber attackers already know it. For this reason, these highly connected nodes or hubs need to be protected.

Social Network Theory Applied to Cyberterrorist Networks

Now that we know how the Internet is mapped from a social network perspective, and what the dangers are if the hubs are destroyed, let us focus on how networks of cyberterrorists function. Applying social network theory to the study of cyberterrorist networks is the first step to understanding the structure of their networks. While most conventional terrorist networks today tend to be scale-free networks (Robb, 2004), it is difficult to determine whether or not networks of cyberterrorists are scale-free. No empirical research on social networks of cyberterrorists has been published in a scholarly journal so far. I, the researcher, have found, based on the data that I collected, how social networks of cyberterrorists operate and whether or not their networks are scale-free.

A scale-free network obeys a power law distribution in the number of connections among nodes on the network (Pastor-Satorras & Vespignani, 2001). While some few nodes display extremely high connectivity (essentially scale-free), the vast majority of nodes are fairly poorly connected (Barabasi & Bonabeau, 2003). Yet, from the literature

on cyberterrorism (i.e., Dunnigan, 2003, Mitnick & Simon, 2002; Schwartau, 1996; Zepp, 1999), it appears that all cyberterrorists can be highly connected when they feel they need to. Cyberterrorists do not meet in the physical realm as conventional terrorists do. Yet, cyberterrorists still need a "location" where they can meet, share ideas, swap insights, exchange tools and software programs, all of which provide the means, knowledge, and motivations they need to wreak havoc against Internet and computer networks.

One of these important locations is the chat room. Indeed, cyberterrorists use the Internet to communicate with each other and, among the many Internet locations where they can meet, the chat room is the one they need the most (Zepp, 1999). A chat room can be used as a hub by cyberterrorists; it is a central location in the Internet network that has a large number of highly connected nodes. Put in layperson's terms, it is a service given by Internet providers that allows Web users worldwide to communicate. Communication in the chat room is done via Internet Relay Chats (IRCs). There are countless chat rooms where cyberterrorists can communicate and network among each other. Some are, of course, more important than others. In these chat rooms, a cyberterrorist can simply ask another how to conduct an attack and get almost instant feedback. This really enables the cyberterrorist not to waste time searching what they need on the World Wide Web or through newsgroups (Zepp, 1999).

So, the chat room is like a hub, a central location with a vast number of highly connected nodes. Therefore, the "scale-free network" theory can be applied in this very context. The larger the chat room – that is, the hub – has been in place, the greater the number of links to it. By the same token, the greater the capacity of the hub, the faster its

growth. Yet, cyberterrorist network hubs cannot be identified based on the number of links alone. Hubs vary in value depending on multiple vectors such as depth of connections, frequency of contact (which may indicate that the individual is a conduit for information flow rather than a resource), and duration of links (which is tied to the importance of that individuals skill set to ongoing operations of cells that they connect to).

Of equal relevance is the fact that cyberterrorists operate in an "all-channel" type of network, as it was previously explained (see Bavelas, 1950; Leavitt, 1951). The "all-channel" network is a network where all dispersed nodes can be interlinked for simultaneous dissemination of information and instant coordination (Barabasi, 2002). This is precisely how the chat room works: simultaneous dissemination of information and immediate coordination. The chat room is the perfect example of an Internet hub because it has decentralized command and control, as well as extremely fast communication flow between numerous nodes in the network. The main corollary thereof is that geography and location in the network are not the primary factors that determine connections among cyberterrorists. Rather, in a scale-free system like the chat room, Web users connect to well-connected others. For this reason, chat rooms, some of which become even bigger and more attractive to cyberterrorists, can best be explained by social network theory.

Now that we know social network theory, its definition, its main components, its origins, its application to the Internet and to computer security, and what cyberterrorist networks are, let us proceed to use social network theory in comparative analysis between terrorist networks of Antiquity and cyberterrorist networks today.

A Comparative Analysis of Terrorist Networks in Antiquity and Cyberterrorist Networks Today

This section is a comparative analysis of terrorist networks in Antiquity and cyberterrorist networks today. Particularly studied is the comparison between the social network of the Jewish Revolt in 66-73 CE and the cyberterrorist attacks during the Kosovo war in 1999. The Revolt in 66-73 CE, also known as "the First Revolt," was propelled by a social network of terrorists, of which the main group was the Zealots. Other groups joined them later. The Kosovo conflict saw the rise of the first major Internet war where malicious independent hackers targeted NATO and US government Web sites. The analysis is based on social network theory because it embodies a particular theoretical orientation towards the structure of terrorist networks. It also enables the author to make the point that social network theory is the best theory that can be used to demonstrate that cyberterrorist networks resemble networks in Antiquity in some ways, and differ from them in many other ways. The ultimate goal is to bridge the gap between theory and practice. An important conclusion from the analysis is that the centrality of the Zealots during the Jewish Revolt exemplifies the measure of the prominence of the "star" or "wheel" network. In other words, the ties that the Zealots have with other factions make them prominent because they are "particularly visible to the other actors in the network" (Wasserman & Faust, 1994, p. 172). What is also relevant is that the relations among the groups were nondirectional (Wasserman & Faust, 1994). After the analysis of the Jewish revolt, I provide an analogy with the cyberterrorism incident over the Kosovo conflict. What was shown was that

cyberterrorist networks follow a pattern of the all-channel network, where all the nodes can connect with any other node, without the fear of being caught.

This section starts with an extensive literature review. Drawing on a description of terrorism in Antiquity and what their networks looked like, the point is made that the current shape of cyberterrorism casts a new light on the examination of terrorism in Antiquity. In fact, based on six factors, many analogies can be made between cyberterrorist networks in this day and age and terrorist networks among the Ancients. Those factors include (1) similar terrorist motivations, (2) similar illegal money-making, (3) similar end result: fear, (4) similar patterns of communication, (5) similar connections and kinship webs, and (6) similar obstacles. The conclusion of the section is to not only compare the similarities between the two types of networks, but also the many differences that exist. A cyberterrorist network is a postmodern type of network, where no leadership is needed, no center exists, and where communication is ultra flexible and quasi limitless. As opposed to those Ancient hierarchical structures that were vertically designed, cyberterrorist organizations are actually not *organizations*. They do not exhibit an intrinsically "group" or "design" nature.

Terrorist Networks in Antiquity

Terrorist networks, for the purpose of intimidating or destabilizing entire peoples, regimes, or systems, have existed from the days of Antiquity (Anderson & Sloan, 2002b). In fact, networking is a strategy that has long been used to reach political, religious, economical, or social goals. Nevertheless, the historical reality of terrorism in a certain period and in a certain place is not easy to determine. One of the reasons is that the legal description of particular forms of behavior of people informs much about the attitudes

and expectations of the state, but not about the activities and motivation of criminals (Mitchell, 1998), or extremist groups. The imposition of blame takes the form of labeling (Jones, 1964). Some acts and their agents are labeled "criminal," others are not. This is why it is deemed necessary and beneficial to characterize what a terrorist was in Antiquity.

What Was a Terrorist in Antiquity?

Terrorism is as old as the human discovery that people can network into social groups. Since the rise of barbarous tribes that conquered agricultural communities and expelled them from the land (i.e., to live in walled cities), terror has been a powerful weapon in humans' efforts to achieve domination (Baring & Cashford, 1991; Saksena, 1985). In Antiquity, terrorists – although a term that did not exist until 1793, the tragic period that followed the French revolution – were those who were hunted down by the Roman and Greek states (Horsley, 1986), as well as territories in the Middle East (Farmer, 1956), for political or religious reasons.

Pre-state societies generally did not have an idea of "crime" (Roberts, 1979). They considered torts committed against a member of that society as an issue for dispute-solving, rather than the penalization of one side by an external body (Burkert, 1983; Girard, 1977; Mair, 1962; Roberts, 1979). Yet, in Antiquity, the conception of violent "crime," or what would be "terrorism" today, came to the forefront. When it was not violence produced by the state, but delivered by other agencies (i.e., rebels in early central Italy of the sixth and fifth centuries BCE) (Rawlings, 1998), the criteria defining terrorists were imposed by Greek and Roman power-holders who decided to place them beyond the pale of civilized society. Terrorist actions extended across a spectrum from

killing political figures "to regional insurrections and the bids for power of would-be emperors" (Mitchell, 1998, p. 157). The illegitimacy of terrorism and all forms of banditry was the perfect correlate of the legitimacy of the Mediterranean empires. The codified law of the Roman Empire, for instance, was able to place rebels in a category of literal outlaws, enemies of the state, and with absolutely no form of legal recognition (Mitchell, 1998). More importantly, they were identified not merely as "enemies of the state," but also as those who belonged to society in conflict, divided from one another by class, by deviant political systems or by primitive geographical conditions (Mitchell, 1998).

In line with these contentions, the term "reapers of terror" (and all its related forms) was not in normal usage a self-descriptor adopted by terrorists themselves, but a sticker attached to them by the state, as well as by their victims' families, potential victims, and supporters from other states, who viewed them as spreading dismay, fear, and panic. Terrorists were those sufficiently alienated from the "order" to take violent action against the local elites and their property (Hopwood, 1998). Usually, they were organized criminal gangs, a.k.a. *ergasterion* (in the singular), that is, "workshop of violence" (Davidson, 1997), or "workshop of offenders" (Fisher, 1998). They were engaged in assassination, kidnapping, fraud, either in the countryside or in the urban areas (Fisher, 1998). Some of them were called *latrones* (bandits), others were called *kakourgoi* (wrongdoers) and *poneroi* (villains), all of whom had a perverse nature to be in constant rebellion (Hopwood, 1998). Those hardcore rebels and violent objectors to the state were typically headquartered in mountains. From these territories, they launched their attacks on the plain and its cities (Hopwood, 1998).

Equally, important, terrorists in Antiquity were also "semi-professionals" who expected some reward. They were typically independent mercenaries who considered themselves free. They were armed retainers drawn from the same source as those labeled as illegitimate, freelance users of force (Hopwood, 1998). Terrorism on a small scale became terrorism on a national scale when some of them took their family interests into the foreign-policy arena.

What Did Terrorist Networks in Antiquity Look Like?

As Hopwood (1998) nicely puts it, these "part-time deviants" needed organization. Organized terrorism tended to gain the legitimacy of official policy, particularly when aimed at external targets, such as neighboring polities or their prominent citizens (Rawlings, 1998). Terrorism in Antiquity also involved careful network planning; it was made of informal, loosely structured open networks, usually divided into small fragmented, and ephemeral enterprises (Potter, 1994). The habits and the movements of the targets were watched by one group, weapons were procured by another group, and transport as well as safe housing was provided by either network cells or private owners interested in terrorist activities.

Because each terrorist group had its own private intelligence network, no one group would have created a single central intelligence organization that might fall into the hands of a rival faction. Part of the reason was that small groups sometimes plotted against each other (Fisher, 1992). The power and status of these terrorists was measured by their ability to attempt to out-do members of rival states or communities. Those groups were "competing interest groups of individuals who may well have used their personal supporters and a range of methods for their own advancement" (Rawlings, 1998,

p. 99). As such, while conflict and violence were ever-present in the network among two or more factions, the balance between autonomy and domination was most often mediated by personalized links between leaders or leading representatives of those groups (Mitchell, 1998).

The aristocratic families of early Greece shared similar characteristics with terrorist networks in that they resembled Mafia-like criminal gangs. They were small, closely knit groups that were composed of the same kith (Laqueur, 1999b). They committed killings for political and economical motives. Killing was actually the first resort, as they were impatient for quick results. They gathered wealth by violent, deceitful, and otherwise illegitimate means (Wees, 1998b). They were also difficult to infiltrate in that they were well organized, dedicated to aggressive material goals, and relentlessly inclined to flourishing their economic enterprises. Spying, plotting, and informing seemed to be, at least at times, organizationally complex affairs (Berdan, 1998). Networked groups needed a safe location where they could plan their actions with minimal risks involved. As Fisher (1998) explains it, they would congregate in

> an establishment where friends and associates might choose to regularly meet, if necessary in relative secrecy (perhaps under the front of a retail business), and in a "workshop" for a specific group of criminals, and hence an organized criminal network with an identifiable base (p. 55).

A rarely mentioned example of such networked terrorism is the chaotic and violent practice of terror by revolutionaries in the area of Taurus, southern Anatolia. In that area, terrorists were responsible for threats to society which fell short of warfare, that is, organized interstate violence, but which were more than merely individual and random

acts of criminal behavior (Mitchell, 1998). They were groups that reached the peak of their power and whose disastrous energies had to be checked by an authority powerful enough to enforce law and order on its members (Whitby, 1998). They networked with others in order to commit horrible killings as well as upper-class crimes against property (Fisher, 1992). Likewise, in other ancient societies, such as the ancient Aztec society, multiple actors were involved in similar abominable networks. For instance, any bribe-taker would network with a bribe-giver (that is, stolen goods had to be obtained and passed from person to person) (Berdan, 1998), and some acts of killing required the organization of more than one perpetrator.

Another important consideration of terrorism in Antiquity was their networks of "patronage." Indeed, not only were clans of terror highly stratified, but they also harbored extra-legal and violent forms of patronage (Zehr, 1978). In fact, patronage should be considered a form of treason or improper collaboration. It implied that the more personal the relationship, the less expensive, overtaxing, and demanding the "contract." The verbal agreements on which these contracts were based were followed for the sake of "friendship" and involved the exchange of services and favors (Blok, 1974). Patronage was practiced by hierarchical, Mafia-like organizations based on *gentes*, or clans, often exploiting relationships between "perpetrators" of terror and "sellers" of terror, like patron-client relationships (Rawlings, 1998). Through patronage, clans provided a network of resources and contacts (Rawlings, 1998). In many societies, patronage was vital to maintaining a degree of social harmony (Silverman, 1977; Wees, 1998a). Yet, the problem was that patronage was also synonym with harboring terrorists. There was much legislation concerning the harboring of terrorists on estates which were taken together

with laws directed against those promoting acts such as "fencing" properties. These were usually interpreted as efforts to close off potential support for bandits, and thereby render them more isolated (Shaw, 1984).

The Boukoloi

The rebellion of the Boukoloi is a very good example of terrorist networks in Antiquity. The Boukoloi (pronounced *vookolee* in Modern Greek) lived across the central and northern Egyptian Delta. The Delta is "a huge flood-plain formed by the division of the Nile into its various branches just to the north of modern Cairo" (Alston, 1998, p. 137). The Delta consisted of a number of urban areas, surrounded by a number of villages or small settlements (Brink, 1987, 1988). The Boukoloi had to network in order to survive. A bloodthirsty group living in a meandering of lakes and marshes, they were considered what we would call today "terrorists" by various peoples such as the Romans (Alston, 1995). One of the areas, Mareotis, where they possibly lived, was an area of terrorist activity, led by different tribes. The networking between the Boukoloi and such groups was complex, but, apparently, they could only survive by exchanging foods and goods from the agriculture. The Boukoloi killed a lot of Romans in the Egyptian Delta in the 170s BCE; they infringed upon local security measures and intimidated the Syrian forces, possibly helped by forces from Arabia (Alston, 1998). More importantly, the Boukoloi were also considered "an enemy within," "a source of potential disruption and criminality throughout the Delta" (Alston, 1998, p. 142) and "outlaws" (p. 144). They were enemies who were stigmatized. Becoming Boukoloi was becoming "other."

With the Boukoloi, we observe the account of a rebellious group that is characteristic of terrorist network activity. Terrorism here appears to be a social

phenomenon. Their rebellion was caused by a combination of ruthless and uncompassionate government, drastic social conditions, economic difficulties, and escape from oppressive Roman taxation (Alston, 1998). In these circumstances, the state had trouble gathering forces to put down their rebellion. As one can see, the Boukoloi really resemble terrorist groups in modern banditry and guerrilla warfare. What we have here is "rural banditry stemming from within the settled community and exacerbated by economic problems" (Alston, 1998, p. 144).

The Comparative Analysis

The current shape of cyberterrorism casts a new light on the examination of terrorism in Antiquity. In fact, based on six factors, many analogies can be drawn between cyberterrorist networks in this day and age and terrorist networks among the Ancients. Those factors include (1) similar terrorist motivations, (2) similar illegal money-making, (3) similar end result: fear, (4) similar patterns of communication, (5) similar connections and kinship webs, and (6) similar obstacles.

Similar Terrorist Motivations

Terrorist matters are quite volatile and unexpected, yet motivation has always been the key (Sloan, 1995). Four categories of motivations have been identified: (1) political ambitions, (2) economic deprivations, (3) crime for crime's sake, and (4) the need for publicity. The first category of motivation is political (Fisher, 1998). The word "political" here is used as a broad term that comprises "religious" and "social." Political murder appears in the earliest annals of humankind (Laqueur, 1999b). Political oppression and social idealism are generally mentioned as the root causes of terrorism.

As Schweitzer (2002) puts it, terrorism in Antiquity was primarily based on political motivation. It was mainly,

> premeditated violence directed against both armies and general populations characterized the actions of rebellious forces, seeking new political orders, that destroyed the early civilizations of the Dark Ages, triggered the decline of the Egyptian Old Kingdom, brought down the states of Greece and Crete, and toppled the Roman Empire (p. 25).

In line with these contentions, the Zealots felt the need for radical political change as well. The Zealots were a Jewish extremist group of the 1st century CE involved in fierce terrorist acts during the Roman Empire (Smith, 1971); they refused that Jews pay taxes to Rome and did not acknowledge the authority of the Roman emperor. Their closest "co-workers" were called the Sicarii. *Sicarii* is a word derived from the word *sica*, a short sword used to attack their targets (Laqueur, 1999a). They held out against Rome for six years before choosing mass suicide over surrender in Masada in 73 CE (Ben-Yehuda, 1998), when the second Temple was burned down and the Jewish state ceased to exist (Gray, 1993). They were convinced that political change could come only through "propaganda of the deed" (Laqueur, 1999b). Their hate and fanaticism were so deeply ingrained that they were willing to use any weapon to strike Roman soldiers (who had by military force occupied the Holy Land and the City of David), Jewish "collaborators" who favored these Romans (i.e., the Pharisees), and Jewish moderates in Palestine who had succumbed to Hellenistic influences. This is why they adopted terrorism as their main form of struggle. Their most basic motive was that all means were justified to attain political and religious liberation.

Political ambition and commitment are also part of the agenda of cyberterrorists (Denning, 2001). Sabotage of electronic networks, power grids, and other elements of a nation's infrastructure may not be solely aimed at crippling specific individuals or groups (Schweitzer, 2002). In some cases, these cyberterrorist acts are also aimed at achieving political goals. Nevertheless, they may prove to be alarmingly effective in the disintegration of institutions, thereby disrupting thousands, indeed millions of lives (Schweitzer, 2002). Governments also use cyberterrorists as propagandists, or even soldiers. Their intent is to overthrow specific political systems. During the conflict over Kosovo, government actors and nonactors were dangerous hackers because they launched email bombs against other governments' computers, taking over their web sites, deluging viruses, and even coordinating actions with fellow conspirators (Denning, 2001).

Such government-sponsored terrorism is an old practice. Terrorism in Antiquity "found its sponsors in the hallowed halls of officialdom, in the entity known as government" (Collins, 2002, p. 3). The motivation was also to create social engineering stratagems to transform terrorists into conscienceless machines (Collins, 2002). History has recorded that, up to this day, most terrorists have been young, the great majority being male, especially for right-wing movements. If, however, the state was to "own" violence, it had not only to apportion redress, but also to impose blame. To this extent, it is fair to say that some of the terrorist acts in Antiquity were a result of state-formation. Today, rogue governments supply the technological know-how to cyberterrorists "either by political design or for commercial gain" (Laqueur, 1999b). When cyberterrorists fight anonymously against political opponents, they try to hide their tracks. For instance, the

damaging Code Red virus of 2001 came from China (Dunnigan, 2003). Foreign experts even believed the Chinese government backed it up, but China denied any responsibility.

A second category of motivation is economical. Terrorism has oftentimes been a movement against the rich. Aristotle already found connections between poverty and crime (Fisher, 1998). In this sense, terrorist acts help us make sense of the forms of oppression among certain groups. We saw in the previous section that the Boukoloi rebelled against the Romans mainly for economical reasons: they were suffering from drastic social conditions, financial difficulties, and arduous Roman taxation (Alston, 1998). To cite another example, Herod the Great accumulated immense wealth by acquiring Judea and building Caesarea, an artificial harbor on the eastern Mediterranean coast. His income was about 40 million denarii per year, which amounted to approximately one tenth of the estimated total budget of the Roman Empire (Starr, 1982). This, among other reasons, created an economic upturn in Judea and led different extremist groups to revolt and commit crimes against the power-holders. Today, terrorist crimes can also be perpetrated for financial reasons. It is not unusual to learn that viruses and other damaging Internet-based weapons have been sent by cyberterrorists who live in countries that are poor, sometimes extremely poor. Pakistan, considered a third-world country by the United Nations, has a large population of skilled programmers and Internet explorers (Dunnigan, 2003) who are ready to support the Taliban and Al Qaeda in return for all kinds of favors (some of them are financial rewards). One of their tasks is to cause economic damage to their enemies.

A third terrorist motivation is criminal in character. In this case, terrorists commit crimes for crime's sake, not based on shared values. The rise of small sectarian groups in

Antiquity showed that they lacked clear political and economical agendas. Their goal was to destroy infrastructures or, in some cases, humankind (Laqueur, 1999b). Terrorism was an undeclared, but open war; their motivation was to hurt. Emerging from a temple's doorway, after studying a target's routine every night, they knew the exact moment to strike. This is how some Roman emperors were assassinated. Some of the cyberterrorists have the same goal and tactic. As Mansfield (2000) puts it, "it's usually contempt. Most virus writers and hackers feel left out of the mainstream society… money isn't their primary motivation in most cases" (p. 20). Indignation and a wish for revenge (for transgressions against them, whether real or imagined) can be their prime motivations. Cyberterrorists are even branded as "the intellectual version of those spray-painting teenagers" (Mansfield, 2000, p. 40). After all, what types of crime do most cyberterrorist acts entail? Breaking into somebody else's computer network, corrupting data, damaging files, or even changing a product's dosage (in a hospital) that relies solely upon an electronic device. Hackers whose sole purpose is to "destroy" have their own nickname. They are called "black hats." "Black hats," or "crackers," are out to do damage (Mansfield, 2000). A good analogy could be made with criminals in Antiquity: *kakourgoi* (wrongdoers) and *poneroi* (villains) wore a sort of dark hat when they were out to commit a murder. No matter what, the goal of cyberterrorists is criminal. It is even more than that; it is insidious. What makes the United States so powerful is not only its economy, values, and people, it is also the hardware, software, and electronic infrastructure upon which the country's development and growth rest (Verton, 2003a). Cyberterrorists know that. Their attacks inflict heavy symbolic injuries on this nation.

A last category of motivation is the need for publicity. Classic terrorism is "propaganda by deed." Terrorism is news (Laqueur, 1999b). Terrorists need publicity. In 66-73 century CE, the Zealots sent their members to places where they would slit the throats of Romans (and those who favored them) in public. In fact, they employed very visible and visual acts of murder against Roman legionnaires or Jewish citizens they saw as guilty of apostasy or treason. Their killings frequently took place in broad daylight and in front of witnesses, in crowded market places or on feast days. The reason the Zealots committed those acts so blatantly was to show themselves who they were (Roth, 1959). Their ultimate goal was to send a message to the Roman authorities and those they called "Jewish traitors."

Later, this tactic was repeated by subsequent generations of terrorists. Not surprisingly, cyberterrorists also try to gain publicity. As such, not only do they attempt to find flaws that exist in private and federal computers (and other Internet-based and electronic systems), they also show their targets that they are what they want to be, that is, computer geniuses who, after having sold their souls to a cause for diverse reasons, like to catch computer users by surprise. What it boils down to saying is that cyberterrorism, just like terrorism, is inherently a communicative process (O'Hair & Heath, 2005). Cyberterrorism can be promoted via the Internet, a public communication channel. As such, it is publicized and perpetuated through new media communication. Therefore, it is essentially through semiotics and the exploitation of new media that cyberterrorists find success in accomplishing their primary goals. In 2002, a group of cyberterrorists, known as the World Fantabulous Defacers (WFD), hacked into the official Web site of Israeli Prime Minister Ariel Sharon and defaced it. As a title, they

wrote, “The Face of the World’s Biggest Murderer.” At the bottom of the Web site, they left a message with the signature of the group. The WFD’s hacking into Sharon’s official Web site stands out as one example of a cyberterrorist group that was in a position to do far more damage and perhaps cause a national crisis in Israel (Verton, 2003a). This example shows that cyberterrorism is a semiotic act that is a message, a symbol, and a new media image. Clearly, by gaining such visibility – and sometimes they can infiltrate hundreds of thousands of computers – terrorists are able to spread terror in cyberspace and evoke fear. Of course, they would never divulge their real identity. Besides, it is impossible to categorize a whole group of people with a single character portrait (Mansfield, 2000). Some merely seek publicity to show their excitement and power, although they can cause a lot of ravage in the process. The Zealots would also kill people in broad daylight for “publicity” purposes, but they would still cover their heads and not reveal who they were as individuals.

As one can see, for two millennia terrorists of all sorts have committed their acts based on four motivations, that is, political, economical, merely criminal, or for publicity purposes. Those last five pages are important because they lead to the premise that motivations are what unite people with the same convictions, the same goals, people who have a common denominator. Given this, they are ready to move on and join forces by creating local groups that will spread out like mushrooms. This is how terrorist networks emerge. The motivation to kill leads to propagation of killing. And what is the best way to propagate? The best way to propagate is to network. As we will see later, cyberterrorists divide themselves in smaller cyberterrorist factions, like it was in Antiquity. Sometimes, they act alone.

Similar Illegal Money-Making

Among the similarities that can be identified between terrorist networks in Antiquity and cyberterrorist networks today, it should be noted that they both engage in illegal money-making undertakings. This yearning for obtaining funds is significant as an aim of terrorist acts, sometimes as a transitional step to finance ambitious plots, to back expanded operations, or even to satisfy personal greed (Sloan, 1995). We saw earlier that networks of patronage were plentiful in Antiquity. Through patronage, clans provided a network of resources and contacts (Rawlings, 1998). This form of illegal money-making was practiced by organizations based on *gentes*, or clans, often exploiting relationships between "perpetrators" of terror and "sellers" of terror, like patron-client relationships (Rawlings, 1998). As such, it meant that terrorists would be harbored by "patrons" in order to yield "revenue."

Similarly, in Ancient Greece, organized terrorist activity was also determined by the need to obtain money unjustly. Crimes, Fisher (1998) notes, were committed through *philochrematia*, that is, greed and desire for money. Some of the groups to blame were collections of rich elite men accepting large bribes from unknown parties. Of equally corrupted minds were some members of the Roman elite who used "terror" groups for money laundering. They negotiated with dangerous, extremist, and rebellious parties such as the Cilicians of Mount Taurus, or Roman Rough Cilicia, living in southern Asia Minor (Hopwood, 1998). Not all states in Antiquity considered illegal money-making a serious crime, due to an awareness of a lack of effective monitoring of currency movements. Consequently, even "respectable" citizens did not feel obligated to refrain from

networking with criminals, to report suspicious transactions, or to use any monetary instruments payable to bearers.

Two thousand years later, it seems that few of the networking practices have changed. What is very different, however, are the means used by current terrorist groups to obtain illegal funds. It is already known that governmental actors and terrorist organizations (as well as drug cartels like those in Columbia) network as "enterprises" of criminals driven by a thirst for accumulation of wealth (Schweitzer, 2002). In this regard, cyberspace also seems to open doors for the development of such "enterprises" as it [cyberspace] is a relatively simple and secure base to obtain substantial amounts of money (Laqueur, 1999b). When back in the early 1980s Internet users represented small communities where everyone knew everyone (Dunnigan, 2003), no one dared to engage in networked money laundering on the Net. Today, cyberactions are so unrestrained that terrorists can easily operate as stockbrokers, looking for the best deals. As brokers, they simply offer dirty money to the highest bidder (Andelman, 1994).

Another meaningful consideration is that cyberterrorists use e-cash, the most widespread form of currency that flows through the financial laundromats (Schweitzer, 2002). Some of their e-cash comes from wire-transfer companies. Although wire-transfer companies provide a valuable service to low communities which can now have easy access to banks, they have also served as laundering operations for terrorists (McFadden, 1997). From this, it may be inferred that wire-transfer companies make transactions and terms with cyberterrorists who, in turn, consider those companies as important constituents in their network of illegal money-making. A significant analogy can be made here with the networks of patronage in Antiquity, where clans and "patrons" provided a

network of resources and contacts (Rawlings, 1998) to terrorists by harboring them and using them as "members of the workforce."

In the same train of thought, the immense growth of international trade and business transactions also leads to ever-increasing automation; this means less personal interaction with customers (Schweitzer, 2002). For instance, the European Union Bank (EUB), "sited" in Antigua, was the first full-service Internet bank. As it operated within a banking and Internet free-trade zone, anonymity was guaranteed and no one could trace any transaction. This was already the case in some governmental practices in Antiquity where, as mentioned earlier, no one felt obligated to report suspicious transactions or to use any monetary instruments payable to bearers (as such, nothing was traceable). The European Union Bank's Web site disappeared in 1997, but until then the bank was exempt from regulation and not subject to inspection (Farah, 1997). The bank is thought to have laundered important sums of money from Russian cyberterrorists.

A last meaningful similarity is the desire to commit a terrorist act or kill for the purpose of obtaining funds. In Ancient Greece, some crimes were committed through *philochrematia*, that is, greed and desire for money (Fisher, 1998). Earning their financial keep is also a motive that cyberterrorists share with their Ancient counterparts. They would not hesitate to employ threats and violence. It was reported, for example, that cyberterrorists and criminal hackers from the Jihad threatened to engage in disruptive attacks to blackmail and extort funds from private sectors and commercial enterprises that have business affairs with the Israelis (Zanini & Edwards, 2001). To all appearances, cyberterrorist prime targets are financial institutions, whose networks could be hacked and delved into, and whose money and assets could be plundered. In the same process,

financial markets could be affected by the destruction of data or the transfer of phony information. Truly, cyberterrorists target those institutions that stand in their greedy trajectories to financial payoffs (Schmid, 1996). This is why businesses around the world are spending billions of dollars in an attempt to make their bookkeeping and inventory control systems untouchable, their transaction billings and payments, proprietary information, and personnel records safe (Medd, 1997).

Similar End Result: Fear

Acts of extreme violence have always been abominable. As the Zealots considered themselves the elite of a new world order, cyberterrorists see themselves as "the elite of a new electronic order" (Laqueur, 1999b, p. 77). The ultimate consequence of terrorism is fear. Terrorists are part of a movement of a certain period. Understandably, the public is fearful of the secret and mysterious character of those who would commit such acts, sensing that any actions could occur at any time (Schweitzer, 2002), even when it is the least expected. In some cases, it even causes as much havoc and detriment as the terrorist act itself: panic, the chaotic response from the population that is likely to occur when a terrorist act is committed or the threat exists that there may be such an act. True panic is contagious, a crowd phenomenon, not an individual one (Laqueur, 1999b). As Laqueur (1999b) continues,

> the consequences of a mass panic in both material and human terms can be huge; they can lead to a paralysis of normal life, epidemics, post-traumatic stress, and tremendous anxiety, especially if the nature and extent of the danger remains unknown (p. 272).

Let us take the example of the Zealots. Their terrorist actions caused trauma and turned Roman citizens (and Jewish sympathizers to the Romans) breathless, speechless, or motionless. They became paralyzed. More importantly, the Zealots' revolt influenced subsequent revolts in Mediterranean and Middle-Eastern history, such as the murderous crusade led by the Assassins (11^{th}-13^{th} centuries) against those who would not conform to their religious beliefs (Anderson & Sloan, 2002b). The sum of their crimes resulted in far-reaching dismay and desolation, especially after the Romans destroyed the Temple in Jerusalem. Around that time, assassination of politicians was an appraised tactic adopted by terrorists to send chills down the spine of the population.

These goals were achieved to a degree that cyberterrorists, who would instantly relate to them, can certainly aspire to. In 2001, for instance, just three viruses caused over 60 % of the cyberterrorist attacks reported that year (Dunnigan, 2003). That was only three viruses. Now let us say that a network of several cyberterrorist groups decides to join forces on one single devilish project. All the hopes, all the intergroup cooperation, all the energy, all the technology, all the time, and all the money they have will be concentrated on that particular project in an attempt to destroy an important infrastructure of our nation. Imagine the following situation: they send hundreds of computer viruses, plus damaging software, trapdoors, Trojan horses, worms, and spy chips. What would the end result be? Fear. Not that defense against cyberterrorists is difficult and in many cases impossible (Laqueur, 1999b), but even if the project fails, its magnitude and the impact it has on the potential targets are sufficient for cyberterrorists to get their message out. As seen earlier, one of their motives is to receive publicity; it is a vital component of terrorist strategy that seeks to undermine the will of an enemy. When terrorists publicize, they

justify their crimes to a global audience. The media also contributes to heightened panic on the part of the population. Most developed societies have numerous media outlets, and the more developed a society, the more vulnerable it is to the consequences of hysteria.

The word "network" itself can be frightening to those who are aware of the potential harmful effects of "scattered terrorism." Already in Antiquity terrorist groups relied on networks to deceive their targets. As such, they created the illusion of invincible numbers by hiding in wide areas such as mountains. The Cilicians are a good example of a terrorist group that inflicted such fright upon the population. From the 1st to the 4th centuries CE, the Cilicians were peasants who became extremist insurgents against the Roman order. Organized into cells that were dispersed all over the ridges of Mount Taurus, they came down the mountains in widely separated groups and used violent force against townsfolk (Hopwood, 1998). As such, they struck fear among farmers, shipowners, and merchants. Other terrorist groups in Antiquity organized their activities around speed. They used rapid group maneuvers, making them look more numerous than they really were. All these actions caused a serious weakness in their enemy's psyche, and the terrorists were feared wherever they went. Today, cyberterrorists might not even have to network with one another in order to engage in their activities. It may just be one or two masters in cyberspace with evil intentions. Society's reactions to an Internet-mediated attack, nevertheless, might be that the people who are to blame are members of a vast cyberterrorist network, while in reality it was only one or two individuals. Cyberspace has contributed to the fear of the unknown because nobody can be sure about what is "out there." While ancient activities led to crises which, in turn, led to *coups d'état* (Wees, 1998b), cyberterrorist activities lead to panic, which, in turn, *should* lead

power-holders to take more measures. Yet, if security measures are insufficiently taken, the end result will eventually be a weakness of our psyche.

Another factor that leads to fear is the meticulous selection of targets by terrorists. In Antiquity, some of the exposed victims of terrorists were actually important figures that criminals wanted: politicians with "superior power," vastly-expanding influence, notable personalities, and even rich business owners. In the 5th century BCE, for example, networks of "semi-professional" rebels assassinated Ephialtes (c. 460 BCE) and mutilated Hermai (Fisher, 1998). In drawing a parallel here, it is interesting to mention that some of the most vulnerable victims of cyberterrorists are those owning PCs that also have "superior power" (richly supplied), as well as fast and always-on connections (cable modem and DSL). These computers are abundant, not always protected, and just the type of machines cyberterrorists like to take over (Dunnigan, 2003).

The point made here is that terrorism leads to "smarter crime" (Laqueur, 1999b). Whether it is through speed, through an illusion of invincible numbers, through the assassination of important figures, or through independence and invisibility in cyberspace, terrorist networks in Antiquity and cyberterrorist networks today share the common fact that, in order to strike fear and catch targets by surprise, new and radically different offensive techniques have been developed.

The main element of their offensive technique is the development of new "weaponry." Not only were the Zealots distinguished by strict discipline and obedience, but they also had the absolutely best equipment. One of their allies' weapons was the *sica*, a small dagger, so small that it could be hidden and pulled over in a second to cut a throat. With the spread of metals technology, terrorists in Antiquity were able to arm

themselves to such a degree that they could easily wreak havoc on both the ruling elites and the commoners (Johnson, 1990). As one can imagine, cyberterrorists also have powerful equipment. Yet, no one is sure whether they can match US homeland security (Dunnigan, 2003). From what we know, however, high-tech damaging software, cracking tools, and encryption programs are among many of the cyberterrorists' tools (Schweitzer, 2002). Of more concern is the damage terrorists might inflict upon the electronic underpinnings of many American institutions, as they save colossal funds for cybersabotage. In 1995, there were already over 250,000 hacking attempts, modifications of data, and destruction of software and information bases. Attacks against emergency response systems, our hospital infrastructures, and educational and commercial institutions that are contingent upon computer-based networks may soon become real. Calculated short circuits and more serious knots in these electronic webs could bring the dynamism of our daily lives as we now know it to a screeching halt, to the delight of cyberterrorists waiting to maul technically paralyzed victims (Schweitzer, 2002).

Similar Patterns of Communication

Throughout human history, communication has always been a crucial weapon for attacking targets (Dunnigan, 2003). Across the centuries, the ability to orally convey huge amounts of complex information, and later put it in writing, allowed humans to develop particular patterns of communication. In Antiquity, terrorists were already aware that managing networks of criminals required new forms of communication, such as long-range communication. The result, however, was that authorities could rarely intercept or monitor terrorist communication. For instance, the Zealots used a number of signals to identify one another and communicate with each other (i.e., private gestures

and secret handshakes). They also communicated agendas with the help of word of mouth. Since there were no microphones at that time and since most of the Zealots were very familiar with the areas where they would commit their crimes, they knew they were able to communicate without Big Brother eavesdropping. Only an extreme hazard such as treason or a serious mistake on the part of the terrorists themselves would have them caught by the Roman authorities.

Additionally, what was difficult for Roman commanders, in their attempt to bust or identify the Zealots, was that communication emerged and changed according to the task at hand (Zanini & Edwards, 2001). As such, their patterns of communication were often loose, informal, and, depending on the needs of the group, marked by varying degrees of intensity. Terrorists have always been interested in studying their enemy's patterns of communication before they attacked. As such, they collected information, a lot like what intelligence service agents would do today, with the intent to relay it to the power-holders of terrorist groups who needed it as quickly as possible. Besides, for several millennia, the objective has always been to disrupt enemy communications (Dunnigan, 2003). In the past, this meant sending deceptive signals during an attack.

Deception is also part of cyberterrorism; the Internet is a powerful, cunning semiotic tool for its practice. Deception is the act of both hiding the real and showing the false. Its ultimate goal is to promote a desired outcome or to reach an end, a personal objective. In "Towards a Semiological Guerrilla Warfare," Umberto Eco (1986) already claimed that "the battle for the survival of man as a responsible being in the Communications Era is not to be won where the communication originates, but where it arrives" (p. 142). The definition of deception stresses the second party that is involved,

where the cyberterrorist is consciously trying to create deception in order to reach an end, such as defeating security measures. To defeat security measures, a cyberterrorist or any attacker must find a pattern to deceive trusted users into revealing information, or engage in disinformation (i.e., trick an unsuspecting mark) into providing them with access (Mitnick & Simon, 2002). There are, of course, other deceptive practices such as swapping gender, using other people's computers, or relying on encryption programs (Schneier, 1996; Stallings, 1998; Wayner, 1996).

Undoubtedly, new technologies have acutely facilitated communication among cyberterrorists and reduced the time for the delivery of information (Monge & Fulk, 1999). Particularly, not only does the Internet diminish the costs of this delivery of information, but it also accelerates the speed of communication and the bandwidth (Heydebrand, 1989). As explained earlier, increased terrorist speed was a tactic already employed in Antiquity to frighten the enemy or make their defense less capable. Speed can also be used to improve communication, multiplying the efficacy of cooperative or joint attacks. This became a significant impact of speed. It is the essential quality of an attack on the Internet: the more speed cyberterrorists have, the less time the defense has to respond (Dunnigan, 2003). When the environment for terrorists is rapidly changing, however, so too are the problems. For that reason, intense communication among them becomes an ongoing necessity. Communication is indispensable among individuals whose tasks are mutually dependent, in the sense that one sends or receives information or resources relevant to the other (Watts, 2003). It is not surprising, then, that the Zealots were energetically protecting their own patterns of communication by making them more

intense and effective. Similarly, protecting one's own ability to communicate is still a vital strategy for any cyberterrorist.

What comes next is the evidence that terrorists really *did* and still do operate through networks. Although terrorist networks in Antiquity were different from the ones that we know today, they still have significant elements in common with cyberterrorist networks. Emphasized here are the similarities, not the differences (those will be dealt with later). As such, the author makes a series of analogies of Ancient terrorist connections and kinship webs with those of cyberterrorists.

Similar Connections and Kinship Webs

We should think of terrorist networks not merely as "networks of information processors" (Watts, 2003, p. 273), where the role of the network is to operate large volumes of information without overloading any individual processors, but also as connections and kinship webs. "Connection" means "link," "tie," "contact," and "association." "Kinship" means "relationship," "friendship," "alliance," and, oftentimes, "dependence." All these synonyms not only imply the importance of working in webs, but they also involve a notion of trust. Terrorist networks all have similar trust patterns, as predictable as the paths by which they come together to form a stronghold. Trust can be sometimes so strong that terrorist groups – as it was the case for the Zealots – protect their vital communication flows by having their members pledge allegiance that they will commit suicide if they are caught. Among other rules imposed by terrorists is that members had to eat cyanide or cut their tongues when captured. What is also interesting is that part of the failure of Roman and Greek power-holders to dismantle terrorist groups was their inability to learn how to harness the power of their networks. Unfortunately, we

also live in a time where it is difficult to disrupt cyberterrorist networks because global key technologies themselves have become networked.

The principal task of a terrorist connection or kinship web is not production, but coordination. Coordination serves "as an information pump between the individuals whose task is production" (Watts, 2003, p. 275). All successful terrorists in Antiquity engineered social webs that distributed information. They went after as much information as possible. They not only wanted to know fundamental facts and tips (i.e., where the enemy was and who was leading them), they also looked for additional details by networking, for instance, with people working for the Senate themselves. So they were able to make good use of all this information. Anyone waging an attack on the Internet must do the same (Dunnigan, 2003). The more the cyberterrorist knows about what he or she is dealing with, the more successful he or she will be. Yet, if the cyberterrorist knows too much and if the cyberterrorist has been part of a massive cyberterrorist network, he or she could compromise the group if he or she were captured.

Now, another question pops up: how did the terrorists in Antiquity obtain vital information on their enemies? There are many answers to this question and it would take too many paragraphs to make a historical account. What is necessary to know, however, is that some terrorist groups developed connections with corrupt politicians. Yes, terrorism-driven corruption is very old. As explained by Blok (1979), it was not unusual to see the political elite developing connections with the "evil ones." Crime involved webs of influence that linked heinous insurgents with those in positions of power in the political world. Besides, connections in the form of harboring and "fencing" were activities on the boundary between straight and Machiavellian. Such interstitial activities

became benchmarks for the negotiations between the bandits and the Roman elites in their role as law enforcers (Hopwood, 1998). Shaw (1990) reveals a consistent pattern of connections between the state-based authority of the Mediterranean lowlands and the loosely-structured, but no less capable power structure of the highlands, which focused on those in charge of eliminating targets, that is, the big men and their kinship networks.

As one can see, it is not unfair to say that, in order to be effective, part of the terrorist success depended on healthy support, or at least support by a certain segment of society. They formed hybrid organizations that were pursuing a combination of political and economic agendas. While terrorists in Antiquity were somewhat helped through their connections with people working for the Senate, the elites, or even business owners (remember "patronage"), cyberterrorists today are able to "get together" via email and Internet chat rooms. Such connections are of particularly great appeal to those also interested in pursuing a combination of political and economic agendas through Internet-mediated destruction. As such, creating malicious software has become a networked effort and, as a result, more powerful "vandalware" has come to the forefront of electronic media (Dunnigan, 2003). As Dunnigan (2003) continues,

> the Internet has enabled people of like mind and intentions to, well, network. In the past there would be small communities of programmers all over the country (and world), largely brainstorming new products and working in isolation. This changed as more software developers got an ARPANET. This ability to connect with like-minded people in far-off places was intoxicating (p. 7).

It is plain to see that the Internet, which used to be a safe haven for small communities of programmers, has become "intoxicating." It is affecting not only the

types of targets and weapons terrorists choose, but also the ways in which such groups network and structure their organizations. What is even more frightening is that many of the nasty terrorist activities are based solely on the use of the Internet, computers, and telecommunication devices. The goal is to create connections and coordinate dispersed activities (Zanini & Edwards, 2001). So, the effects of networking in cyberspace can be detrimental. Now, by being part of a virtual horde, cyberterrorists can be productive with others from remote places. No one – at least only a few – anticipated that this opportunity to create social networks on the Internet would lead terrorists to form their own worldwide connections as well (Dunnigan, 2003). What they have done is understand how the system worked and develop ways to take over. Consequences can be devastating because,

> they allow those with destruction in mind to get together… For years it was thought that the first Trojan horses and viruses, spread around on the Net to destroy people's data, were the work of demented loners. Eventually the realization came that even loners like to get together (Dunnigan, 2003, p. 8).

The rise of networked cyberterrorism is part of a more significant shift to netwar (Arquilla & Ronfeldt, 2001). Netwar involves measures taken by terrorists to create "dispersed, small groups that communicate, coordinate, and conduct their campaigns in an internetted manner" (Zanini & Edwards, 2001, p. 30).

In line with these contentions, it is essential, in order to have a good grasp of what terrorist networks in Antiquity and cyberterrorist networks share in common, to focus more on internal ties among terrorist groups or even within a terrorist group itself. As such, it might prove useful to extrapolate the point that was made a couple of paragraphs

earlier that state-based authorities were involved with the "loosely-structured" kinship networks of the Mediterranean highlands. What it means is that they were loose networks of individuals and subgroups with strategic guidance, but that nonetheless enjoyed more tactical independence (Zanini & Edwards, 2001) than soldiers of the Roman and Greek armies, shaped like strong hierarchical pyramids. Terrorist networks were also hierarchical, yet members still benefited from taking more independent measures. They "tended to work in pairs or groups, whether through the casual co-operation of friends, temporary groupings of political allies, or as part or more organized, mutually supportive, social clubs or political *hetaireiai*" (Fisher, 1998, p. 57). This was also reflected through interactions among members that were sometimes volatile (Ranstorp, 1994), but oftentimes flexible.

There is another advantage of having flexibility and ties among terrorists. Individuals with mutual agendas and goals could form subgroups, convene at a target location, carry on terrorist operations, and then subsequently terminate their relationships and redisperse (Zanini & Edwards, 2001). The Zealots, for instance, collaborated with outside groups (from regions outside of the Roman Empire) that would be considered "ad hoc" groups today. Part of this strategy to work with "outsiders" is that it is easier to punish large groups that feed off of terrorism than to deal with splinter groups that are more difficult to figure out, much less to locate (Schweitzer, 2002). Of equal relevance is the fact that in networks, as opposed to organizations that have no connections or kinship webs, terrorists are not always limited to how much work they can do. Internally, the volume of the work is conducted by self-managing teams, while external linkages compose "a constellation involving a complex network" (Monge & Fulk, 1999, p. 71) of

contributing cells. The Zealots already exemplified the notion that interactions among members were flexible and so were their tasks and workloads. Since then, it has been recorded that both internal and external ties are made possible not by bureaucratic sanction and order (like in vertically-led business corporations of far-Eastern Asia), but rather by collective norms and values, as well as reciprocal trust (Zanini & Edwards, 2001).

Whether composed of internal or external linkages, the Internet is, let us face it, a network of networks. It consists of countless interconnected networks spread around the globe. Our computers form the Internet range from huge mainframes. Yet, what is different from terrorist networks in Antiquity is that the sprawling Internet networks, of which cyberterrorists are some of the key members, have replaced hierarchical organizations (Laqueur, 1999b). Even though members of terrorist networks were somewhat loose and enjoyed more tactical independence than soldiers of the Roman and Greek armies, they were still, as mentioned above, forced to obey and to follow a strategic guidance. They had a central commander, sometimes established outside the regions where the terrorist cells were located. By extension, in the case of patronage in the Roman period, we can see some resemblance with the Italian Mafia: it is a network of connections with other violent folks, which makes the leader a friend of the friends.

More importantly, while terrorist networks can be linked by groups that consist of hundreds, if not thousands of members, some terrorist parties can be very small, sometimes consisting of just one individual (Laqueur, 1999b), such as an independent terrorist, sharing the same goals as other terrorist groups, but acting as a mercenary. History is replete with examples of independence terrorism; even Antiquity has recorded

a couple. While private smallholders liked to rely on bands of marauders and hired killers (Schweitzer, 2002) to do the bidding of bribed politicians, members of the Roman senate, or terrorist kingpins, it was not unusual that private groups had fellow politicians themselves assassinated by independent terrorists. The Zealots encouraged citizens to take a dagger and become involved in the act of committing murders, on their own, against the Romans. Some terrorist acts were also executed by lonely individuals such as Herostrat, the citizen of Ephesus, who burned the local temple (Laqueur, 1999b). Likewise, in 70 BCE, when Rome had a republican form of government, the wealthy politician Marcus Licineus Crassus, who later became Rome's Praetor, was using fire-fighting mercenaries to burn the buildings of owners who refused to sell him their land (Collins, 2002).

As it has always been, the smaller the group, the more difficult to detect (Laqueur, 1999b). Traces are even more difficult to find if it is just one terrorist "out there." Now imagine the current situation, where one of the most successful skills a cyberterrorist has learned in an attempt to master the Internet is "stealth." Surprise and getting away undetected are precious weapons for cyberterrorists (Dunnigan, 2003). Given this, they can smoothly act as malicious independent hackers propelled by technical challenge, as criminals interested in personal financial gain, or as foreign espionage agents looking to exploit information for economic, political, or military objectives (Department of Defense, 1996). They can also act as part-time terrorists: individuals who are not directly affiliated with a given terrorist organization, but who still support its agenda and use damaging software tools and instructions available at the terrorist Web site (Zanini & Edwards, 2001). As such, these part-time terrorists can be business rivals, spies, thieves,

disgruntled employees (Laqueur, 1999b), "hackers for hire," part-time "volunteers," and "script-kiddies" (comparable amateurs who rely on off-the-shelf and easy to use tools) (Zanini & Edwards, 2001).

These individuals who are technically skilled have to constantly test their tools and weapons. Although they are willing to strike targets by both disrupting and employing destructive means to further a political agenda, they still need the acumen of spies and not be detected (so they can return for more secrets later). This espionage also serves the purpose of scouting for damaging cyberwar attacks (Dunnigan, 2003). By playing the role of independent computer soldiers, it is oftentimes difficult to identify the source of the cyberterrorist act, the computer network's "weaponry," knowledge, funds, or summon to actions that are employed. They do not even need to put their lives on the line to protect the interests of others.

Similar Obstacles

In spite of all the advantages that networks offer to terrorists in general, it should be said that there have been attempts to thwart – if not destroy – the development of such networks. Looking for similar obstacles that both terrorists in Antiquity and cyberterrorists had to face, it has been found that targets will best hinder the progression of networked terrorism by protecting themselves. The best attack is defense (which seems like the opposite of what protection should be). One such defense is protection of property. Already in Ancient Greece protection of land was enforced against the threat posed by dangerous men (Fisher, 1998) to shield property even against any type of destruction. These measures were also designed to make life easier for the poorest farmers being squeezed by the Mafia-style depredations of criminals.

Today, protection of property against terrorists is synonym with firewalls built by companies and anti-virus programs anyone can download for free on a personal computer. Firewalls, for instance, are obstacles to cyberterrorists. As McNamara (2003) states,

> firewalls offer protection from intruders by serving as a barrier between a computer system and the outside world (usually the Internet). Firewalls work by preventing certain data packets from reaching the computer while allowing other types of data in. Think of a firewall as a guard for all TCP/IP traffic on your network, constantly challenging packets to identify themselves as friend or foe, based on a set of rules you've provided the firewall with (p. 247).

This is the purpose of the firewall: to be a shield (protection from attackers) and obstacle (challenging packets to identify) at the same time. There are other types of firewalls such as packet-filtering routers (to forbid an outsider to connect to applications within the network) and the proxy server (to check the content of each data packet as it arrives) (Mansfield, 2000). Major Web sites and corporate networks have protected themselves because they have the funds and impetuses to do so. Power plants have well-protected Internet operations, and are equipped to detect intruders, often divulging where they come from (Dunnigan, 2003).

Counterterrorist agencies have also considered the option of collaborating with a large number of cyberterrorists and learning from their knowledge for defensive and even retaliatory purposes (Zanini & Edwards, 2001). They have increased their reliance on experts such as Richard Clarke. Richard Clarke was the US first counter-terrorism chief during the Clinton administration. He is now the *de facto* anti-cyberterrorism czar

(Verton, 2003a). He has pushed the American government to improve cybersecurity and create obstacles against cyberterrorism. The reliance on experts or academics to strengthen barriers against terrorism is not new.

In Antiquity, Josephus (37 CE-circa 100), a Jewish historian (Thackeray, 1968), was also Rome's "private consultant" on terrorism. In his writings, he warned Romans against the Zealots (Bilde, 1988; Feldman & Hata, 1987; Josephus, 1982; Maier, 1993) and warned others against the folly of opposing the Romans. What Josephus also represented for the Zealots is a political obstacle during the remainder of the war. Part of the reason is that he assisted the Roman commander Titus in negotiating with the so-called revolutionaries (Rajak, 1984). Not surprisingly, Josephus was branded as a traitor and, unfortunately, was unable to convince the defenders of Jerusalem to surrender to the Roman siege, which led to the destruction of the city and the Holy Temple.

The biggest obstacle that terrorist networks have always faced is "crippling intrusion" such as misleading information and distrust. History is abundant with cases of treason, even among terrorists themselves or those "old-boys'" networks. This makes the perspective of networks sometimes limited in scope. As explained by Zanini and Edwards (2001),

> to the degree that erroneous or otherwise misleading information is planted into a network's information flows by what are seemingly credible sources, over time the integrity and relevance of the network itself is compromised. This in turn could breed distrust and further cripple a group's ability to operate in a dispersed and decentralized fashion (p. 53).

As one can see, terrorist networks in Antiquity and cyberterrorist networks today seem to mirror each other on many patterns of evil stratagems. No matter what century, no matter what geographical area, no matter what the motivations are, no matter how the network is formed, no matter who is involved, and no matter who the target is, terrorists seem to have always attempted to create a new order with their new kinds of technology, be it a shiny dagger or software to penetrate computer files. Even some members of the Roman elite collaborated with terrorists. So networking with criminals is as old as gold. As explained in this section, the Zealots, for instance, had an extensive network that operated in Antiquity and that is still relevant today. Indeed, its network is a forerunner of cyberterrorist networks not only in aspects of motivation, but also in aspects of kinship, design, targeting, and goals. Although the Jewish Revolt was ultimately a failure (mass suicide in Masada), the fact that the Zealots are remembered two millennia later demonstrates the deep psychological influence they have brought.

In line with these contentions, it is fair to say that successful cyberterrorism, like terrorism in Antiquity, depends on two major elements: means and vulnerability. The means are the human resources, tools, and weapons available to the attacker. The vulnerability is the extent to which the target's defense and networks are effective (Dunnigan, 2003). However, it also proves factual that terrorist networks may be somewhat limited for reasons mentioned earlier. In turn, potential victims since early history have always invented ways to protect themselves, not only by attacking, but also by *defending* themselves against attacks, or even relying on experts. For instance, "human intelligence" in Ancient Rome was taught by Josephus. It was slightly akin to what Homeland Security does today,

A Comparative Analysis of the Jewish Revolt and the Cyberterrorism Incident over Kosovo, Based on Social Network Theory

This section uses social network theory to make a comparison between the social network of the Jewish Revolt in 66-73 CE and cyberterrorist attacks during the Kosovo war in 1999. The Revolt in 66-73 CE, also known as "the First Revolt," was propelled by a social network of terrorists, of which the main group was the Zealots. It took time for other groups to join them. The Kosovo conflict saw the rise of the first major Internet war where independent hackers targeted NATO and US government Web sites. The use of social network theory is important here because it [the theory] embodies a particular theoretical orientation towards the structure of terrorist networks. After all, networks are one of the most common forms of social organizations (Williams, 2001). This is why it applies perfectly to the Jewish Revolt and the war in Kosovo. It also enables me to make the point that social network theory is the best theory that can be used to demonstrate that cyberterrorist networks resemble networks in Antiquity in some ways, and differ in other ways. The ultimate goal of this analysis is to bridge the gap between theory and practice.

To begin with, a historical explanation of the reasons that led angry Jews to rebel against their Roman oppressors is provided. Then, an explanation of the relevance of social network theory in this analysis is given. This is a springboard from which the author draws hubs and nodes, through graphs, of the networks that link the Zealots and their collaborators. The main argument is that the centrality of the Zealots (in Masada) exemplifies the measure of the prominence of the "star" or "wheel" network (Bavelas, 1950) during the Jewish Revolt. In other words, the ties that the Zealots in Masada have with others make them prominent because they are "particularly visible to the other

actors in the network" (Wasserman & Faust, 1994, p. 172). What is also relevant is that this prominence is neither due to the reception nor the transmission of many ties, since the relations were nondirectional (Wasserman & Faust, 1994). After the analysis of the Jewish revolt, the author provides an analogy with the cyberterrorism incident over the Kosovo conflict. The main argument is that cyberterrorist networks follow a pattern of the all-channel network, where all the nodes can connect with any other node, without the fear of being caught. Plus, there is no centrality in the all-channel since it has a horizontal and flat structure, and not a hierarchical or vertical one.

The Jewish Revolt of 66-73 CE

We already know that a great deal is factual about the Zealots thanks to Josephus Josephus's writings (Josephus, 1982). "We will kill all collaborators" and "No king but God" were some of the many slogans that emerged from these politico-religious insurgents. The Romans labeled them "a sworn fraternity of fanatics" and "rebels." Josephus called them brigands of a new type, in the same way that we call cyberterrorists "terrorists of a new future." At first, the Zealots were very active in the Galilean hills, waging occasional guerrilla warfare and being a widespread nuisance. By early 1st century CE, the locals and the religious groups were unwilling to support them, so their numbers were small (Josephus, 1982). The main reason is that the Zealots, unlike the Pharisees, wanted to expedite the process of religious liberation by direct action (Farmer, 1956). However, in about 30 CE, Jesus Christ began his journey of prophecies. As his prophetic vision increased, so did the pressure from Roman despotism. Such cruelty led more and more Romans to profane religious institutions and, consequently, more and more disgruntled folks would join the Zealots' rebellious group (Smith, 1971). As the

years went by, they created an extensive web of terrorists and developed a major information network. This helped terrorists slit the throats of Romans, who had occupied Israel since 63 BCE, and their "collaborators." What followed was a Jewish rebellion in 66 CE, after Florus, the last Roman procurator, stole vast quantities of silver from the Temple in Jerusalem. Thousands of Jews (of different walks of life), maybe a million, inspired by religious conviction, created a mass uprising not only against the Romans who governed both Greeks and Jews (Telushkin, 1991), but also against the Greeks in Judea. As such, they ambushed sentries, sabotaged military stores, stole horses, and destroyed roads and water works, poison wells, granaries, and the water supply of the Holy City (Bloom, 2002; Roth, 1959).

The above historical account is better known as the Jewish Revolt of 66-73 CE in Jerusalem (Goodman, 2002; Roth, 1959). Through their actions, the rebels aspired to act as propellers of a long-prophesized messianic intervention. The reasoning behind this was that, for the rebels, the Roman oppressors would either not resist at all or do it so poorly because of fear and a sense of being outnumbered. The ultimate goal of the rebels was to create a panic more alarming than the affliction itself. Although few people supported the Zealots at first, the Zealots' ranks grew exponentially as more profanities were committed against Jewish heritage and many Jews rapidly became persuaded that they could defeat Rome (Horsley, 1986). The Zealots and other "liberators of Jerusalem" had thousands of fighters (the accurate number is unknown) divided into groups. The Zealots, under Eleazar ben Simon, occupied Masada (the most important besieged area of the Revolt), the Antonia, and the Temple. The Sicarii (led by Simon ben Giora) ran the upper city of Jerusalem. The Idumeans held Southern Judea (Bloom, 2002). There were other

allies such as the partisans under John of Giscala and other groups of lower-class citizens who, nonetheless, were willing to sacrifice their lives for a new world order.

Applying Social Network Theory to the Jewish Revolt

All these groups joined forces in 66 CE; they were linked through a social network. At first, the network had no apparent plan or organized leadership. Yet, it took time for the Roman legions to realize that the leadership was eventually "headquartered" at the fortress of Masada (Cohen, 1982), where strong ties started to develop with the other rebels who seized control of Jerusalem section by section. At some point during the Revolt, their social network was so strong that they massacred the sole cohort of Roman infantry left behind by Florus as a garrison. They also besieged Herod the Great's two strong fortresses, Herodium and Machaerus (Bloom, 2002). The Zealots in Masada did not always have strategic significance in the overall structure of the Jewish network of rebels. Part of the reason is that a lot of ties were cut, while other new ties developed. After all, the Jewish revolt lasted seven years. So it is no surprise that the network was at times significant and at other times weak. Figure 1 (on the next page) shows the most important nodes (or actors) in the social network of the Jewish revolt, when their network was strong. The most important nodes were the Zealots in Masada, the Zealots at the Temple, the Zealots at the Antonia, the Sicarii in the Upper City, the Idumeans in Southern Judea, and other partisans in the Lower City. Figure 1 is a highly centralized graph. The purpose of using a graph in social network theory is to identify the most important nodes (or agents) in a social network (Wasserman & Faust, 1994). The idea of centrality of individuals or groups in a social network was one of the first to be pursued by social network analysts (Scott, 2004).

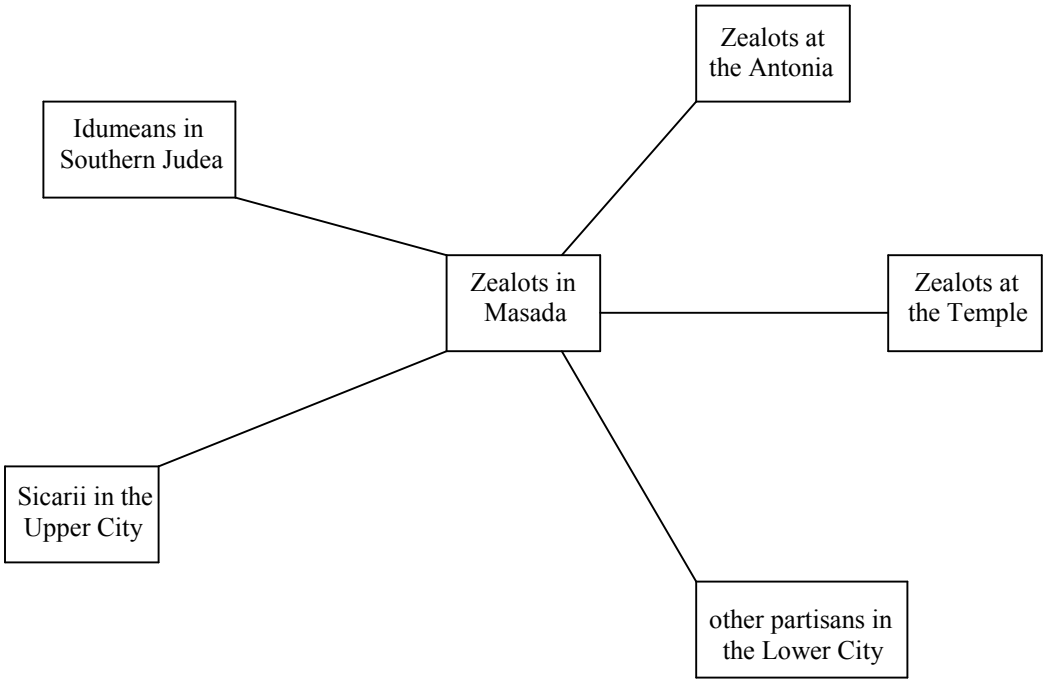

Figure 1 *Example of a "star" or "wheel" network, as in this network of the Jewish rebels*

The network shown in the graph is also called the "star" or "wheel" network (Bavelas, 1950) because there is a central point that is at the hub or core of different Jewish connections. In other words, the most *prominent* individual or group (in this case, the Zealot leadership at the fortress of Masada) stands at the center of the network and has influence on its environment (i.e., in terms of decision-making, etc.). Whether this prominence is due to the reception or the transmission of many ties is not a particular concern here, since the relations were nondirectional (Wasserman & Faust, 1994). What is important is that, according to social network theory, the Zealots in Masada represent a

point that is said to be *locally* central because "it has a large number of connections in its immediate environment" (Scott, 2004, p. 82). However, it is not *globally* central because, as we have seen, the Zealots in Masada did not always have strategic significance in the overall structure of the Jewish network of rebels.

In line with these contentions, it might be difficult to know the exact validity of the measures of centrality. Do they really capture what we substantially mean to be "prominence" or "significance"? Can we simply focus on nodes that are "selected" the most to find the most important nodes? (Wasserman & Faust, 1994). The answer to these questions can prove accurate if we consider the historical fact that all ties that link the Zealots in Masada to the other groups are not interchangeable. For that reason, the Zealots in Masada are not equally central. For instance, the tie between the Masada folks and the Sicarii outranks the others because, historically speaking, their relationship and cooperative efforts during the Jewish Revolt were stronger than the others. By the same token, it is not surprising that the link between the Zealots in Masada and the Idumeans in Southern Judea is weaker than the others, since Southern Judea is further away than the areas where the other rebels were located. In other words, the Idumeans were not as extensively involved in relationships or "well connected" with the Zealots as the others were. A validity of prominence and centrality in a social network "corresponds to the intuitive notion of how well connected a point is within its local environment" (Scott, 2004, p. 83).

What comes next is an explanation of "network self-destruction," based on social network theory, due to an historical fact of internal hatred within the social network of the Jewish rebels. What happened was that the links between the important actors in their

social network became heavily damaged after Emperor Nero heard about the success of the Revolt and dispatched Vespasian to command three legions and auxiliaries (nearly 60,000 men) to march to the port of Caesarea, and then to Jerusalem. This campaign successfully secured Roman progress (by besieging many places in the Holy City). This progress provoked internal conflict within the social network of the Jewish rebels themselves, leading the Zealots and one group of allies, the Idumeans of Southern Judea, to overthrow the Jewish aristocrats and seize control of Jerusalem. Simon and other terrorists entered Jerusalem and opposed the Zealots' control of the rebellion. Part of the rationale behind this opposition was that the Jewish leadership in Masada did almost nothing to help their besieged allies. They had concluded that the Revolt could not be won. The Jewish forces were eventually deeply divided, which, in turn, crippled the coordination of operations or even mutual support. This led to self-destruction of their social network because from the year 70 until 73 CE, most large nodes were removed (in other words, most Jewish ally groups were massacred by the Romans), which isolated the central node in Masada. This meant the end of the social network of terrorists during the Jewish Revolt. It takes a lot to destroy a network (Barabasi, 2003). The failure of the Jewish Revolt was due to deep hatred among the Jewish rebels themselves.

Figure 2 (on the next page) shows a cripple social network of terrorists, where all the links are destroyed, isolating the central node in Masada. Because social network theory suggests that compartmentalization into node structures is crucial to the "survival" of the network of terrorists, and because the compartmentalization of terrorism into nodes allows for more openness, flexibility, and diversity which, in turn, enables different nodes to communicate with less difficulty, the social network of Jewish rebels could not survive

because all the links and resources shared between the Zealots in Masada and the other terrorist allies were progressively destroyed.

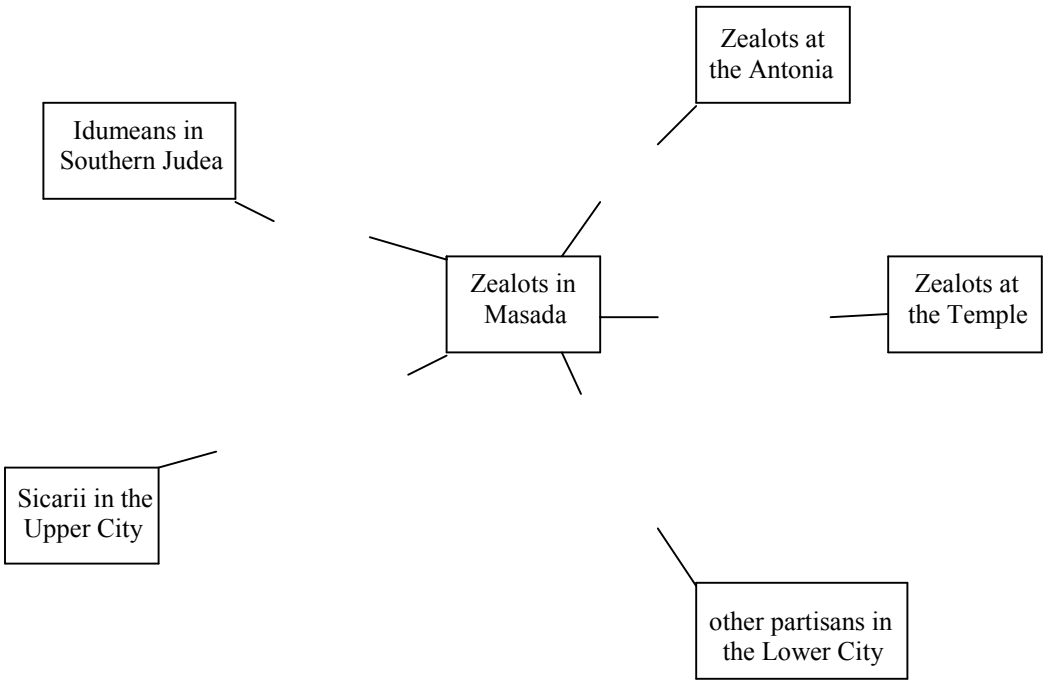

Figure 2 *The crippled social network of the Jewish rebels from 68 to 73 CE, the year the remaining Jewish rebels committed mass suicide at Masada*

The nodes could not even survive through "autopoiesis" (Bailey, 1997; Bednarz, 1988; Benseler, Hejl, & Kock, 1980; Mingers, 1994; Zeeuw, 1992; Zeleny, 1981), that is "self-organization" (Heylighen, 2003), because the existing interactive elements of the nodes were nullified, which gradually incapacitated the social network to regulate itself. This meant self-destruction. The only escape for the remaining Jewish rebels (from Roman capture) was to commit mass suicide in Masada in 73 CE.

The Kosovo War as an Incident of Cyberterrorism

The social network of the Jewish revolt of 66-73 CE shows recognizable characteristics of cyberterrorist networks. A good example of a cyberterrorist network incident is the one that occurred during the Kosovo war in 1999. The conflict over Kosovo has been characterized as the first war on the Internet. Government and non-government actors alike disrupted service on government computers and took over their Web sites, particularly US government Web sites (Denning, 1999). What happened is that in 1999 NATO airplanes bombed Serbian targets in an effort to stop the Serbs from attacking Albanians (Dunnigan, 2003). In the process, they accidentally bombed the Chinese embassy in Belgrade, Yugoslavia. For this reason, thousands of young Chinese hackers targeted US government Web sites, including the Energy and Interior Departments' Web sites, the U.S. Embassy site in Beijing, and the U.S. Naval Communications Command. By the same token, cyberterrorists attacked NATO's main Web site, causing a line saturation of the server by using a "bombardment strategy" (Seffers, 1999). NATO computers were also flooded with email bombs – sending an email bomb consists of deluging hundreds of thousands of emails into a computer network – and hit with denial-of-service (DOS) attacks by hacktivists protesting the bombings against the Serbs. Likewise, American businesses, public institutions, and academic institutes received tons of virus-laden e-mails from a certain number of Eastern European countries. One group, the Kosovo Hackers Group, a coalition of European and Albanian hackers, attacked five Web sites (Regan, 1999). Nothing serious happened, but had their attempts been successful, the consequences thereof would have been devastating.

The dispute over Kosovo was really "turning cyberspace into an ethereal war zone where the battle for the hearts and minds is being waged through the use of electronic images, online discussion group postings, and hacking attacks" (Dunn, 1999, p. 42). But that was not all. Another group, the Black Hand hackers (from Serbia), deleted all data on a U.S. Navy computer. Members of an affiliated cell, Serbian Angel, planned daily actions that blocked and disrupted military computer operated by NATO countries. They also delved into a Kosovo Albanian web server and threatened to destroy the Alliance's information system (Adams, 1998). In the same geopolitical area (that is, Serbia), both Milosevic (the Yugoslav president at that time) and people opposed to NATO engaged in cyberterrorism. So did civilians caught in the conflict, who considered cyberspace a powerful tool to express sentiments about the risks under the fatal exposures to NATO carpet bombings. The Russians took part in cyberterrorism too. They attacked governmental Web sites of NATO countries, using virus-infected e-mail and "infiltration" attempts. Over one hundred institutions in the United States received these e-mails. Various British organizations lost files and databases in the process.

More importantly, Americans were also involved in the cyberterrorist incident of the Kosovo war. What happened was that this incident ignited the passions of American cyberterrorists to bring down several Web sites in Yugoslavia (Regan, 1999). Team Split, an American group of cyberterrorists, broke into government Web sites, posted statements such as "Tell your governments to stop the war," and even assaulted them. Others tried to corrupt e-mail systems, which were also saturated by one individual who sent two thousand messages a day (Seffers, 1999). Nevertheless, individuals from allied countries retaliated. For instance, one group, Dutchthreat, based in the Netherlands,

blasted a Yugoslavian Web server after they grew infuriated about a message posted on a Yugoslavian ISP that called NATO members "Nazis." Besides, an order passed by President Clinton in 1999 allowed American government computer hackers to infiltrate Slobodan Milosevic's foreign bank accounts and siphon off his hidden funds that could have been used for military purposes (Hoffmann, 1999). The computer attacks on his foreign bank accounts were also committed to alter his banking records (Becker, 1999). The main rationale behind this covert action was to help the CIA overthrow the Yugoslav president (Sherwell, Nikolic, & Strauss, 1999).

Applying Social Network Theory to this Cyberterrorism Incident

The incident of cyberterrorism during the Kosovo war demonstrates that various groups can be located far away from one another and still have the same targets, that is, NATO and US government Web sites. What is also interesting is that these groups probably did not know one another. As such, there were hacker groups from China, from Russia, from Serbia (several), from Albania, and even from the United States. The Internet was their conduit. Drawing a parallel, it might also be the case that, considering the high number of rebels during the Jewish Revolt of 66-73 CE (maybe one million), some of the partisan groups did not know each other either. Applying social network theory to the Kosovo cyberterrorism phenomenon, we can see that cyberterrorists can easily connect all over the map, from sites to sites, and aim at the same targets. Figure 3 (on the next page), based on Dorothy Denning's (2001) description of the situation, is an interpretation of what the cyberterrorist network over the war in Kosovo in 1999 could have looked like. Figure 3 shows the all-channel network (Bavelas, 1950; Leavitt, 1951), where any node in the cyberterrorist network can connect with any other node.

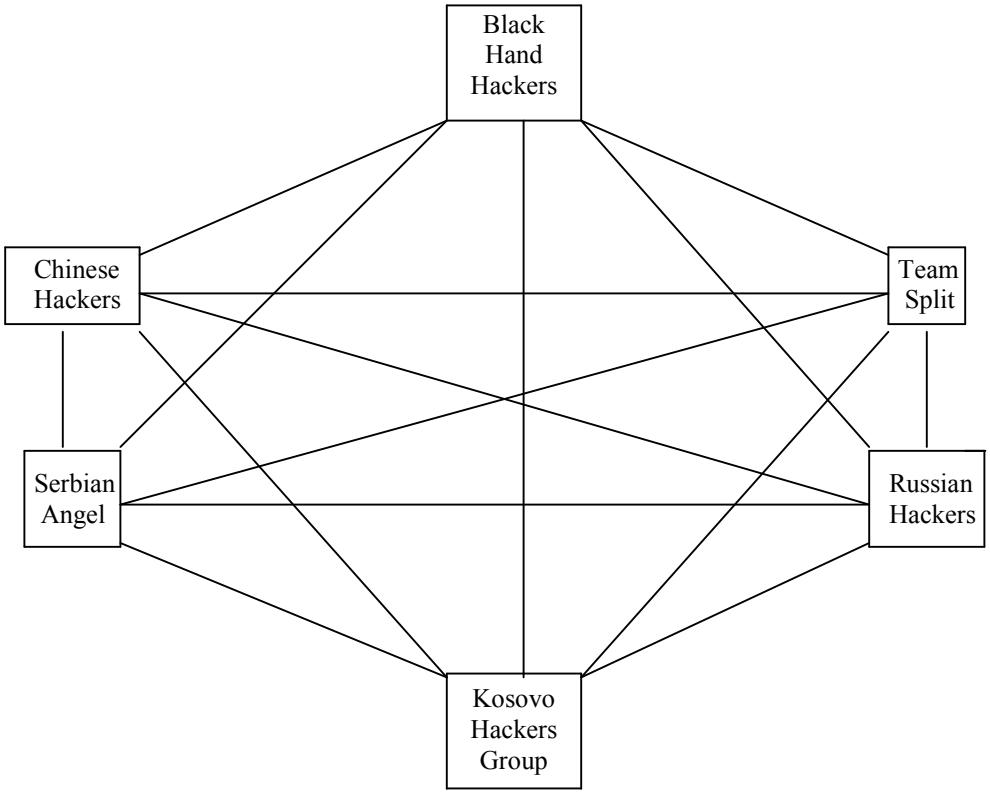

Figure 3 *Example of an all-channel network, typical of a cyberterrorist network*

In this model, the Kosovo Hackers Group could have communicated with the Team Split about bettering their endeavors to target Web sites. The all-channel network is collaborative, quick, effective, and multi-directional. It implies that there is no central node as in the star or wheel network. Therefore, there is no central commander. In other words, it is a full-matrix networks, where every cell is connected to and can communicate directly with every other cell (Evan, 1972). What can also be said is that the Kosovo Hackers Group may have acted alone without communicating with anybody. As soon as a cyberterrorist group is created on the Internet, the Internet automatically puts that group

in an all-channel network because cyberspace is in fact an ultra-flexible network of billions of nodes that can communicate with one another, even unbeknownst to each other. Based on social network theory, the Internet enabled various groups of cyberterrorists – or even independent hacker groups that did not know each other – to cross national boundaries and operate safely by targeting American and NATO Web sites without being caught. This is where postmodernism is applicable because the FBI could have been there too. Not only can coordination be tricky, but, also, anonymous nodes such as FBI cells can infiltrate cyberterrorist networks too.

No matter what, in the all-channel network, the measure of visibility is tantamount to the number of links (Barabasi, 2003). More importantly, cyberterrorist networks do not break apart under failure. The voluntary destruction of nodes will not be fatal. Even if NATO and US experts had brought down nodes one after the other, any of the remaining nodes would have survived because nodes on the Internet are autonomous and resilient. However, if the cyberterrorist network has large hubs, and if these hubs are destroyed, then the network can break. In the grand scheme of things, independent cyberterrorist cells such as the Black Hand Hackers and Team Split are small nodes. Indeed, the nodes from the graphs are small, in comparison with a node such as the US government's central computer system, which constitutes, of course, a very large node on the Internet. This means that the elimination of several *large* nodes, or hubs, on the Internet could create a catastrophic disorder, like a cascading failure. As explained by Albert Barabasi (2003),

> if crackers launched a successful attack against the largest Internet hubs, the potential damage could be tremendous. This is not a consequence of bad design or

flaws in Internet protocols. Such vulnerability to attack is an inherent property of all scale-free networks (p. 117).

NATO and the US government could not really do anything to destroy the nodes of the hacker groups because they were not fixed and they were very difficult to find. They operated from small private computers that were presumably located in other countries. For a cyberterrorist network to be vulnerable to a counteroffensive attack led by an army of cyberwarriors, several of the largest hubs must be *simultaneously* removed to crush them (Barabasi, 2003). What is even more complex in cyberterrorist networks is that they are horizontal and flat, rather than vertical and bureaucratically governed (Arquilla, Rondfeldt, & Zanini, 1999). There is no central leadership as there was during the Jewish Revolt. After the remainder of the rebels committed suicide in the fortress of Masada in 73 CE, the Revolt was over. The Romans had won. Cyberterrorists' horizontal and flat type of organizational structure is different from the traditional terrorist network's hierarchical design. It is different in that this type of organizational structure is based upon flexible communication relationships. This information is not covered in this section, but it will be later.

Discussion

What this section has demonstrated is that terrorist networks in Antiquity and cyberterrorist networks today seem to mirror each other in their patterns of evil stratagems. Yet, they also differ in many ways. Looking at their similarities, we have seen, for instance, that they both seem to have comparable trust patterns. While Ancient terrorists would connect with other individuals who have mutual agendas and goals to form subgroups, convene at a target location, carry on terrorist operations, and then

subsequently terminate their relationships and redisperse (Zanini & Edwards, 2001), cyberterrorists today navigate on the Web and try to connect there. More importantly, cyberterrorists and their Ancient counterparts also have the same motivations (that is, political ambitions, economic deprivations, crime for crime's sake, and the need for publicity). While the Zealots were convinced that political change could only be attained through "propaganda of the deed" (Laqueur, 1999b), and while their most basic drive was that all means were justified, political ambition and commitment are also part of the agenda of cyberterrorists (Denning, 2001). Sabotage of electronic networks, power grids, and other elements of a nation's infrastructure may not be solely intended to cripple specific individuals or groups (Schweitzer, 2002). In some cases, these cyberterrorist acts are also aimed at achieving political goals. After foreign experts learned that the damaging Code Red virus of 2001 came from China (Dunnigan, 2003), they believed the Chinese government backed it up, but China denied any responsibility. Terrorism is also news (Laqueur, 1999b), publicity. In 66-73 CE, the Zealots slit the throats of Romans (and those who favored them) in public, in the same way that cyberterrorists like to send email bombs on thousands of Web sites, enough to disrupt an entire state's computer network.

What this section has also argued is that alongside the old terrorism, new kinds of terrorism have arisen, but until more fitting terms gain general acceptance, old labels will have to suffice (Laqueur, 1999b). Premeditated acts of terrorism have always dotted our world's history. This is why it was deemed necessary, in order to make a good comparison with cyberterrorists, to characterize what a terrorist was in Antiquity. The point was made that the criteria defining terrorists were determined by Greek and Roman

power-holders who decided to place them beyond the pale of civilized society. No matter what, planning a damaging terrorist attack requires talent and technology. Two millennia later, the adage "terrorism leads to 'smarter crime'" (Laqueur, 1999b) still prevails. The impacts of technology that devastated entire armies and peoples provide an interesting analogy with our contemporary anxieties over the possibility of harmful cyberterrorist incidents. As they act in networks or with hired mercenaries, they aim for ingenuity, both for using their technology and for outsmarting their enemy (Schweitzer, 2002). They also need money to carry out their plots. This is why another motivation is economical (i.e., money laundering). Cyberactions are so limitless that terrorists can easily operate as stockbrokers, looking for the best deals. Economic deprivation also leads us to believe that terrorism is a social phenomenon. As described in the example of the Boukoloi, networks emerged as a result of a combination of ruthless and uncompassionate government, drastic social conditions, and escape from oppressive Roman taxation (Alston, 1998).

What has been emphasized is that all those motivations are what blend individuals into the same melting pot of convictions and goals. When people have a common denominator, they will join forces by creating local groups that will propagate into sprawling networks. This is how terrorist networks are created. This comparative analysis of networks exemplifies the notion that terrorism has made colossal progress, but human nature has not changed. There is as much evil and insanity as there ever was (Laqueur, 1999b). We all know that the ultimate result is fear. Indeed, fear. Fear of networks. In Antiquity, networks were already made of informal, loosely, and open structures, usually divided into small, fragmented, and temporary ventures. This took the appearance of an

illusion of invulnerability, making the enemy feel that they were outnumbered. They also organized their activities around speed, which is the prime quality of an attack on the Internet: the more speed cyberterrorists have, the less capable the defense is (Dunnigan, 2003). Some of these networks are actually hybrid organizations that pursue political and economic agendas. The main goal has always been the same: to create connections and coordinate dispersed activities (Zanini & Edwards, 2001). One way the Ancients organized terrorism was through patronage (Zehr, 1978). Patronage was synonym with harboring terrorists; it was practiced by hierarchical, Mafia-like organizations that exploited the relationships between "perpetrators" of terror and "sellers" of terror, like patron-client relationships (Rawlings, 1998). While terrorist networks can be linked by groups that consist of hundreds, if not thousands of members (as it was during the Jewish Revolt), some terrorist parties can be very small, sometimes consisting of just one individual (Laqueur, 1999b), such as an independent cyberterrorist, sharing the same goals as other cyberterrorists, but acting as a hacking mercenary. They would sell their souls to a cause for diverse reasons, like to catch computer users by surprise. The ultimate corollary will be a weakness of our psyche, because panic resulting from terrorism causes as much detriment as the terrorist act itself.

Finally, a comparison between the social network of the Jewish Revolt in 66-73 CE and cyberterrorist attacks during the Kosovo war in 1999 was made. The use of social network theory was important here because it embodies a particular theoretical orientation towards the structure of terrorist networks. The theory also applies perfectly to the Jewish Revolt and the cyberterrorism incident over Kosovo. It is actually the best theory that can be used to demonstrate that cyberterrorist networks resemble networks in

Antiquity in some ways, and differ in other ways. The ultimate author's goal in the analysis was to bridge the gap between theory and practice. Of particular relevance in this comparison was that the social network of the Jewish rebels was the "star" or "wheel" network (Bavelas, 1950) because there the graph (Figure 1) shows a central point that is at the hub or core of different Jewish factions. The Zealots in Masada were the most *prominent* faction and had influence on their environment. The relations they kept with their allies were nondirectional (Wasserman & Faust, 1994). Besides, based on the premise of social network theory, the Zealots in Masada represent a point that is said to be *locally* central because "it has a large number of connections in its immediate environment" (Scott, 2004, p. 82). It is not *globally* central because the Zealots in Masada did not always have strategic significance in the overall structure of the Jewish network.

In line with these contentions, the point was made that the social network of Jewish rebels was caught in "self-destruction" because, as suggested by social network theory, compartmentalization into node structures is crucial to the "survival" of a network. Yet, the social network of Jewish rebels could not survive because all the links and resources shared between the Zealots in Masada and the other terrorist allies were progressively destroyed (see Figure 2). This resulted, historically speaking, in internal hatred within the social network of the Jewish rebels. As such, large nodes were removed. These nodes could not even survive through "autopoiesis," that is, "self-organization," because the existing interactive elements of the nodes were rendered naught, which gradually incapacitated the social network to regulate itself. This meant self-destruction and a mass suicide in Masada in 73 CE.

As we have seen, this led to an analysis of the cyberterrorism incident over the Kosovo war in 1999. The graph (Figure 3) shows an all-channel network (Bavelas, 1950; Leavitt, 1951), where any node in the cyberterrorist network can connect with any other node. The all-channel network is collaborative and, above all, multi-directional. It implies that there is no central node and no central commander. It is a full-matrix networks, where every cell is connected to and can communicate directly with every other cell (Evan, 1972). Part of the reason is that the Internet automatically puts any user in an all-channel network; cyberspace is literally an ultra-flexible network of billions of nodes that can communicate with one another, even unbeknownst to each other. Based on social network theory, the Internet enabled various groups of cyberterrorists to cross national boundaries and commit their cyberactions safely. We have also seen that it is very difficult to remove independent cyberterrorist cells such as the Black Hand Hackers and Team Split because they are small nodes. The US government's central computer system, however, is a very large node, which means that the elimination of several large nodes in cyberspace could lead to a catastrophic disorder, like a cascading failure.

What should be emphasized to a large extent in the future is the very fact that a cyberterrorist network is a postmodern type of network, where no leadership is needed, no center exists, and where communication is freer than birds in the air. Based on social network theory, I will make the point that, as opposed to those Ancient hierarchical structures that were vertically designed, cyberterrorist organizations are actually not *organizations*. They are movements. They do not exhibit an intrinsically "group" or "design" nature. Nevertheless, one should not downplay the importance of hierarchies; they are excellent structures for exerting control (Watts, 2003), as it was the case for the

Jewish rebels. Regarding cyberterrorists, there is certainly a lot to be said about their networks. As Schweitzer (2002) puts it, "while traditional concepts of terrorism may have withstood the test of centuries, the new millennium breaks the mold and calls for a rapid retrofit" (p. 290). The author is no counter-terrorism guru like Richard Clarke and no historian *à la* Josephus, but he encourages academics, experts, and private consultants to continue their never-ending struggle to understand cyberterrorism and Internet-based networks.

Postmodernism and Networks of Cyberterrorists

This comparison between networks of terrorists in Antiquity and networks of cyberterrorists exemplified the very notion that cyberterrorist networks are postmodern types of networks, where no leadership is needed, no center exists, and where communication is ultra flexible and quasi limitless. As opposed to conventional terrorist organizations, with their hierarchical structures that are vertically designed, cyberterrorist organizations are actually not *organizations*. They do not exhibit an intrinsically "group" or "design" nature. Rather, they are volatile and unexpected, a very postmodern attribute. For these reasons, this section purports itself to define postmodernism and to discuss its application to cyberspace with respect to (1) Baudrillard's hyperreal/real continuum, (2) the fragmentation, fluidity, and decentralization of the self, (3) cyberterrorism *per se*, (4) the organizational challenges faced by cybersecurity and law enforcement agents, and (5) the absence of leadership in cyberterrorist networks.

Definition of Postmodernism

Postmodernism is a cultural movement of the late twentieth century (Docherty, 1993; Jameson, 1991) that endorses the view that we are living in an era of individual

freedom from imposed rules and social constraint (McQuail, 2000). The postmodern movement has been prominent in media and communication studies (Williams, 2003). One of the fundamental assumptions underlying the theory of postmodernism is that it implies a blurring of the boundaries between previously distinct or opposite phenomena (Lister et al., 2003), and represents a shift away from spatialization and a triumph over linearity (Bubitt, 2002). For postmodernists, "nothing is the same, the world is decoherent, discontinuous, uncertain, inconsistent" (Kramer, 1997, p. 10). Meaning is not important because it is always indeterminate. Meaning is deconstructed (Derrida, 1973).

In order to have a good idea of what postmodernism is, it would be interesting to compare it with modernism. While modernism is synonymous with the early twentieth-century machine age, postmodernism represents the age of simulation, of online selves, and of computer and electronic media (McDermott, 1992; Turkle, 1992). Crotty (1998) follows the same lead in his comparison of the two worldviews below:

> Postmodernism refuses all semblance of the totalizing and essentialist orientations of modernist systems of thought. Where modernism purports to base itself on generalized, indubitable truths about the way things really are, postmodernism abandons the entire epistemological basis for any such claims to truth (p. 185).

Other scholars such as Lyotard and Baudrillard have been major influential theorists on the matter. For Lyotard (1984), a French scholar, postmodernism is a perspective; a means for understanding the conditions in which people live and learn now. According to him, postmodernism implies that individuals reject the grand narratives and paradigms that have defined culture and behavior in the past. For Jean

Baudrillard (2003), a French sociologist and one of the leading postmodern social theorists (Kellner, 1989), the postmodern world is reflected in the "hyperreal" world in which we live.

Postmodernism and Cyberspace: Hyperreal vs. Real

Cyberspace is a manifestation of the postmodern condition (Gur-Ze'ev, 2000). Ross (1988) goes even further by saying that the Internet "is the postmodern medium *par excellence*" (p. 7). The era of the public sphere as face-to-face interaction has gone (Poster, 1997). Today, the public sphere is postmodern because it is based on the notion that it is a mediated and mediating space. What this means is that cyberspace is the new public sphere and it is postmodern; it treasures the concept of the "public" while disengaging it from any particular time or place (Zarefsky, 1994). As a result, the postmodern map of cyberspace becomes the totality itself, superseding the world. Baudrillard (2003) refers to this moment as the "precession of simulacra" (p. 1). Simulacra and simulation, for Baudrillard (2003), constitute the world of cyberspace, what he calls the "hyperreal." Simulacra are mere signs which come to constitute new realms of experience. Simulations make these new realms of experience practical, allowing humans to do things that are not normally doable, to observe phenomena that are not normally visible, to control processes that are not normally controllable, or to participate in scenes or situations that would normally be dangerous, fatal, impossible, or too expensive.

This all boils down to saying that the adoption of cyberspace as a way to communicate and "do things" enabled by the elimination of the old, impeding structures is a postmodern condition that signals a rupture with modernism. Postmodernism implies

a positive reading of cultural and social change where new media technologies such as the Internet free themselves from the repressive hierarchies of the era of modernism (Lister et al., 2003). Postmodernism implies the hyperreal. The hyperreal is "the blurring of distinctions between the real in the unreal in which the prefix 'hyper' signifies more real than real whereby the real is produced according to a model" (Best & Kellner, 1991, p. 119). From Baudrillard's vantage point, humans are at the end of history and history may be reversing itself; humans live in a hyperreality, a sort of "post-orgy state of things" (Best & Kellner, 1991, p. 137). Our simulation of the real is our production of the real as pre-coded signs that function as the real, which leads to a hyperreality. As such, Baudrillard (2003) suggests that any effort to materialize the real as *the real* involves its artificial materialization as its own perfect exemplar, and thus as a hyperreality. He also sees the resulting real as veiling our own experience in its hyperreal semiotic perfection (Baudrillard, 1990).

This postmodern view of the real can be illustrated through the notion of "virtual terrorism." Today, terrorists know how to engage not only in horrors of real terrorism, but also "virtual terrorism" by using cyberspace to amplify the threat, mislead the public, and be widespread by media. Sloan and Kearney (1978) also call this phenomenon "non-territorial terrorism." The postmodern view of cyberspace is that it makes the fine line between image and reality collapse into itself. What we are left with is hyperreality. Baudrillard (2003) writes,

> no more mirror of being and appearances, of the real and its concept. No more imaginary coextensivity: the genetic miniaturization is the dimension of simulation. The real is produced from miniaturized cells, matrices, and memory

> banks and models of control, and it can be reproduced an indefinite number of times from these. It no longer needs to be rational, because it no longer measures itself against either an ideal or negative instance. It is no longer anything but operational. In fact, it is no longer really the real, because no imaginary envelops it anymore. It is a hyperreal, produced from a radiating synthesis of combinatory models in a hyperspace without atmosphere (p. 2).

Der Derian and Douglas (2005) corroborate the same idea when they argue that cyberspace produces effects and results that blur our accustomed ways of perceiving the world. What we see are new worlds that emerge; although real, they are less than physical. What we see are new spaces that emerge; although extensive, they are immediate and not at all distant. To come to the point, as the virtual becomes ever more actualized in our everyday lives, many of the usual ways in which we have perceived the world are being reversed (if not turned upside down). Wakabayashi (2002), a Japanese scholar, substantiates Der Derian's and Douglas's thoughts when he contends that our new ways of living and perceiving things are seen in the emergence of cyberspace and the "virtual city" in computer networks (especially on the Internet). Cyberspace, for Wakabayashi, is a change in the physical urban environment, whereas the "virtual city" in computer networks is a phenomenon of the non-physical environment (inside computers). These phenomena are the direct consequence of the postmodern social transformation, that is, the new relationship between space and society. The hyperreal is a semantic emptiness; the sense of "placeness" as we know it in physical, contemporary society does not make sense in cyberspace. For this reason, cyberspace is regarded as a postmodern phenomenon (Wakabayashi, 2002).

Truly, real space and hyperreal space are separated for two reasons: on the one hand, in the sense of not being consistent in their spatial construction and, on the other hand, in the sense that real space and hyperreal space are also physically separated by the screen that divides one spatial modality from the other. Therefore, the difference between "being" outside the space and "being" within the space is contingent upon the context, framework, and circumstances within the space. Let us follow the lead of Sobchack (1992) when she says that hyperreal space,

> becomes abstract, ungrounded, flat – a site for play and display rather than an invested situation in which action "counts" rather than computes. Such a superficial space can no longer hold the spectator/user's interest, but has to stimulate it constantly in the same way a video game does. Its flatness – a function of its lack of temporal thickness and bodily investment – has to attract spectator interest at the surface… In an important sense, electronic space disembodies (p. 57).

This notion of hyperreal also implies that cyberspace enables the "self" to become fluidity, a flow of identity that converges under the sign of the virtual environment. According to Poster (1997), "Internet technology imposes a dematerialization of communication and, in many of its aspects, a transformation of the subject position of the individual who engages with it" (p. 215). As a result, identity, then, becomes a flux or, as Rheingold (1998) suggests, a "fluid" that causes humans to be disembodied. Human disembodiment in cyberspace is one of the central tenets of postmodernism. In postmodernism, "identity is not unitary or essential, it is fluid or shifting, fed by multiple sources and taking multiple forms" (Kumar, 1997, p. 98). The next section highlights the

postmodern transformation of the "self" through fragmentation, fluidity, and decentralization of the "self."

Postmodernism and Cyberspace: Fragmentation, Fluidity, and Decentralization of Self

In regard to cyberspace, postmodernism emphasize fluidity, and the immediate and constant re-referencing of identities. The flow of identity converges under the sign of the virtual environment. We enter the nature of the real that enables the virtual. Instead of printed matter, what we have are recombinant energy processes or flows (Matusitz, 2005c). Identity, then, becomes a flux or, as Rheingold (1998) suggests, a "fluid" (p. 84) that causes humans to be disembodied. In this sense, we take a fluid role in the construction of identity through different levels and qualities of interaction. Fluidity of the self means that the self can be manipulated on the whims of its creator; it also implies fragmentation of the self, a term of postmodern identity construction (Matusitz, 2005c). While modernist notions of the self are based on the ideal of a stable, non-shifting identity, postmodernism conceives identity as continuously being reconstructed (Deibert, 1997). For postmodernists, identities in contemporary life are fleeting philosophical entities, moments of hyperreality likened to the swirling signification of cyberspace (Baudrillard, 1991).

In addition, it is important to mention the notion of decentralization of the self in cyberspace. The self becomes decentralized because cyberspace has no center; it has acquired the form of a self-regulating system with billions of chunks of information accessible to anyone. From a postmodern standpoint, as humans communicate in virtual space, they experience a continuous, time-based junction of symbolic meaning forces (Matusitz, 2005c). What this means is that interaction in cyberspace presents one field of

symbolic meaning force that can only be understood contextually *vis-à-vis* other adjacent forces. As a result, our spatio-temporal ways of world-making (Goodman, 1978) and of conceiving the world are not a flexible and uniformed system. The postmodern inflexibility of the self in cyberspace "constitutes a form of absolute presence (one abstracted from the continuity that gives meaning to the system past/present/future) and changes the nature of the space it occupies" (Sobchack, 1992, p. 57). In other words, with respect to the decentralization of the self and the reconstruction of identity, in the disembodied world of cyberspace, many of the basic cues to personality and the social roles we are accustomed to in the physical world are absent (Gill, 1996). Therefore, Baudrillard's simulacrum, mentioned previously, creates a passive subject living his or her own existence in his or her own reality, or simply someone who takes the simulation as the only significant, compelling reality. In fact, for the Web user, identity in cyberspace may not be a representation of a self any more. Rather, it may become the self against which life in the body is weak psychic competition. Postmodernism imagines the self, in this case the Web user, not as a producer of meaning, but as a consumer defined in her or his interaction with others in cyberspace.

As one can see, as opposed to modernism, postmodernism posits that the concept of "me" as an entity is just an illusion, a simulacrum. This idea of the postmodern self in the virtual world had already been illustrated by Habermas (1980) when he wrote that,

> the postmodern stance heralds many of the arguments that have arisen from new technologies. Like postmodernism, electronic communications constitute the subject in different ways than do modern institutions… At the same time, technology also can configure multiple representations of the self. In a virtual

> space, appearance replaces the real… Internet recalls the postmodern idea of "simulacrum" – there exists no concrete essence apart from that which is seen or reproduced" (p. 296).

In this sense, while the "me" in the real world is something that appears through our own unique point of view, the "me" in the hyperreal world of cyberspace is reduced to the ontology of the image thanks to the digital media – following the lead of Habermas, one can have multiple representations of the self. In postmodernism, not only are the phenomena results of our point of view, but the "me" is now exclusively for "me." From this postmodern perspective, the Web user can, on the one hand, embody a single subject who is volatized and fragmented (Simpson, 1995; Turkle, 1995) and, on the other hand, personify many different characters in cyberspace. Of equal significance is the fact that individuals are in contact with people from different cultures and with people they have met only as virtual constructs. Consequently, by interacting beyond the stigma of real life, it is difficult to determine how identity is to be projected; likewise, the online medium has the potential to become a deceptive social space where individuals become victims of malevolent acts.

Part of what postmodernism introduces is a set of non-linearities in time, in space, in virtual environment, and in decentered self (what Sherry Turkle calls "life on the screen"). Molded on Gibson's (1984) matrix of informational space, "postmodernism's objects now exist outside science fiction" (Turkle, 1995, p. 45). Sherry Turkle (1995) continues by saying that,

> They [postmodernism's objects] exist in the creatures of a SimLife computer game, and in the simulations of the quantum world... All of these are life on the

> screen. And with these objects, the abstract ideas in Jameson's account of postmodernism become newly accessible and even consumable (p. 45).

A thought-provoking worldview through which to consider the process of the "self" has been presented to human beings (Matusitz, 2005c). The next sub-section emphasizes how cyberterrorism has been made possible thanks to the postmodern world that makes up cyberspace, including multiple representations of the self and new conceptions of space and time.

Postmodernism and Cyberspace: Cyberterrorism

Cyberterrorism is a postmodern method of reaping terror for five reasons. First, cyberterrorists can cover their true identities and locations a mouse click away; they can choose to remain anonymous, pretend to be another self, or simulate multiple selves within a few seconds. Postmodernism stands against reified corporeal bodies and regimented social structures. Identity as we know it in the physical world is something constructed (Lister et al., 2003); cyberspace, however, makes identity fluid, deconstructed, and faded away, which enables the cyberterrorist to come and go without notice. In cyberspace, the self can take on a different meaning and can be represented rather than real. This justifies the existence of Otherness (Matusitz, 2005c). Otherness dwells in the cyberterrorist's identity and his or her network – both in their production of meaning and in their interpretation. Identity does not exist without meaning and interpretation. In order to find out who is who behind a cyber attack, part of the objective of the computer expert is not only to play the role of the Other, but also to construct meaning and interpretation when tracking a cyberterrorist online. Reputations on the Internet are developed and maintained or challenged and blasted (Matusitz, 2005c). By

looking closely at these cues, at how they work and when they fail, computer experts can learn a great deal about how cyberterrorists communicate among one another.

Second, the opportunities for interaction among cyberterrorists on the Internet can create a sense of immersion and engagement far different from anything that sensory or motor realism can provide (Schiano, 1999). Computer technology and the Internet enable cyberterrorists to establish social interdependence (and, hence, communities) that is more difficult to achieve in the corporeal world because of the stumbling blocks posed by modernity's social structures and physical divisions, all of which prevent conventional terrorists from communicating as quickly and easily as they do it on the Internet. Yet, cyberterrorist networks are more than online communities; they organize relationships into powerful synergies that have an ultimate goal: to create a new world order by destroying the existing world order. How do they do that? They do that by not only striking their targets through viruses and other malicious tools, but, also, by tactfully using cyberspace to alter human interactions and by making the sense of self – as we know it on earth – senseless. This is a manifestation of postmodernism.

Third, cyberterrorism is also a postmodern strategy for spreading terror because it seemingly has no limits, no inside or outside. The postmodern theatre of war may be fundamentally changed by the Information Age revolution, at both the strategic and tactical levels (Peters, 2004). Cyberterrorism is global and exceptionally fast and mobile. In highlighting the danger of cyberterrorism, Pillar (2001) points out the ease of movements across international boundaries and the growing potential for cyberterrorists to maneuver despite long distances. The space-time compression established by a postmodern communications environment (Lister et al., 2003) enables cyber attacks

against the Internet and other computer networks to be carried out far away, making borders, X-ray machines, and other physical barriers irrelevant. Cyberterrorism uses new computer technologies not only for improving communication and information exchange, but also for harming computer-based targets. Cyberterrorism is a reality as airport controllers have discovered to their consternation. Cyberterrorism is also postmodern because it is telegenic; it is aware that terror today must use computer media in all its forms to shape the subjectivities of the viewing public (Peters, 2004).

Fourth, and in line with these contentions, cyberterrorism is postmodern because it creates a "small world" consciousness. Thanks to the unprecedented flexibility and resourcefulness of the Internet, cyberterrorists are able to find connecting paths to other groups (of individuals with similar intentions) in remote locations with just a few jumps. The key to discovering short paths within networks is the existence of clusters of related nodes [cyberterrorist groups] in addition to "short cuts" within the network (Barabasi, 2003). These short connecting paths between cyberterrorists are the postmodern effect of human interaction in cyberspace; hence, the notion of a "small world" consciousness comes into play (Barabasi, 2002)

Fifth, cyberterrorism is postmodern because it is made possible through a self-assembly process: the Internet. In an analysis of the vulnerabilities of the Internet to cyberterrorism and destruction through malicious software programs, Albert and Barabasi (2000) came up with the idea that the Internet is a self-assembly process, which can cope with multiple minor failures. Yet, it is also in great danger *vis-à-vis* cyber attacks along its key pathways. The view of the Internet as self-assemblage is reminiscent of constructions of the fragmentary postmodern subject. This fragmentation is incomplete;

instead, the postmodern subject and the Internet possess the same characteristics of having central lines of construction, with many potential and variable outcomes (Albert & Barabasi, 2000).

As one can see, the cyberterrorist can be the one next door, a "mouse click away," or 10,000 miles apart, still a mouse click away. Through multiple representations of the self, new conceptions of space and time, all of which are made possible in a "small world" consciousness, cyberterrorism is a postmodern way of spreading terror. The new world order of terrorism has already started. What comes next is a description of how difficult the task is for computer experts to cope with the postmodern organizational structures of cyberterrorists.

Postmodernism and Cyberspace: An Organizational Challenge

Networks are the basis of globalization and communication. As humans naturally form a network society (Castells, 2000), they find that networks are group support systems. They are supportive in the sense that they "are created through coordinated activities and relationships that permeate organizational boundaries" (Stohl, 1995, p. 23). Cyberterrorists also have the very characteristic of using networks to communicate. Thanks to this, they are able to create worldwide liaisons; they realize that communication in cyberspace is so easy and accessible to anyone that networks can ensure efficiency and security in many situations. Cyberterrorist networks are self-organized, rapid, efficient, and flexible. They represent an organizational innovation (Berger, 1998), but also an organizational challenge to computer experts and law enforcement agents in their attempt to track down those responsible for cyber attacks. The fact is that it is very difficult to control the flow of information on the Internet

because the volume of information is colossal and access is decentralized (Matusitz & O'Hair, in press). This is a perfect trait of postmodernism.

Cyberterrorist networks are postmodern because they cross continental borders within seconds; they have no fixed geographic centers and they rely on the software of ideas rather than the hardware of the Army, Navy, or Air Force (Matusitz & O'Hair, in press). The Internet facilitates easy exchange of information; cyberterrorists can remain distant from areas where they are considered *persona non grata* (Matusitz & O'Hair, in press). Terrorism has moved from hierarchical toward information-age network designs (Arquilla, Rondfeldt, & Zanini, 1999). This is an organizational challenge because, in the past, law enforcement agents would know who was who behind terrorist acts (usually a country or a leader from a hierarchical terrorist organization). In this day and age, the postmodern type of network of terror is horizontal and flat, and not vertical and bureaucratically governed (Matusitz & O'Hair, in press). As a result, more effort is required on the part of counter-cyberterrorism experts to build networks that fight networks. As it will be explained later in detail, these experts are usually cyber forensics experts who feel compelled to communicate with other agencies through networks. Yes, through networks, just like cyberterrorists do.

Cyberterrorist networks are postmodern because they are organized in a fully networked, decentralized, and "all-channel" (Bavelas, 1950; Leavitt, 1951) manner. Recall that the "all-channel" network implies that any node in the network is connected to any other node. No wonder why the main backbone of cyberterrorist networks is not a top-down hierarchy, but a massive set of interconnections through the Internet. These interconnections are established so quickly that it takes a lot of patience and tremendous

skills for computer experts to catch even a potential linkage that has been made between cyberterrorists. Cyberterrorist networks contain extremely developed IT structures that support flexible emergent systems of communication (Monge & Fulk, 1999). These organizational structures enable communication relationships that go beyond organizational levels and boundaries. Flexibility, in turn, "implies that these relationships wax and wane" (Monge & Fulk, 1999, p. 71). One can very well imagine how complicated this "wax-and-wane" element can be for those who do not have the necessary means or expertise to track down cyberterrorists.

What adds to the success of cyberterrorism is not only the simple stance of carrying out attacks while staying "in the dark" (Arquilla & Ronfeldt, 2001) or by remaining anonymous, but also the fact that the Internet allows cyberterrorists to structure their networks with virtually no risks involved. This postmodern method of causing harm on the Internet and computers is truly a challenge for international computer security. For the past several decades, postmodern theorists such as the deconstructionist Jean Gebser (1985) have been discussing changes in our perception of time. Their main argument is that time is not fixed. While conventional terrorists still have notions of time as they know it in real life, where the fundamental concepts for understanding reality – that is, space, time, and distance – do not change (Matusitz & O'Hair, in press), cyberterrorists have altered these notions of time as cyberspace drives them to cross the spatial divide. This puts an end to geography. Cyberterrorists are only a mouse click away from Web servers in China or Russia. For Cairncross (1997), this even means the death of time.

Truly, cyberspace makes irrational and senseless the time needed for a communicative act to occur between cyberterrorist A and cyberterrorist B. By coordinating their activities via cyberspace, by living with these postmodern conceptions of time, by living in spatial emptiness [that is, in denial of any physics of spatiality and of any presence; even the presence of absence], cyberterrorist networks not only make the Internet a postmodern battlefield, but they also make their network structure extend geometry (Matusitz & O'Hair, in press). This is exactly how the Internet works. As Mitchell (1995) suggests,

> the Net negates geometry; it is fundamentally and profoundly antispatial. It is nothing like the Piazza Navona or Copley Square. You cannot say where it is or describe its memorable shape and proportions or tell a stranger how to get there. But you can find things in it without knowing where they are. The Net is ambient – nowhere in particular and everywhere at once (p. 8).

Considering all this, it is not surprising how challenging it is for cybersecurity experts and law enforcement agents to identify cyberterrorists. Yet, the reason why most cyberterrorist attempts have failed does not lie in the fact that cyberterrorist networks are weak or that they have relatively low impact. The reason is that cybersecurity experts have the required knowledge, skills, and expertise to resist cyber attacks; they install firewalls and other preventive measures. The last sub-section of this discourse on postmodernism pertains to the absence of leadership in cyberterrorist networks.

Postmodernism and Cyberspace: Where No Leadership Is Needed

We saw earlier that, from an organizational vantage point, postmodernism in cyberspace is reflected in the transition from a centralized, hierarchical, and rigid

organizational structure to a decentralized and very flexible structure. Postmodern networks of terror also have flat, horizontal type of structures that do not require cyberterrorists to have a leader and that allow them to operate in an "all-channel" (Bavelas, 1950; Leavitt, 1951) manner. Since no leadership is needed, cyberterrorists do not have rigorous schedules to follow; they do not have long correspondence times of weeks, or even months. Instead, they are able to communicate on a daily basis, masking their identities and movements by operating in a series of Internet cafes (Ballard, Hornik, & McKenzie, 2002).

For sure, cyberterrorists do not require permission for action from a leader, even if cyber attacks require the formation of a network. It goes without saying that cyberterrorists do not need a collaborating or weak government to harbor them as they train and plot. The majority of cyberterrorist acts are in fact not state-sponsored. In the cyberterrorist world, there is just no single, central leadership. Neither are there headquarters (Matusitz & O'Hair, in press). While the chief leadership of a conventional terrorist group does give orders and assignments, if the members of the group become cyberterrorists, they will tend not to follow the leader(s); rather, they will use him or her as a messenger, go-between, or gatekeeper. Nevertheless, the group will remain a sophisticated organization with vast capability.

Beyond doubt, cyberspace alters the very concept of terrorist leadership. Even the most fundamental leadership techniques have been transformed by the influence of the Information Age and its highly sophisticated technological resources. Postmodernism questions the necessity of reason in the service of power, and the types of leadership that require unification and harmony within centrally governed chains of command (Williams

& Sewpaul, 2004). In the same perspective of postmodernism, the upcoming section is an examination of how the battle between computer experts and cyberterrorists can be explained through the central tenets of game theory. As the argument will be made, in this analysis of social networks of cyberterrorists, game theory is a solid supplement to social network theory.

A Postmodern Theory of Terrorism in Cyberspace: Game Theory

Postmodern Internet-based terror reapers are cyberterrorists; they constantly seek to turn the technological superiority and complexity of their targets into liabilities rather than assets. Just look at how immeasurably vulnerable our postmodern society is in the face of malicious software programs or any destruction – or even any disconnection – of our information systems or power supplies. Despite the fact that abundant technical safeguards may be created by the finest experts worldwide, the dangerous game we have to face against cyberterrorists will be a strategies-versus-counterstrategies game in which the players who will prevail will be those who possess the structural advantage. In many cases, to disrupt is, so to say, structurally less difficult than to protect. Hence, the modern protectors may be playing a losing game against the postmodern disruptors. This section purports to analyze how the battle between computer experts and cyberterrorists can be explained through game theory, which, in this study, perfectly complements the role of social network theory. Many applications of game theory are related to economics, political science, voting decisions (Bilbao et al., 2002), as well as other numerous domains, including an important one in this study: law enforcement (Fent, Feichtinger, & Tragler, 2002).

Rationale for Using Game Theory

Game theory is important in this study because the theory examines the relationships between individuals or groups, using models with clear statements of consequences (individual payoffs) that depend on the actions taken by more than one individual (Aumann & Hart, 1992; Fudenberg & Tirole, 1991; von Neumann & Morgenstern, 1944). The rationale for using game theory in this study lies in the fact that game theory is about power and control. It deals with two-person (or more) decision-making situations (with opposing or joined interests). As explained later, game theory can also be applied to the study of cyberterrorism. Since games frequently reproduce or share characteristics with real situations, they can offer strategies for dealing with such circumstances. The basic assumption is that the players (decision makers) follow specific objectives and take into account both their skills and expectations of the other player's (decision maker's) behavior.

Another reason why game theory is suited for this study lies in the fact that, against opponents who carry out attacks in a postmodern fashion, conventional strategies lead nowhere. The cyber attacker and the computer security agent not only engage in real-time game play; they also use strategies that are not conceivable in conventional conflict. Game theory can explain how viruses evolve through carefully taken actions (Turner, 2005). For this reason, the theory can greatly contribute to a better understanding of cyber strategy and its implications. For instance, when a public Web server administrator notices something unusual in the network (i.e., caused by a DOS attack), he or she may suspect that an attack has occurred and that action must be taken now. This implies that the two players are in the same context. One player wants to attack a

computer system; the other wants to protect it. The context involves short-term strategies on the part of both sides. The interactions between the cyberterrorist and the computer security agent are to be viewed as a postmodern two-player game. The goal here is to explain what strategies are used by both players and how computer security agents can use the outcomes of the game to improve the security of their network.

Origins of Game Theory

Game theory was first outlined by John von Neumann, a Hungarian-American mathematician, in a paper entitled "Theory of Parlor Games" that he presented at the Mathematical Society of Göttingen in 1928 (von Neumann & Morgenstern, 1944). In his paper, von Neumann laid out a mathematical model for identifying the best strategy for a player to achieve the greatest possible results with minimal losses in any type of contest (that involves more than one player). In order to do so, von Neumann examined the tactics in which either of two players could make moves so that he or she could achieve the optimal "pay-off" at any given moment in the game (Poundstone, 1992). von Neumann's inspiration for game theory was poker. Poker, for von Neumann, was not based on the theory of probability alone. Rather, an important factor in the victory of any of the player is the idea of "bluffing," a strategy used to deceive the other players or conceal information from them (Poundstone, 1992).

A couple of years later, von Neumann collaborated with Oskar Morgenstern, an Austrian economist at Princeton, to develop game theory into a book. Their book, "Theory of Games and Economic Behavior" (von Neumann & Morgenstern, 1944), radically changed the field of economics. In fact, the winners of the 2005 Nobel Prize in Economics were two game theorists, Thomas Schelling and Robert Aumann. The former

is best known for tackling practical questions, while the latter, a mathematician, is credited with more theoretical contributions (Holden, 2005). Game theory has also had a significant impact in the domains of psychology, sociology, politics, political science, terrorism, warfare, games (i.e., chess and simulation games) and, for the past twenty years, video games, the Internet, and many emergent fields.

On a side note, game theory has been successful in the social sciences because it pertains to fundamental studies of diverse aspects of collective behavior: care for others vs. selfishness and cooperation vs. competition. Game theory has also been used by social scientists to predict which behaviors can spread through a particular group of people, particularly in contests involving classic strategies such as "trust" versus "cheater" (Turner, 2005).

Description of Game Theory

Game theory studies how individuals behave when they are placed in situations that require them to interact with other individuals. As a branch of applied mathematics, the theory analyzes rational behavior in interactive or interdependent situations and proposes a set of mathematical tools and models for analyzing these interactive or interdependent processes (Neel, 2005). It rests on the premise that each person "must first know the decision of the other agents before knowing which decision is best for himself or herself" (Jehle & Reny, 2001, p. 267). As the theory suggests, a game consists of players. The number of players does not matter, but the theory is best applicable when the number of players does not exceed "a few." So, each person is a player in the game and the player is also a decision maker, choosing how he or she acts. Because each player wants the greatest possible consequence according to his or her preference, every

decision made by each player will have an impact – whether positive or negative – on the outcomes of the game. In other words, each outcome is the result of particular moves made by the players at a given point in the game (Rapoport, 1974).

The fundamental characteristic of game theory is the assumption that players are rational and, therefore, look for the maximization of the difference between their own costs and benefits when considering an action they want to take. In other words, by providing tools for analyzing strategic interactions among two or more players, game theory uses simple models to study complex interactive relations. The advantage of this is that game theory helps illustrate the potential for – as well as the risks associated with – collaborative behavior among distrustful players in the game. As one can see, this all looks like a chess game, where each player does not know what moves his or her opponent will take. Therefore, each of the players must find a strategy to examine the possible actions of each other in the situation. The ultimate goal is to determine the best course of action for himself or herself (Jehle & Reny, 2001).

Below is a model of how game theory is used to simulate real-life situations. The model typically contains five elements and is based on Rapoport's (1974) explanation of game theory:

1) players (or decision makers);

2) strategies available to each player; each player has several choices at any given time during the game; every possible strategy pursued by each player leads to a defined end-state (either a "win" end-state, a "lose" end-state, or a "zero-sum" end-state);

3) rules that govern each player's behavior; each player has full knowledge of the rules; violating the rules can lead to an end-state that would have been different had one or all players followed them;

4) outcomes; each outcome is the result of particular choices made by players at any given point in the game; and

5) payoffs accumulated by each player as a consequence of each possible outcome; a player will always take the path that will result in a greater payoff to himself or herself (which means that each player knows the payoffs both to himself or herself and the opponent(s) at any given end-state).

According to Rapoport (1974), these elements assume that each player seeks to follow the strategies that will help him or her accomplish the most beneficial goal in every situation. Of equal relevance is that game theory implies strategic thinking about how player A will act in a situation where his or her moves will affect player B, whose moves, in turn, will have an impact on player A. What comes next is a description of four types of outcomes that result from the actions taken by the players in the game: (1) the Nash equilibrium, (2) the zero-sum game, (3) the positive-sum game, and (4) the negative-sum game.

Nash Equilibrium

The concept of Nash equilibrium was coined by John Nash (1950), a game theorist and famous 1994 Nobel Prize winner (Milner, 1995). It refers to the outcome of a game that occurs when one player takes the best possible action based on the action of another player. Likewise, the latter player takes the best possible action based on the

action of the first player. In the Nash equilibrium, both players perform their dominant strategies. What this means is that none of the two players would change his or her strategy if they were offered the chance to do so at the end of the game. So, each player makes the best decision for himself or herself that he or she can, taking the actions of his or her opponent as given (Mehlmann, 2000).

In addition, the Nash equilibrium also implies that each player maximizes his or her own actual or expected payoff. Recall that the payoff is the outcome obtained by a combination of decisions. Again, each player takes the other player's current strategies as given (Nash, 1950). So, a player has nothing to gain by changing only his or her own strategy. If a player has chosen a strategy and if he or she cannot benefit by changing his or her strategy, while the other player keeps his or hers unchanged as well, then the current set of strategies and the payoffs that result from the outcome of the game constitute a Nash equilibrium (Fudenberg & Tirole, 1991).

Zero-Sum Game

A zero-sum game is a game in which the interests of each player are diametrically opposed (von Neumann & Morgenstern, 1944). In other words, regardless of the outcome of the game, the winnings of one player are exactly balanced by the losses of the other player. What this means is that each of the payoffs must be the negative of the other(s) (Fudenberg & Tirole, 1991). The outcome of the game is named "zero-sum" because when a player adds up his or her total gains and subtracts the total losses of the other, they will sum to zero. All in all, player A can win only at the expenses of player B (or vice versa) and the benefits and losses to both player A and player B amount to the same value (von Neumann & Morgenstern, 1944).

Positive-Sum Game

A positive-sum game is a situation in which each player can benefit from the actions taken by all players, even if some players benefit more than others. Thus, it can result in one player losing and another gaining with an overall gain (Mehlmann, 2000).

Negative-Sum Game

A negative-sum game is a situation in which the actions of each player hurt both themselves and their opponents. It can also result in one player losing and another gaining with an overall loss (Mehlmann, 2000).

Cooperative vs. Non-Cooperative Game

As one can see, different outcomes are possible. Given this, it would be interesting to know if computer security experts should better engage in cooperative behavior instead of non-cooperative behavior (or vice versa) when facing cyberterrorists. Simply defined, a non-cooperative game, in game theory, is one where each player pursues his or her own interests independently. In a cooperative game, players form coalitions and combine their decision-making problems (Basar & Olsder, 1999). Let us focus on a past collaborative situation very briefly. According to Verton (2001b), it is sometimes the case that investigators from the Federal Bureau of Investigation develop close relationships with cyberterrorists through the use of chat rooms (Internet Relay Chat rooms). Rapidly, cyberterrorists are asking the investigators to take part in coordinated cyber attacks and eventually they offer, in exchange for their participation, to share stolen information (Verton, 2001b). Here, the two parties work together and do fairly well in their collaboration ("If you participate in our cyber attacks, we will give you what you need").

The Role of Communication in Game Theory

Communication plays a central role in game theory because the theory involves the analysis of conflict, cooperation, and the degree of communication needed to reach a desired outcome by each player (Osborne, 2003). Game theory also deals with strategic interaction. A strategic interaction requires that the players make decisions; the outcome of the game depends on the players' choices. A strategic interaction inherently involves human communication. For instance, the cyberterrorist needs to find a way through communication and trust in order to reach a collaborative outcome with the computer security agent. In fact, in a collaborative game, the ability with which each player communicates, the intensity of communication, and even the organization with which these players communicate can deeply affect – whether positively or negatively – the outcome of the game (Osborne, 2003). If there is no communication between two players, then no cooperation can be formed. However, if they can communicate and engage in cooperative behavior, the outcome would be quite different. For this reason, repeated interaction might lead to different outcomes.

Applications of Game Theory in the Study of Terrorism

Several game-theoretic models of terrorism exist (see Sandler & Hartley, 1995). Since the 1980s, a group of scholars in economics and political science have applied game theory to the study of terrorism (Lapan & Sandler, 1988, 1993; Lee, 1988; Scott, 1991; Selten, 1988), which refers to the premeditated use or threat of use of violence in order to achieve political objectives through intimidation or fear (Overgaard, 1994). Sandler, Tschirhart, and Cauley (1983), for instance, offer a rational-actor model that explains the negotiation process between terrorists and federal counter-terrorism agents

for hostage crises or property seizure (and where demands are issued). In the model created by Sandler, Tschirhart, and Cauley (1983), the terrorists' assessment of the likely concession to be given by a government is contingent upon a probability distribution, conditioned on previous governmental concessions. The analysis made by Sandler and his colleagues (1983) shows that the choices and actions made by the terrorists are influenced by those of the government and vice versa.

Game theory has also been applied in the analysis of terrorists' choice of targets, for a three-player game that involved two targeted countries and a common terrorist threat (Sandler & Lapan, 1988). In this game, each country independently chooses its deterrence expenditures. The goal is to determine the terrorists' probability of logistical failure on that nation's soil. The terrorists choose the option for the highest expected payoff for their attack. Each country's choice of deterrence bestows benefits and costs on the other target. By transferring the attack abroad, each country imposes an external cost on its counterpart. Yet, by limiting the number of attacks and their gravity at home, each country offers an external benefit to foreign residents.

There are other applications of the game-theoretic model that could be described in great lengths, such as the one that analyzes a situation where the terrorists know their true strength, but the targeted country must estimate the terrorists' resources based on the level of their attacks. If, for example, the country knows that the terrorists have sufficient resources to force the country to surrender eventually, then the most beneficial strategy for that country is to concede at the outset and suffer no damage (Sandler & Lapan, 1988). The application of game theory to cyberterrorism contains the same fundamental elements needed for the players to reach their desired outcomes, as it is explained next.

Game Theory as Applied to Cyberterrorism: An Overview

Just as we are able to understand the strategies used by conventional terrorists in a particular game, we may also be able to understand how cyberterrorists act in a given situation. Two basic principles that make up game theory are that the players are rational and intelligent in strategic reasoning. With respect to cyberterrorists, why do many of them try to destroy the computer system of the Pentagon or other federal agencies? Why do they not cripple more targets outside those organizations? The answer to these to questions is simple. Cyberterrorists like to commit malicious acts where they believe it will help influence those who make decisions directly in the way of the cyberterrorists' goals. A network of cyberterrorists has as its main objective to cause damage to the computer system that it attacks. This damage can take many forms. First, any action undertaken by the computer network to strengthen its security system against attacks generates benefits for the cyberterrorists because it imposes costs on the computer network. Second, any move taken by the cyberterrorists that causes damage to the computer network increases benefits for the cyberterrorist (i.e., self-glorification as the "enemy" suffers, and so on).

Conversely, the response from the computer network against a cyberterrorist action can be twofold: retaliation (offensive) or conciliation (collaborative). Oddly enough, collaboration between the attackers and the defenders can contribute to the shrinking of the cyberterrorist network by reducing the number of members who were part of their network. What happens is that the computer network can make it appear that the conciliation was not the result of the actions taken by the cyberterrorists. Consequently, some of the members may feel that the cyberterrorist attacks in question

have not carried the impact they had hoped. In reality, though, the end-result is a draw (or a win-win outcome). Retaliation can also increase winnings for both sides because it expends resources.

The outcome can also be a Nash equilibrium. According to Lye and Wing (2005), a Nash equilibrium gives a computer security expert – or even a public Web server administrator – an idea of the cyber attacker's strategy "and a plan for what to do in each state in the event of an attack" (p. 9). Finding additional Nash equilibria allows that public Web server administrator to learn more about the cyber attacker's best attack strategies. Just like in a chess game, player A (say, a computer security agent) does not know the next move of player B (the cyberterrorist) and vice versa. Player A only needs to act when an attack on the computer network is suspected. It is fair to assume that both players know what each other is capable of doing. Yet, they do not know what each other's next move will be. Again, it is just like a chess game, where the game is evolutionary.

Game Theory as Applied to Cyberterrorism: A Postmodern View

As opposed to conventional war techniques, game theory in cyberspace allows for the use of grand strategies aiming at fast and easy disintegration of the respective opponent. Not only can a player make multiple moves simultaneously (as if he or she were composed of multiple selves), but, also, both players can make multiple, simultaneous moves in the same context as well. While in most conventional games, players alternate moves, in cyberspace this is not true anymore. An opponent can launch multiple, simultaneous attacks easily and quickly (Littman, 1994). What this also means is that time is not "constraining" in the context of cyberterrorism. In other words,

opponents in cyberspace are under no time control constraints (Carmel & Markovtich, 1996). Timing for move and state updates is not fixed. Neither is it defined. In actual space, time is perspectival (Gebser, 1985), while in cyberspace, time is "aperspectival." For this reason, time becomes a "fluxing intensity, rather than a fixed extensity, and as such it is not prone to being fragmented into identical and repetitive units of measurement such as past, present, or future" (Kramer, 1997, p. 122). This is postmodernism.

On a side note, remember our description of the terrorist networks created by the Zealots and their comrades in Antiquity. Game theory would perfectly apply in that context. The Zealots and the Romans were clear opponents. The rules of the game were different than those in cyberspace: the Zealots and the Romans were taking actions against each other in a linear dialectical process. They were learning from each other's tactics as they were networking and creating cells at the right locations. One of the game strategies that could not be used was spying or infiltration. For instance, it was difficult for the Zealots to infiltrate the Romans because the terrorist game they were playing occurred in actual space. A Zealot was clearly a Zealot, that is, a Jew possessing well-defined Jewish facial features, speaking Hebrew, and so on. However, on the Internet, there is so much anonymity that it is not only difficult to tell what game the cyberterrorist is playing or what network he or she is involved in; it is also difficult to determine who the other player is or what his or her ulterior goal is. Is the other player a real threat or is it just an FBI agent acting as a cyber spy? Because of the postmodern nature of the Internet, and because of the absence of spatiality (as opposed to the spatiality during the period in Antiquity), the Web user can move effortlessly across the spatial divide.

The fragmentary aspect of the Internet and communication in cyberspace gives each of the players more autonomy to create their own environment and identity. While modern identity is a location, postmodern "identity" is nonlocalizable, and "therefore often seen as nonidentity" (Kramer, 1997, p. xviii). Because they are able to change their identities every second with just one mouse click, cyberterrorists are free from imposed rules and social constraint as they know it in the perspectival, physical world. Is the other player a real threat or is it just an FBI agent acting as a cyber spy? Because of the postmodern nature of the Internet, and because of the absence of spatiality, the Web user can move effortlessly across the spatial divide. When confronting each other in cyberspace, the cyberterrorist and the computer security agent find themselves in a space and time that are aperspectival. Kramer (1997) writes extensively on aperspectival time. For Kramer,

> aperspectival time is a dimensional constituent of the world. Time is not anywhere, nor is it going "anywhere." Nor is time a "constant." Instead, it enables "going." It enables difference, constance (identity), and discontiguity. In the aperspectival universe of infinity and eternity, the center is everywhere and the circumference nowhere. Every "place" and "person" is the/an *axis mundi*, the center of everything as well as an edge. Because there is no single edge one is always the center and never the center (p. 122).

Based on a game-theoretical model, the traditional way of looking at conflict is the following: is there another strategy to evaluate the opponent? How do his or her actions differ from mine? How likely am I to win the conflict? Or how likely is my opponent to lose the conflict? In the context of cyberterrorism, this symmetry tends to be

broken. Postmodernism always implies change and fluidity. This is Derrida's (1967) deconstruction of meaning and of the Other's sense-making and intentions. The player's opponent may have an end goal that is compatible with his or hers. Likewise, the opponent may be trying for something that the player does not like, yet the opponent does not compromise the critical objectives of the player's mission (Hsu et al., 1990; Tesauro, 1994). Also interesting is that the Internet and computer technology allow players to change their goals more quickly and more frequently (Carmel & Markovitch, 1996). They can even change the rules. In most games, the rules are known by all participants beforehand. In the situation of cyberterrorism, anything goes.

In line with these views about change and fluidity, the opponent's resources may change during the game, based on new tools, new weapons, new techniques, new strategies, all of which can be acquired within seconds. Any network that is unable to handle that is at a critical disadvantage. In cyberterrorism, where new opportunities for attack are rapidly, effortlessly, and repeatedly introduced, online learning of these opportunities for increasing the chances of achieving the expected desires and outcomes is a starting point. It certainly is a good approach. Plus, the opponent may be able to design programs that will get a computer network in bad habits, which the opponent can later exploit for his or her own purposes. Programs susceptible to this are called "leadable" (Littman, 1994). One approach to resisting leadability is to learn only from mistakes, not from successes. The idea of losing the game is not always a bad idea, since computer security agents can learn from mistakes. This is where game theory perfectly fits. The approach just mentioned limits the opponent's power to use rewards for bad moves to train the computer security agents' network (Littman, 1994).

Intersection of Game Theory and Social Network Theory in the Study of Cyberterrorism

The reason why game theory can intersect with social network theory in the study of cyberterrorism lies in the fact that the Internet is a large-scale communication network that cannot be managed by one central authority, but by various nodes or hubs communicating among each other and that use all sorts of strategies. Some of those nodes or hubs are cyberterrorists themselves and they are also part of the game. This lends to the analysis of the network system using the game theory model, in which communication paths or data streams can be altered by selfish nodes – cyberterrorists in this study – who try to cause damage or modify the state of the network. Besides, instead of being a homogeneous network where users interact safely and in an honest way, the Internet is more like a social network of heterogeneous, selfish users who try to maximize their personal desires (Floyd & Fall, 1999). This is where game theory and social network theory intersect. Game theory is a natural modeling framework for understanding how nodes in the network make decisions independently and how they seek to optimize their desires by using strategies. Computer security agents happen to be the standard defenders of the network (Floyd & Fall, 1999). They have to intermingle with cyberterrorists and use different strategies in order to reach their desired outcomes (for the benefit of the network, of course).

The scenario on the next page (Figure 4) represents our game model during the interaction between a cyberterrorist and a computer security agent. The public Web server, the private file server, and the private workstation are very important nodes in the graph. Since these three nodes are highly connected to thousands of computers, they are actually hubs. The cyberterrorist represents an external node, very small, working from a

single computer. The cyberterrorist is not a hub; however, his or her actions could be damaging. The links that we see are direct communication paths. The computer security agent can work, for instance, from a private workstation and can have direct access to all the features of the public Web server.

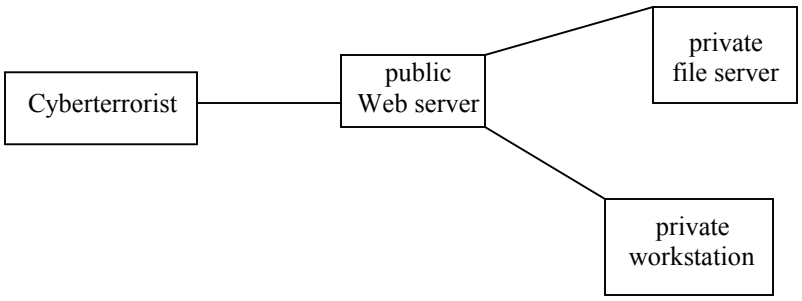

Figure 4 *Example of a local network attacked by a cyberterrorist*

From a game theory perspective, all kinds of strategies are available to each player. For example, "a common target for use as a launching base in an attack is the public Web server" (Lye & Wing, 2005, p. 4). By using this hub as a springboard from which serious damage could be inflicted, the cyberterrorist could try to flood private-home computers with sniffer programs or viruses. No matter what, until the cyberterrorist takes action, the computer security agent does not know whether there is an attacker or not. He or she does not even know about the existence of the node. Plus, we should keep in mind that not all actions taken by the cyberterrorist can be observed. Once the game has started, each player has several choices at any given time during the game. An action pair (composed of both the cyberterrorist and the computer security agent) can cause the local network to move from one state to another (Lye & Wing, 2005).

There are highly expected payoffs based on the actions taken by each player. The cyberterrorist's rewards might be in terms of the amount of damage done to the network. For instance, a "defaced corporate website may cause the company to lose its reputation and its customer to lose confidence" (Lye & Wing, 2005, p. 3). This is a reward for the cyber attacker. By the same token, disrupting a hub (public Web server) can be the desired outcome of the cyberterrorist, even if it just takes 15 minutes for the public Web server administrator to determine the strategy that was used and restart the service. On the other hand, the reward of the computer security agent would be to see the strategies taken by the cyberterrorist fail, which happens in most cases (Mitnick & Simon, 2002). The game can be a "cooperative" type of game if a cyberterrorist uses inducements to get a public Web server administrator to take actions that will reach a positive outcome. The choices and actions made by the cyberterrorist can be influenced by the administrator (and vice versa). For example, the cyberterrorist can urge the administrator to install two levels of password protection to make the effort required to wreaking havoc more challenging to the attacker. Maybe he or she would love that. It might be the case that the cyberterrorist wants the network to be in a very good state in order to create the biggest damage. After all, it takes a big target to create big damage.

Based on the motives of the attacker, the administrator might, in turn, increase security to prevent him or her from carrying out their plan. The cyberterrorist might perceive this next move as a trade-off. Conversely, computer security agents might be able to contemplate the idea that, while unknown cyberterrorist actions may occur at any time, some of their moves are more likely to occur than others. As such, if a cyberterrorist is presumed to have access to a particular hub within a network, the

chances of being able to perform a previously unknown move using that hub are much greater. The task of cyber officers, then, becomes easier. Now that we have seen how computer security experts cope with cyberterrorists through various strategies and techniques, based on game theory intermingled with social network theory, let us focus on the types of networks they create in order to thwart, or be cognizant of, networks that cyberterrorists web or span for themselves.

It Takes Networks to Fight Networks

It takes networks to fight networks. These six words were stated by Arquilla and Rondfeldt (2001). Hierarchies are clumsy techniques to use against cyberterrorist networks. Since our government purports to defend its universities, organizations, hospitals, businesses, and other agencies (and all its citizens) against cyberterrorism, it might be interesting to understand what networking designs and strategies are used in order to stop, or at least, to understand social networks of terror. This does not mean imitating the cyberterrorist networks *per se*; rather, for law enforcement agencies, IT networks, and cyber forensics labs, it means learning to draw from experience or previous encounters of their networks. Hopefully, readers will have a better understanding of the rise of network forms in the Information Age (Arquilla & Rondfeldt, 2001). Networks between the agencies and groups mentioned above rely heavily on technological innovation, as well as the development of new mechanisms for interagency and multi-jurisdictional collaboration (Arquilla & Rondfeldt, 2001).

The literature tells us that it is necessary for governments, in their tracking down of cyberterrorists or recovery of seized and frozen data, to consult with local officials and other cyber organizations in order to maximize their outcomes (Rist & Chee, 2004). As

explained in this section, the network of computer security experts and other important agents is enabled by cyber forensics experts involved in federal or local networks (i.e., experts from university cyber forensics labs, etc.), immediate incident responses, and high-rate security analysis tools (Rist & Chee, 2004). Note that it is not easy for cybersecurity experts and law enforcement agents to identify networks of cyberterrorists. Yet, the reason why most cyberterrorist attempts have failed does not lie in the fact that cyberterrorist networks are weak or that they have relatively low impact. The reason is that cybersecurity experts have the required knowledge, skills, and expertise to resist cyber attacks. They install firewalls and other preventive measures.

Lack of Cyber Forensics Expertise in Law Enforcement

The majority of law enforcement agencies do not clearly recognize occurrences of cyberterrorism (Aeilts, 2005). As Goodman (2001) puts it, "victims may have serious doubts about the capacity of the police to handle computer crime incidents in an efficient, timely, and confidential manner" (p. 13). Ten years before Goodman wrote this quote, Hafner and Markoff (1991) already remarked that law enforcement agencies were frequently ill-prepared and insufficiently trained to capture computer criminals and handle digital evidence. The technologically-related hurdles that might prevent nations from mitigating cyber threats primarily deal with the tools and knowledge used in cyberspace. Put in layperson's terms, law enforcement often lacks the appropriate knowledge to keep up with cyberterrorists (Gabrys, 2002). Many people involved in computer forensics feel the main problem is the lack of education in law enforcement relating to cyberterrorism and the like. Law enforcement agents have devoted themselves to the high-degree crimes, lumping cyber crimes into a low priority status. Yet, the

financial losses resulting from a computer attack could fund a small country (Zangrilli, 2002). Fortunately, for the past few years, things have gotten better; computer technology has increasingly been valued in the realm of law enforcement that used to wage wars without computers. As a matter of fact, law enforcement agencies are backed up months in cyber forensic investigations (McGinn, Raymond, & Joseph, 2002).

Cyber Forensics: An Area for Fighting Networks of Cyberterrorists

Cyber forensics experts are computer experts with highly technical skills. Cyber forensics, also known as computer forensics, is a method to improve investigation into an ever-growing era of crimes that uses computers, computer-aided terrorism, cyberterrorism, espionage, bank and business fraud, and identity theft (Thilmany, 2004). Cyber forensics refers to retrieving and analyzing evidence from computer systems, including small bits of computer hardware and electronic data on the Internet (Delio, 2005; Holsapple, 2005; Smith, 2000). A similar definition of cyber forensics is that it is the identification, examination, and reconstruction of evidence that is extracted from any element of computer systems, computer networks, computer media, and computer peripherals that allow forensics analysts to solve a computer-related crime (Hosmer et al., 2000). Cyber forensics experts usually have solid knowledge in a wide range of computer/networking hardware, software, and operating systems.

Part of cyber forensics is what is also called "network forensics." Network forensics experts preserve, identify, extract, document, and interpret network data (Roberts, 2005). Network forensics lies at the interface between electronic information systems and the law, and also involves reviewing a compromised network and figuring out step-by-step what happened (Prosise & Mandia, 2001). Network forensics experts

have three functions that make up networking security more reliable: (1) to analyze vulnerability assessment and risk management, (2) to detect network intrusion and incident response, and (3) to ensure computing and networking forensics by making computer systems more secure. One recent way to do this has been closing computing/networking loopholes exploited by cyberterrorists to launch attacks, such as Denial of Service (DOS) (Oklahoma Digital Forensics Lab, 2005).

Who Is Part of the Network Fighting Networks?

According to the cyber forensics lab at Purdue University, there are four network communities involved in cyber forensics: law enforcement, military, private sector, and academia (Cyber Forensics at Purdue University, 2005). To begin with, law enforcement officers have been encouraged to learn the arts of digital forensics (Boyle, 2005). When working with an ongoing investigation, it is important for them to be able to gather evidence as fast as possible (Holsapple, 2005). Plus, cyber forensics software can protect electronic evidence for use in investigations (Boyle, 2005). Because computers are machines that can stay in a lab waiting to be processed for a year or more, it gives malicious hackers time to hide their traces before evidence can be collected and processed. Therefore, gathering evidence in a quick fashion allows law enforcement agents to discover new leads early in an investigation (Holsapple, 2005). The Federal Bureau of Investigation is seriously involved in cyber forensics (Beucke & Grow, 2005; Moore, 2005).

Second, the military is also involved in vast network of computer security activities that aim at purging cyberterrorists from the digital realm (Swartz, 2004). Not only does the U.S. military have cyberwar tools and cyber-warfare capabilities, but they

also collaborate with local organizations and defense experts (Fisher, Nobel, & Taft, 2003). Another collaboration is the one between military, security, and corporate bodies, all of which know that the United States is vulnerable to a full-scale electronic attack (Graham-Rowe, 2003). Let us not forget to mention the importance of cyber crime centers around the nation for the military investigation of digital evidence. For instance, investigators in the Army, Navy, Air Force and Marines frequently contact the cyber forensics lab in Baltimore to analyze digital evidence that is held as part of the military's most complex cyberterrorism-related investigations (Messmer, 2005).

Third, the private sector is also seriously involved in the network against cyberterrorists. The main reason stems from the fact that cyberterrorists have already manifested themselves by using worms or viruses they plant on our personal home computers to launch assaults on private-sector infrastructures (McCracken, 2004). Since companies today rely heavily on cyberspace and the Internet, they tend to network with organizations that ensure Internet safety. Such organizations encourage researchers and developers to join forces in the identification and patching of vulnerabilities (McCracken, 2004). The private sector is also collaborating with the U.S. Federal Government, which, for a couple of years, has taken a leadership role in stopping cyber attacks and other intrusion attempts. One such leadership role is the creation of the National Cyber Security Summit Task Force, a group of more than three dozen corporations and organizations. The goal is to issue an information security policy framework in the resistance against hacking and cyberterrorism (Carlson & Fisher, 2004).

In a similar vein, law enforcement agencies are occasionally called upon to investigate network and computer intrusions if a hacker or cyberterrorist gains

unauthorized access to a system protected by law. The agencies must also have complete and credible network forensic evidence of potential cyber attacks if they want to prosecute the hacker or cyberterrorist or if they want to seek legal warrants to control suspected activities (Phillips et al., 2005). Federal law enforcement officials claim that cooperation is needed from the private-sector companies since they are major targets of cyber attacks. In 2002, groups were already assisting private-sector companies with protecting themselves from cyberthreats (Thibodeau, 2002). Yet, although federal and private-sector officials have created vast collaborative networks of cyber forensics support such as the network of counter-cybersabotage on the possible information technology-based failures during the summer 2003 blackout in the U.S., the World Bank demands that the private sector make exceptional efforts to work with law enforcement agencies as well as with supervisory authorities within and across borders because of the worldwide nature of Internet technology (Verton, 2003b).

Fourth, the world of academia is crucial in this investigation of networks of cyber forensics experts. A whole section is devoted to university cyber forensics labs and their important role in the collaboration with law enforcement agencies.

Social Networks among Law Enforcement Agencies

With respect to cyberdefense or cyberprotection, there is more maturity among law enforcement agencies today. They realize that a good strategy to obtain the information and resources necessary to counter cyberterrorist activities is to network or operate in a more collegial fashion. At the local level, one such collaboration occurred in March 2000, when the FBI's National Infrastructure Protection Center and the FBI Houston field office stated their investigation into a computer virus that was believed to

have targeted the 911 system for massive disruption (Verton, 2003a). The growth of the FBI's Infra Guard Program, a voluntary organization of companies that both provide information and get information, has demonstrated that joining forces is better than acting alone (especially when it comes to cracking down on threats and risks).

Social Networks between Law Enforcement Agencies and Cyber Forensics Labs

The U.S. Federal Bureau of Investigation employs cybersecurity experts to flush hackers and cyberterrorists out of our digital systems. Cybersecurity technicians work for government agencies worldwide and must keep up with brand-new technology (Moore, 2005). Lance Hawk, a Philadelphia-based cyber forensics expert, trains investigators for law enforcement agencies such as the FBI. Hawk says that the demand is high for specialties such as detecting and fighting computer viruses, worms, Trojan horses, and spyware. Cyber forensics, Hawk continues, has become one of the hot professions in the FBI. Applicants usually must be twenty-three years old. Yet, the call for experts in this field is so colossal that the FBI is making exceptions to that requirement (Moore, 2005).

The Federal Bureau of Investigation is not the only agency that absolutely needs skilled cyber forensics experts. Practically every federal, state, and local government agency – including the U.S. armed forces, the Department of Defense Computer Forensics Lab, local district attorneys, and local police departments – needs skilled cyberinvestigators (Moore, 2005). In order to knock down networks of cyberterrorists, law enforcement agencies also network with university cyber forensics labs (Carlson, 2004; Habeeb, 2004; Smith, 2000). For instance, law enforcement officials regularly demand assistance in pre-search warrant preparations and post-seizure handling of computer equipments (Oklahoma Digital Forensics Lab, 2005).

The National White Collar Crime Center (Mokhiber, 2000; Radcliff, 2002), or NWCCC, is the interface between criminal justice agencies on all jurisdictional levels and is a link between local and state criminal justice agencies. These agencies have economic crime-fighting capabilities and the minimum requirement for federal investigation and intervention. NWCCC provides support for the prevention, investigation, and prosecution of cyberterrorism thanks to its blend of research, training, and examinatory support services. NWCCC also organizes National Cybercrime Training partnerships, which provide training to state and local law enforcement agencies – along with district attorney's offices – in how to respond successfully to cyber incidents. The center also provides training to the Internet Fraud Complaint Center (IFCC), which is in a partnership with the FBI as well (DiNardo, 2004). What the IFCC does is offer a central analytical repository for complaints and provides victims with easy means to alert authorities of a suspected cyber violation (DiNardo, 2004).

University Cyber Forensics Labs

One such cyber forensics lab is the University of Oklahoma (OU) cyber forensics lab, called the ODFL. The ODFL, the Oklahoma Digital Forensics Lab, located at the OU Cyber Forensics Lab, has as its main goal to analyze the traces of cyberterrorists and hackers who launch attacks (through computer viruses) in order to disrupt security issues and disrupt normal functioning of the Internet. Analyzing such traces can provide precious information on the source and type of the attack. The ODFL has a research team, composed of faculty and students from the University of Oklahoma's School of Computer Science (Oklahoma Digital Forensics Lab, 2005). All members of the team

have vast knowledge on computing/networking hardware and software, and are highly qualified to carry out research projects in their fight against networks of cyberterrorists.

Another important cyber forensics lab is the one at Purdue University, part of whose mission is to act as a national center and provide support for investigations in the area of cyber forensics (Cyber Forensics at Purdue University, 2005). Purdue University networks with law enforcement agencies with a program that helps officers to quickly examine computers used to commit crimes (Holsapple, 2005). More specifically, the Purdue Department of Computer and Information Technology offers fast cyberforensics triage, which consist of training for police officers, crime scene investigators, federal agents, and other law enforcement personnel to conduct an analysis of computers suspected to have been used in a crime (Holsapple, 2005). Purdue University also participates in a federally sponsored program that establishes national standards for education and certification of computer forensics (Thilmany, 2004). One Purdue research project seeks to profile cyberterrorists' behavior based on their habits of using computers.

A third cyber forensics lab that is worth mentioning in this study is the Digital Forensics lab at the University of Central Florida (UCF). The UCF Digital Evidence division staff is composed of UCF professors from the Departments of Computer Science and Engineering Technology, law enforcement officers, and undergraduate and graduate students. The main goal of the Digital Forensics lab at UCF is to network with state and local law enforcement agents in order to assist them with cyber-related challenges (Digital Evidence, 2005). UCF Professors and law enforcement officials collaborate on a variety of digital forensics topics. Their work involves identifying, gathering, safeguarding, examining, and analyzing digital evidence (i.e., trails made by

cyberterrorists). The activities of the UCF digital forensics staff are very technical and computer-related, involving the collection and examination of evidence from computers (Digital Evidence, 2005). As one can imagine, the Digital Forensics lab at UCF is a tremendously useful source of help for agencies such as the FBI in the Southeastern area of the United States.

A fourth cyber forensics lab is the one at the University of North Texas (UNT). UNT's Computer Privacy and Security Lab has been acknowledged as one of the finest computer security teams worldwide (Coleman, 2002). Not only does the UNT Computer Privacy and Security Lab create computer security specialists, but it also networks with the Denton Police Department in Texas and other federal agencies. A fifth cyber forensics lab is the one at the University of Tulsa. This lab focuses on applying computer forensics and collaborating with law enforcement. Law enforcement agencies ask the lab at the university to examine computer evidence. Cyber forensics experts also train law enforcement officers. They train professional support technicians as well (Mercer, 2004).

Informal Social Networks

One of the formal rules in social networks is that agents are supposed to do a background check on their informants (Thornburgh et al., 2005). Yet, social networks between cyber agents and law enforcement officials can also be informal. Because the Federal Bureau of Investigation does not have a sufficient number of top-notch computer experts to recruit for cyber forensics, they will tend to rely on freelance cyber experts (Thornburgh et al., 2005). One of these "vigilantes" is Carpenter. After Carpenter made his first discoveries about a Chinese group of cyberterrorists, Titan Rain, in March 2004, he began exchanging the information with unofficial contacts that he knew in Army

intelligence. The fact is that federal rules forbid military-intelligence officers to work with American civilians (Thornburgh et al., 2005).

Nevertheless, by October 2004, the Army approved Carpenter's input, as well as his informal operations with the FBI. Carpenter says he became a confidential informant for the FBI for the five months that followed October 2004. Later, the situation was reversed. At the end, reports from his cyber-surveillance reached the primary leadership of the FBI's counterintelligence division. As a result, his work, considered illegal, was folded into an existing task force on the cyber attacks (Thornburgh et al., 2005). The morale of the story is that federal law enforcement cyber agents sometimes use informal sources like independent cyber experts (i.e., Carpenter). However, they are also paranoid about doing so, worried that these freelance cyber experts jeopardize investigations by tracking cyberterrorists too noisily or, even worse, that they are the cyberterrorists themselves (Thornburgh et al., 2005).

Ethical Dilemmas for Cybersecurity Experts

Agents from the Federal Bureau of Investigation are right when they say they should be concerned about involving themselves in informal networks with cyber experts like the one mentioned above. Yet, we should also be concerned about how our privacy has changed since the advent of the Internet and the World Wide Web. Although the Fourth and Fifth Amendments of the U.S. Constitution deal with some aspects of territorial privacy, the United States does not have a general law on privacy (Berkman & Shumway, 2003), let alone on information and communication privacy on the Internet and the World Wide Web. The Internet and the World Wide Web enable immediate communication among widely dispersed humans. Unfortunately, private communications

on the Internet and the Web are being intercepted and observed by local security and law enforcement agencies (Berkman & Shumway, 2003). In fact, the FBI has permission from any Internet Service Provider to install a machine, called Carnivore, that observes and reads email, and that monitors other online communications (Mansfield, 2000). Nevertheless, law enforcement officials still need a prosecutor's certification that what is to be investigated pertains to terrorism or cyberterrorism (Berkman & Shumway, 2003). Berkman and Shumway (2003) also note that government surveillance of our only activities is legal, according to Congress, because it is,

> largely due to a 1994 law, which mandates that digital telecommunications barriers, who control the pipelines to the Internet, design their systems to be tappable by law enforcement. In other words, the architecture of the system must be compatible with surveillance software and other monitoring programs (p. 103).

Now, we should keep in mind that what was just said only applies for surveillance or investigation that is to be performed in the United States. Under U.S. law, however, it is illegal for Americans to control or monitor foreign computers (Thornburgh et al., 2005). The FBI would require high-level diplomatic and special authorization from the Department of Justice to sneak into foreign computers. The military would have more flexibility, under a protocol called "preparation of the battlefield," to hack into foreign computers. Yet, if any American agency – whether local, state, or federal – got caught, it could set off an international incident (Thornburgh et al., 2005).

Nevertheless, the United States is keen on engaging in "domestic surveillance" behavior and checking anything that is on our computers. Part of the reason stems from the fact that several bills related to cyberterrorism and cybersecurity have been passed by

the Congress (Archick, 2003). One of these bills was under the umbrella of the USA PATRIOT ACT, as outlined below:

> The USA PATRIOT ACT (P.L. 107-56, introduced as H.R. 3162 by Rep. James Sensenbrenner in October 2001) authorizes the interception of electronic communications for the collection of evidence related to terrorism, computer fraud, and abuse (Sections 201 and 202). It also clarifies the definition of protected computers and increases fines and prison terms for damage (Section 814) (Archick, 2003, p. 5).

Where should the line be drawn? The FBI and other agencies might tell us they are controlling our online activities in a consistent and balanced way. But even if their machines are meant to intercept unlawful communications or actions, and even if new information through this machine leads to new insights or new investigations, the question raises as to whether or not it is ethical to our lives. Is computerized surveillance acceptable from an ethical standpoint, even if the objective is to benefit society as a whole?

More importantly, cyber forensics experts are developing a software program for digital fingerprinting. Digital fingerprinting enables a cyber forensics expert to identify a computer user based on profiling, that is, on the process of analyzing or recording a person's performance or behavior behind the computer screen (i.e., the number of keystrokes per minute, the writing style and type of language that he or she uses online, etc.). This software program is supposed to work at great efficiency. Now comes the big question: is it ethical that we are being profiled when we engage in communication behind the computer screen? In a similar fashion, the Internet enables cyber forensics

experts to participate in chat rooms and online forums in order to gather information about practically any subject they need. While the Internet provides easy access to diverse Internet communities, it presents a new ethical dilemma. Should university students or college professors working for cyber forensics labs be authorized to engage in "cyber spying" in the same way that law enforcement officials do? The answer to some of these questions is given in the analysis of the accounts that is provided later.

Chapter III

Methods

The third chapter of this dissertation covers, in detail, the methods used to conduct the study proper. As such, face-to-face qualitative interviewing was the method used in this study. The importance of qualitative methodology, the analysis of the accounts, and member checking are justified. This chapter also contains a description of the interview procedure (the interview process, the interview questions, and the necessity of using the technique of probing). Of equal relevance in this chapter is the section on the research questions and the section that explains how social network theory and game theory are used for the interpretation of the data, as well as how the two theories are intermingled when interpreting the data. What follows is a section about the participants, that is, who the participants were in this study, why they were selected, in which sites or locations they were interviewed, how they were recruited, and how they were protected. Finally, this chapter validates the reasons that explain why qualitative interviewing methods are best suited to answering my research questions. By the same token, I provide arguments as to how valid, reliable, and generalizable the results of qualitative interviewing can be.

Qualitative Interviewing

Face-to-face qualitative interviewing is a methodological approach that employs in-depth analysis of a particular setting (Lofland & Lofland, 1995). The analysis of qualitative data consists of breaking down a phenomenon to research its components. In doing so, the researcher is able to create a pattern for the whole by relating categories or themes to one another (Schwandt, 2001). This process implies that meaning is inferred

from the data collected. This section focuses on describing qualitative methodology, Kvale's six steps for analyzing the accounts, and the technique of member checking, which consists of reporting back preliminary findings to participants.

Methodology

The research employed qualitative methodology and data were collected via in-depth conversational (face-to-face) interviewing. One of the reasons the methodology was qualitative lies in the fact that a certain number of the participants were highly secure people who refused to fill out statistical surveys. According to them, one of the conditions to answer my questions was to see the researcher face to face. In fact, before I interviewed an FBI agent in the Southwest, I had to go through a scanner and a metal detector. I was not allowed to bring a tape-recorder either. I had to take notes for hours. The same process had to be repeated for a couple of other participants as well. The research employed qualitative methodology and data were collected via in-depth conversational (face-to-face) interviewing, following the procedures given by Kvale (1996). Kvale (1996) calls for seven stages in the interview process: *thematizing*, *designing*, *interviewing*, *transcribing*, *analyzing*, *verifying*, and *reporting*. As described later in detail, the interview protocol is based on questions about cyberterrorists, their networks, cybersecurity experts, their networks, as well as the games and strategies that are used in the context of cyberwar. The protocol is designed in such a way that the interviewees' responses pertain to the research questions. I asked the participants to recount from their personal experiences so that they could supplement the qualitative analysis and give me a sense of how to interpret the data later on.

For the purpose of this study, the answers to the interview questions are to be understood as accounts. An account is a way of describing events to make a story worth telling, with believability. It asks for an extended account of some past time (Riessman, 1993). In an account, participants recall events and memories at their own pace and in a manner that is comfortable to them. Accounts take place in a conversational manner (Wengraf, 2001). Participants also use accounts to justify or explain their own actions or actions of others (Rubin & Rubin, 1995). By the same token, an account given during an interview is the presentation not only of reasons but also of the participant him- or herself. The relevance of the participants' responses (that is, their accounts of past experience) was meticulously tested. Data collection and analysis procedures were well documented (most of the time with an audio-tape recorder). Some very important steps in the analysis of the accounts are the transcription and analysis/interpretation stages. Transcription involves translating from an oral language, with its own set of rules, to a written language, with another set of rules (Kvale, 1996).

Then, after everything was done, I analyzed and interpreted the data. This means that I evaluated the coherence, logic, and comprehensibility of the accounts of each interviewee in great depth. The goal was to make a plausible report to my readers. Note that the analysis of the accounts here is to be differentiated from Labov's and Walestky's (1967) model of narrative analysis. For these two scholars, analyzing a narrative is analyzing its clauses, its general structure (that is, its abstract, orientation, evaluation, resolution, and coda), and so on. Yet, almost forty years down the road, other scholars have come up with new ways of analyzing qualitative data. In this study, the analysis of the data followed Kvale's (1996) model very closely, as it is described below.

Analysis of the Accounts

Kvale (1996) suggests six steps of research, each with its own type of analytic reasoning:

1) The participants describe their lived world during the interview.
2) The participants themselves discover new relationships during the interview and see new meanings in what they experience. They start to see new meanings in their life worlds based on the descriptions of the interviewer.
3) During the interview, the researcher condenses and interprets the meaning of what the participants describes. Then, the researcher sends the meaning back, which enables the interviewee to revise or alter his or her statements.
4) The transcribed interview is interpreted by the researcher: to structure the material, the researcher clarifies the material to make it open to analysis, for instance by eliminating all the deviations and repetitions. Finally, in the analysis itself, the researcher elaborates the meanings of the interview by using one of five approaches to the analysis of meaning (i.e., meaning condensation, meaning categorization, structuring of the accounts, meaning interpretation, and generating meaning through *ad hoc* methods).
5) Re-interviewing is a possible fifth step. The researcher may give the interpretations back to the participants in order to receive comments on researcher interpretations of the accounts.
6) The researcher may extend the continuum of description and interpretation to involve action. A final analysis was made of the transcribed material. That final analysis

produced the significant themes found in the interview data. The result of the analytic processes is the interpretation of these data.

Member Checking

Analysis of the accounts is an omnipresent process throughout the research. While the qualitative researcher needs to know how to assess qualitative interview findings, it is also important that he or she understands that methods of improving research validity must be taken into account. A whole section is devoted to validity and reliability at the end of this chapter. Nevertheless, it is essential to discuss "member checking" as a preliminary step to understanding the importance of the validity and reliability of qualitative methods in this study. Based on the recommendations of Kuzel and Like (1991), "member checking" is necessary in qualitative interviewing methods. Member checking happens when the researcher restates, summarizes, or paraphrases the information received from an interviewee to check if what was heard or written down during the interview is correct. Member checking always comes after data collection and consists of reporting back preliminary findings to participants, asking for crucial critiques on the findings and incorporating commentaries into the findings.

Hence, member checking is a key element of credibility. Guba and Lincoln (1989) describe it as "testing hypotheses, data, preliminary categories, and interpretation with members of the stakeholding groups from whom the original constructions were collected. This is the single most crucial technique for establishing credibility" (p. 239). Member checking is constant checking throughout the investigation process ("do interview transcripts reflect what participants wanted to convey?"). The researcher has to "test" the data and conclusions with the participants. The purpose is, as Lincoln and Guba

(1985) argue, to make sure that the researcher "be able to purport that his or her reconstructions are recognizable to audience members as adequate representations of their own (and multiple) realities, it is essential that they be given the opportunity to react to them" (p. 314).

Research Questions

This is a study about a growing communication phenomenon: social networks. In doing so, I explored the subfields of organizational communication and new communication technology. The purpose of this study is to investigate how cyberterrorists create networks in order to engage in malicious activities on the Internet. Another purpose of this study is to understand how computer security labs (i.e., in universities) and various agencies (that is, law enforcement agencies such as police departments and the Federal Bureau of Investigation) create joint networks in their fight against cyberterrorists.

The ultimate goal is to show that, because of the postmodern nature of the Internet, the fight between networks of cyberterrorists and networks of computer security experts (and law enforcement officials) is a postmodern fight. The participants were computer security experts and law enforcement officials. Among law enforcement officials were local police officers, members of the FBI, the CIA, the National White Collar Crime Center, and other agencies. Computer (or cyber) forensics experts work in universities for the most part. The reason these participants were selected lies in the fact that they have adequate knowledge and expertise to enlighten me on the issue of cyberterrorism. Below were the following research questions to guide my research:

RQ1: What do computer security experts' and law enforcement officials'

accounts reveal about networks of cyberterrorists?

RQ2: What do computer security experts' and law enforcement officials' accounts reveal about their own networks?

RQ3: How can the conflict and interaction between cyberterrorists and computer security experts (and law enforcement officials) be explained through the use of both social network theory and game theory?

RQ4: What are the themes that emerged across the participants' accounts?

In order to answer **RQ1** and **RQ2**, I analyzed the accounts – based on social network theory – provided by the participants through their answers to all the interview questions (as well as the probing questions). In order to answer **RQ3**, I interpreted the data from both the social network theory and game theory perspectives. This is thoroughly explained in the next section. Finally, in order to answer **RQ4**, I looked for common themes that emerged across the participants' accounts.

Theoretical Approaches to the Interpretation of the Data

In order to answer **RQ3**, both theories were used; the arrangement of this interpretation was structured in three different parts. Each was independent from one another. The first part was exclusively a social network theory approach; the second part was exclusively a game theory approach; and the third part was an intersection of the two approaches.

The Social Network Theory Approach

The goal of using social network theory in this study is to explain the behavior and actions of both cyberterrorists and computer security experts (as well as law enforcement officials) in the context of the networks that they create. On the one hand, in

order to understand how cyberterrorists create networks to engage in malicious activities on the Internet, an etic approach was used. An etic account is a description of a behavior or actions in terms familiar to the observer. In other words, it is the "outsider" view (Pike, 1967). Recall that the participants interviewed were computer security experts and law enforcement officials. I asked them to tell me about their experiences and all that they knew about cyberterrorists and their networks. The participants here were observers (or outsiders) and not native informants.

On the other hand, in order to understand how computer security experts and law enforcement officials create networks to combat networks of cyberterrorists, or at least stop or resist them, an emic approach was used. The information they provided was an account of their behavior and actions – the participants themselves – in terms that were meaningful (consciously or unconsciously) to them. Here, it was not the "outsider" view, but the "insider" view, since the analysis of the data reflected the viewpoint of the native informants.

The Game Theory Approach

I did not use game theory as a tool to design new strategies for cyber forensics labs and law enforcement agencies to combat social networks of cyberterrorists. Rather, I used game theory to analyze the data provided by the participants in order to understand the existing strategies used by both cyberterrorists and computer security experts (and law enforcement officials). The main reason game theory was used lies in the fact that existing strategies can be modeled as games. When a game is discovered, a description fulfilling the properties of game theory can be implemented. The conclusions drawn from game theory were presented without computational data and mathematical formulas. As

Lye and Wing (2005) point out, solutions for game models are hard to compute. Hence, based on the main tenets and rules of game theory, I interpreted the data conceptually.

Based on the literature review, since computer security experts and law enforcement officials are involved in game strategies with cyberterrorists (no matter what the outcome or end-result is), they provided an "insider" view, so the approach was emic. By examining the data from my interviews, my goal was to determine what types of outcomes or end-states the games between the cyberterrorist and the computer security expert tend to result in. The questions (and probing questions) to be answered were similar to the following: What type of game is going on here? Does the outcome tend to be a zero-sum game? Is it usually a positive-sum game? Can it be a negative-sum game? Or even a Nash equilibrium? In a non-zero game, for instance, it never makes sense to communicate in an honest way; therefore, it would not be surprising that players use the Internet to increase such complexity.

With respect to a positive-sum game, the trend might be that both the cyberterrorist and his or her opponent eventually reach positive outcomes. Given this, instead of creating a dichotomous divide between the attacker and the defender, why not consider the extent to which the two are intertwined. As such, it was of interest to see whether or not those who defend systems and those who attack them fall into the gray areas in between. Or, think of the following question: "Do 'good' and 'evil' blur into gray?" Finally, a Nash equilibrium gives the computer security agent a good idea about the cyberterrorist's strategy and "a plan for what to do in each state in the event of an attack" (Lye & Wing, 2005, p. 9). Yet, not enough studies have been conducted to reach such a conclusion.

Intersection of Social Network Theory and Game Theory

The intersection of social network theory and game theory is very useful in this study. How the two theories can be intermingled has already been fully explained in the literature review, so it does not need to be explained again. The advantage of such an approach to interpreting data is that it allows me to perform a more accurate analysis.

Interview Procedure

This section describes the procedure for interviewing participants, based on Kvale's (1996) seven stages of interview investigation, outlines the interview protocol, and mentions the importance of probing.

Interview Process

Kvale's (1996) seven stages of interview investigation were methodically and fastidiously followed. The research goal was to collect personal accounts from participants involved, on a daily basis, in the detection and combat of cyberterrorist networks and in the networking with agencies such as law enforcement agencies and cyber forensics labs. I guided a close and private conversation with each of the interviewees. According to Kvale (1996), the interview is a unique form of conversation based on everyday life and, nonetheless, it is a professional conversation which has a structure and a rationale. The rationale is that it transcends the spontaneous exchange of views as in mundane conversation, and becomes a meticulous questioning and listening approach with the purpose of obtaining thorough knowledge about a certain issue. Another rationale is to obtain descriptions of the lived world of the participants regarding the interpretation of the meaning of the described phenomena.

The qualitative interview is a conversation, but not between "equal" partners; rather, it is asymmetrical because the researcher determines and controls the situation. For instance, the topic of research is introduced by the interviewer, who critically analyzes and follows the account of the participants and directs the discussion toward the experience to be understood. In order to conduct in-depth interviews, the researcher has to live within the interview experience, both participating in and directing the conversation at the same time. The outcome of the interviews depends on the researcher's knowledge, sensitivity, and empathy (as research tool). Reflexivity definitely plays a part at every stage of the investigation. Because the researcher is the research tool, everything that happens in the research reflects the researcher's thinking. Reflexivity implies that the researcher is mindful of all the other stages at the same time; that one pays continual, extraordinary attention. Being the researcher is a saturated role that goes from the most general perspective of the entire project to the smallest focus on the moment of the interview, all permeated by the researcher's own experience of the topic that is under examination.

As a researcher, I was very attentive to the accounts told by the participants. A reciprocal level of interpersonal relationship was needed. The more attentive and comfortable I was, the more relaxed the participants became. Both the participants and I were allowed to volunteer information, bearing in mind that we both shared and shaped the space together. In addition to this, observation is important. Observation is a key skill while interviewing. For this reason, the researcher must be a good listener, encouraging, showing interest, and expressing concern. Nonverbal is the first line of contexting the verbal. Nonverbal messages are expected to appear in the conversation (i.e., emotional

cues such as a tense voice, giggling, and nervous laughter). Therefore, I needed to have a good understanding of the participant's world going into the interview so that I could decipher the nonverbal aspects in anticipation of the transcription process.

The transcription process involves translating from an oral language, with its own set of rules, to a written language, with another set of rules (Kvale, 1996). The average length of each interview was about one hour and eight minutes. After the interviews were transcribed, I evaluated the coherence, logic, and comprehensibility of the accounts of each participant in great depth. The interview sessions began in December 2005 and ended at the end of January 2006. Creating the transcription of each interview took, on average, between four and seven hours, and served as part of the process of saturated listening.

Interview Questions

While I took notes when conducting interviews with a few highly secure people who refused to be tape-recorded, most of the interviews were audio-taped with a small recorder that was placed between the participant and me. In doing so, I was better able to concentrate on the topic and the dynamics of the interview. During these face-to-face interviews, participants were asked to answer a series of open questions. The whole interview process lasted approximately one hour and eight minutes per participant and took place in a private room (i.e., a room in a library, a law enforcement office, etc.). Each participant individually sat with me and gave me their account. I met with each participant only once. Many interview questions pertain to social network theory – particularly the first series of questions – and game theory – the last couple of questions. The reason the first series of questions pertain to social network theory lies in the fact that

it is important to first understand what networks of cyberterrorists and networks of their opponents are before having a grasp of how the actors play games in those networks. The twenty questions asked during the interview followed the order that is presented below (see Appendix B for interview protocol). The first series of questions pertain to **RQ1**. The next series of questions are relevant to **RQ2**. The last series of questions concern **RQ3**. No questions were asked to elicit data for **RQ4**. The data from which the themes (for **RQ4**) emerged come from many interviews conducted with the participants. No particular question was favored or asked in order to solicit these themes. All in all, it is the product of all the questions and answers to these questions.

In order to answer **RQ1** (What do computer security experts' and law enforcement officials' accounts reveal about networks of cyberterrorists?), I, the researcher, thought it was wise to center the first two questions on the very issue of this study: cyberterrorism. As such, the first two questions of the interview protocol are "What is cyberterrorism?" and "What are the motivations to engage in cyberterrorism?" Having an understanding of what cyberterrorism is and why cyberterrorists engage in cyber attacks and create those networks of terror is a necessary foundation in this qualitative study. The next questions derive directly from social network theory. Based on the scholarly literature, we know what postmodern terrorist networks look like, but I thought it would be interesting to know the participants' perspectives on those cyberterrorist networks. As such, the next two questions are "What does a network of cyberterrorists look like?" and "What do cyberterrorists do in those networks of terror?" These questions are broad but useful in this study. The next two questions are more technical and reflect the mechanics of social networks of terror. As we have seen, a social network is an interconnected system of

nodes and the relationships between these nodes. The highly connected nodes are called "hubs." These hubs have a high degree of centrality and removing these hubs can lead to the destruction of the network. Therefore, as it is important to know these aspects of cyberterrorist networks, the next two questions are the following: "Describe the role of nodes and hubs [minor and important actors] in the networks of cyberterrorists" and "Describe the degree of centrality in cyberterrorist networks." The seventh question of this interview protocol pertains to the culture of cyberterrorist networks. Every group, every community, and, therefore, every network has a culture, whether it is offline or online. The researcher thought it was interesting to know about the way of life and cultural practices of cyberterrorists. As such, the question is, "Describe the culture or way of life of cyberterrorist networks."

The subsequent series of questions pertain to the social networks of law enforcement agents and cyber forensics experts (**RQ2**: What do computer security experts' and law enforcement officials' accounts reveal about their own networks?). Recall what was said in a previous section: it takes networks to fight networks. These words, stated by Arquilla and Rondfeldt (2001), imply that top-down hierarchies are not effective techniques to use against social networks of cyberterrorists. As such, it is interesting to know what networking designs and strategies are used to fight, let alone understand, cyberterrorism and social networks of terror. Therefore, two fundamental questions are, "What types of networks do you use to combat cyberterrorism?" "What do you do in those networks?" Networking against cyberterrorists is a new strategy. As the point was made in the literature review, law enforcement agents have been engaged in this type of practice for just a few years (McGinn, Raymond, & Joseph, 2002). Yet, it

would be important to know whether or not cooperation among agencies is fruitful and whether or not there are downsides to networking with others in the context of cyberwar. As such, the next two questions are, "Is it necessary to create networks against networks? Explain" and "Describe the downsides to networking with other agencies." It is also important to know whether or not those networks are formal or informal. Therefore, the question is, "Are those networks formal or informal? Explain." By extension, a social network, whether it is a clique, a group of friends, a cyberterrorist network, or a network of law enforcement agents, always has nodes, hubs, and degrees of centrality in order to function. So, the next two questions are similar to the questions asked about cyberterrorist networks for **RQ1**: "Describe the role of nodes and hubs [minor and important actors] in your networks" and "Describe the degree of centrality in your networks."

In order to analyze **RQ3** (How can the conflict and interaction between cyberterrorists and computer security experts [and law enforcement officials] be explained through the use of social network theory and game theory?), a couple of questions – that is, the last series of questions in the interview protocol – were asked to look at how networks of cyber security experts (and law enforcement officials) operate against and *vis-à-vis* networks of cyberterrorists, that is, how the two sides conflict and interact with each other, based slightly on social network theory and mostly on game theory. The reason game theory is very much emphasized here lies in the fact that game theory is well applied in direct interactional and conflicting situations (Fent, Feichtinger, & Tragler, 2002), as it is the case in this study. As such, a good question was, "Describe a direct interaction or conflict between cyberterrorist networks and cyber forensics experts'

(and law enforcement agents') networks?" Because it is important to know how to cripple another network, based on social network theory and game theory, the following question was asked: "How can a network knock down another network?"

We have seen that postmodern cyberwar is a type of warfare that is based on strategies, just like a chess game. The rules are always evolving. The conflict between cyberterrorists and their opponents is an evolutionary game because new methods are constantly invented. The goal of the cyberterrorists is to create tactics and weapons that continually change in an effort to defeat their opponents' networks and systems. Likewise, it is essential for law enforcement agents to find strategies to counter cyberterrorist tactics. Therefore, the last five questions of this interview protocol reflect all this. They are the following: "What game or strategy do cyberterrorists use?" "What game or strategy do cyber security experts and law enforcement officials use?" "Could you give me an example of a collaborative game strategy between the two sides?" "Could you give me an example of a non-collaborative game strategy between the two sides?" and "Do cyberterrorists make the rules of the game or do they go along?"

Probing

The questions in this protocol are important. Yet, it is sometimes the case that participants elicit accounts or situations that call for other questions that are not in the protocol. The first segment of an in-depth interview is spent by both the researcher and participant getting to know each other. The general experiential topic is introduced in the first few minutes, beginning with the first of these broad questions above and then focusing upon the subject progressively. For this reason, the researcher added probes to the questions as the conversation is progressing. Probing questions are used to guide the

direction of the logic or path of the interview. A probe investigates a particular content area that the researcher wants to know more about. Probes were based upon previous research, my own intuitions, and findings from prior interviews. For instance, for the second question, "What are the motivations to engage in cyberterrorism?", as opponents may have different end goals from us, I added a probe and asked the participant what the rewards or desired outcomes are for a cyberterrorist's action. The use of game theory here was important when it came to the interpretation of the data.

The goal of including this section on probing is to show that the interview was not always structured as the interview protocol looks like. For Lofland and Lofland (1995), an unstructured interview seeks "to discover the informant's experience of a particular topic or situation" (p. 18). An unstructured interview is open-ended and informal, which allows for research flexibility and responsiveness to emerging issues. More importantly, this design also enables both the researcher and the participant to control the pace and flow of conversation, including the introduction of new topics (Mishler, 1986).

Participants

This section describes, in detail, who the participants were in this study, why they were selected, in which sites or locations they were interviewed, how they were recruited, and how they were protected.

Who Were the Participants?

I, the qualitative researcher, managed to find twenty-seven (n=27) participants who, from an examination of the research literature, are representative of the research questions. Twenty-seven participants might seem to be an insufficient number for such a long study, but the participants were all primary sources. Participants in this field of study

are uncommon and difficult to convince to participate in a major study. Many of them said that they had never been interviewed before. As such, the data in this study are primary. The participants were experts in computer and information security from ages 18 to 64 (to avoid exclusion criteria). Selected participants were not only computer security agents, cyber forensics experts, IT analysts, and members of information technology (IT) labs; they were also people working for law enforcement agencies such as local police departments, the Federal Bureau of Investigation, and district attorneys' offices.

Why Were these Participants Selected in this Study?

All the participants mentioned above possess the knowledge and expertise to enlighten me, through their direct experiences with computer security and cyberterrorist incidents, on all the various topics that pertain to my research questions. Computer experts have created cyber forensics teams that network with law enforcement agencies in their fight against cyberterrorists. It is important to know that, in this day and age, law enforcement agents (i.e., working for police departments, etc.) work alongside computer security experts who are trained to identify cyberterrorists and arrest them. The Federal Bureau of Investigation has cybersecurity teams as well; they work collaboratively with university cyber forensics labs and other agencies. More importantly, all these participants understand how networks of cyberterrorists work. For all these reasons, they are ideal participants in my study.

Where Were the Participants Interviewed?

The location where the participants were interviewed was mostly in the Midwest and in the Southwest. The major sites of participant recruitment were (1) the information

technology lab at the University of Oklahoma, (2) the information technology lab at the University of North Texas, (3) the information technology lab at Purdue University, (4) the information technology lab at the University of Central Florida, and (5) the information technology lab at the University of Tulsa. The reason I selected these universities for my research lies in the fact that their information technology labs have computer experts who have created cyber forensics teams that network with law enforcement agencies in their fight against cyberterrorists. Other major sites for participant interviewing were the Norman Police Department, the Denton Police Department (Texas), the Lafayette Police Department (Indiana), the Orlando Police Department (Florida), and branches of the Federal Bureau of Investigation. So, I used a convenience sample. One of the underlying reasons for doing this lies in the fact that it just makes it easier – due to temporal and geographical constraints – for a student who attends a Southwestern university and who has negotiated access to these sites.

How Were these Participants Recruited?

To recruit participants who work in university computer labs, I asked the head of a computer lab to give me permission to have a list of names of computer security experts who would be willing to participate in my study. If the head of the computer lab agreed to give me that list, I called (by phone) or I contacted, by email, those experts in the field of computer and network security, and I explained to them the purpose of my study. If they agreed to participate in my study, and before these participants answered my interview questions, I showed them the informed consent form (see Appendix A, at the end of this dissertation).

To recruit participants working for a police department, I asked the head or supervisor of police officers (who are computer security experts) to give me permission to have a list of names of people who would be willing to participate in my study. When I was allowed to have a list of police officers willing to participate in my study, I called them (by phone) or I contacted them, by email, and I explained to them the purpose of my study. If they agreed to participate, and before they answered my interview questions, I showed them the same informed consent form.

To recruit participants working for the Federal Bureau of Investigation and other federal agencies, I used chaining. Chaining is a process whereby one person tries to get another person *entrée* into a group or community that is usually not open to the public. In the world of the FBI and other federal agencies, there is a two-degree separation. I could get interviews with federal agents only through chaining, that is, through an informant who was trusted by FBI agents. The informant was a computer security expert who knew potential participants working for the FBI. When I was given a list of highly secure participants such as FBI agents, I called them (by phone) or I contacted them by email, and I explained to them the purpose of my study. If they agreed to participate in my study, and before these participants answered my interview questions, I showed them the same informed consent form.

How Were these Participants Protected?

For the protection of the participants, and for the ethical issues inherent to every research project involving human participants, I assured them that their identities remained anonymous and that they would have access to the written texts of my research – also useful for member checking – before I would incorporate excerpts of these texts in

my dissertation. To increase the protection of the participants, I also assured them that the tapes would be destroyed when the study is complete.

Why Are Qualitative Interviewing Methods Best Suited to Answering My Research Questions?

Studying the context in which networks of cyberterrorists are examined and Internet and computer systems are meant to be better secured requires an appropriate research methodology. Before explaining why I contend that qualitative interviewing methods are better than quantitative methods to investigate my research questions, it is worth quoting Denzin and Lincoln (1998) to provide a sound and powerful definition for both methods:

> The word qualitative implies an emphasis on the processes and meanings that are not rigorously examined, or measured (if measured at all), in terms of quantity, amount, intensity, or frequency. Qualitative researchers stress the socially constructed nature of reality, the intimate relationship between the researcher and what is studied, and the situational constraints that shape inquiry. Such researchers emphasize the value-laden nature of inquiry. They seek answers to questions that stress how social experience is created and given meaning. In contrast, quantitative studies emphasize the measurement and analysis of causal relationships between variables, not processes. Inquiry is purported to be within a value-free framework (p. 8).

There are many reasons why qualitative interviewing methods are better than quantitative methods for answering my research questions. First of all, qualitative research enables the interviewer to engage in "intensive self-reflection and introspection"

(Denzin & Lincoln, 1998, p. 4). As a researcher, I can get closer to the respondent's perspective thanks to detailed interviewing (Brenner, Brown, & Canter, 1985). With quantitative methods, however, I would hardly ever be able to gain the respondent's perspective because I would rely on more distant, inferential empirical materials (Denzin & Lincoln, 1998). Let me elaborate on that first point. In the context of cyberterrorism, observing sites (i.e., cyber forensics labs, law enforcement agencies, etc.) and interviewing key people in each organization or agency would establish a trusting relationship between the researcher and the participants, which, in turn, can be important in providing insights into the everyday practices of the interviewees. This would also enable these interviewees to reflect in depth upon their lived experiences through accounts (Brenner, Brown, & Canter, 1985).

Second, as a qualitative researcher, I want to write in the first-person account and not engage myself in third-person prose, because with qualitative interviewing, I can incorporate factors of emotionality, reflective interpretation, and mentality into my work (Rubin & Rubin, 1995). Quantitative methods do not allow that. Qualitative interviewing, on the other hand, gives a great deal of attention to both the inner and outer states of human activity (Hamilton, 1998). Interviewing members of organizations or agencies with which I am not familiar make me more aware of other cultural selves. When the interviewer becomes aware of the "cultural self," there is an extra set of resources upon which to draw in interpreting results (Olesen, 2000).

Third, other "truths" about cyberterrorist networks or Internet and computer security may be valid outside of the world of quantitative tools that is analyzed and interpreted to reach different conclusions. Claims to truth are always discursively situated

in relation to power. Truth implicates regulatory rules that must be met for some statements to be more meaningful than others (Kincheloe & McLaren, 2000). For instance, it is sometimes the case that the participants have a specific issue they desire to share with the leaders of their organizations or agencies, but they do not take the step and bring it to them because of the concern of "power" just mentioned. Therefore, the participants might see the qualitative interviewer as their "confidant" in that they can communicate that issue in depth and share it with the interviewer face to face. The positive outcome is that the interviewer might extract more truthful statements from the participants. It is more difficult with statistics or surveys to detect this sort of information because the quantitative researcher might not be aware of the problems that the participants did not raise to the leaders of the organization. Therefore, it is an in-depth and experienced qualitative interviewer who can be more aware of the irregularly mentioned problems and, consequently, can be more aware of how cyberterrorists operate and how organizations or agencies can improve their security systems. In a similar fashion, because the interviewer is the primary instrument of research, his or her conceptual models, beliefs, and prejudices would be able to filter through the interpretations of the claims to truth mentioned above (Kincheloe & McLaren, 2000).

Fourth, there is a gathering momentum for qualitative interviewing in information systems (Lee, 2001; Trauth, 2001). Qualitative interviewing in the study of information technology and cyberterrorism has the ability to transcend the rational domain. Whereas quantitative methods such as statistics, surveys, and questionnaires belong to the rational research domain, qualitative interviewing, as Lincoln and Guba (2000) put it, has at its fingertips many additional ways of collecting data – creativity, movement, direct

knowing, intuition, flow, and so on. Quantitative methods do not allow me to be a *bricoleur*, a "Jack of all trades or a kind of professional do-it-yourself person" (Lévi-Strauss, 1966, p. 3) because qualitative interviewing is multimethod in focus (Brewer & Hunter, 1989). This boils down to saying that, if new techniques have to be invented or pieced together (to help me pursue my research), qualitative research enables me to be more than a "limited" researcher (Denzin & Lincoln, 1998). This is what is meant by *bricoleur*.

Fifth, as opposed to quantitative research, qualitative interviewing is more constructed. While quantitative researchers "leave the field with mountains of empirical materials and then easily write up his or her findings" (Denzin & Lincoln, 1998, p. 29), the qualitative interviewer begins by creating notes. The interview itself, after being recorded, is then re-created as a file that contains the researcher's early attempts to understand and interpret what he or she has learned (Brenner, Brown, & Canter, 1985). Finally, the researcher produces the end-result (that is, the text) that comes to the reader. As such, the reader learns from the carefully reflexive point of view and experience/interpretation of the researcher (Silverman, 1993).

Sixth, because the qualitative interviewer is the chief instrument for the research process, he or she brings to the research process an individual mindset and biases (Janesick, 2000). Yet, I consider it as strength because it adds to the richness of knowledge about complex situations. The study of cyberterrorism and information systems lends itself to analyzing complex situations. One complex task in qualitative interviewing is seeking meaning in context (Bogdan & Biklen, 1992; Mishler, 1986). Not only must the subject matter be set in its social and historical context so that the reader

can understand how the existing situation emerged (Klein & Myers, 1999) – for instance, I would have to take an in-depth look at past network problems (i.e., Brynjolfsson & Mendelson, 1993) – but, also, qualitative interviewing must aim at "producing an understanding of the context of the information system and the process whereby the information system influences and is influenced by its context" (Walsham, 1993, p. 4).

Seventh, tools such as surveys and statistics used in quantitative research are more artifacts of the researcher's program and less the results of analysis. Quantitative researchers work from a schedule of already-made questions that allow a respondent to check a box on a page that is later transformed into quantified analysis of a large number of responses. However, a protocol for interviews is stronger because it guarantees that interviews collect comparable data across collection events. More importantly, the protocol can be used to probe knowledge and give a chance to inform each interviewee at definite times. A quantitative tool such as a questionnaire lacks the human touch that interviewees would need in that situation.

Eighth, it might be the case that the interviewee is not very familiar with the way cyberterrorist networks operate. Nevertheless, this lack of complete knowledge can be overcome if the interview protocol allows for an initial general discussion in order to identify the overall interviewee's knowledge of the subject. By the same token, some time could be even spent creating an informational foundation before the interview continues. As a matter of fact, qualitative interviewing may not specify questions *per se*. The interviewer may ask of the respondent broad, experiential queries as conversational grounds for the respondent to volunteer his or her accounts of lived experience about the information security system in relation to the organization or experience being the focus

of research. With a quantitative tool like a questionnaire, it would be more difficult to follow the procedure mentioned above.

Questions of Reliability and Validity

One question that one might all ask is the following: "Tell me how your 'measures' are reliable and valid, and tell me how you can generalize with this stuff." We saw earlier that the benefit of member checking is that it adds accuracy and richness to a final report and that including member checking into the findings (i.e., gaining feedback on responses from the interviewees) is an important method of increasing credibility. In order to better answer the question that I brought up in this paragraph, I considered whatever discussions of reliability and validity I have been exposed to, including texts in quantitative and qualitative methods classes that I took, in theory courses that I attended, as well as philosophical dictionaries and encyclopedias, and other sources that I read. For several decades, the concepts of validity, reliability, and generalizability in social research have gained the status of a scientific holy trinity (Kvale, 1995). I believe that qualitative interview findings are as valid and reliable as quantitative data for several reasons. The notion of generalizability will be discussed later.

Validity and Reliability of Qualitative Interview Findings

As Clifford Geertz (1973) once remarked, the validity of a statistical table differs from the validity of thick description in an interviewer's report. Therefore, one should not get caught in an "either or" trap. Quantitative research and qualitative research are two different methods for two different purposes. While quantitative research seeks to "explain," or *erklaren* (Maddox, 1985), qualitative research attempts to "understand," or *verstehen* (Trigg, 1993). The goal of *erklaren* is to explain (maybe even predict or

control) how carefully specified groups of people will likely respond or react to specific stimuli under carefully controlled conditions. The goal of *verstehen* is to make people aware of how humans act on meaning. The goal of the researcher is to make readers understand how meaning is created and how it becomes "background expectancies" or "shared understanding" among human beings with shared experience.

Before explaining the main factors that justify qualitative interviewing as a valid and reliable method, let us begin by defining the concepts of validity and reliability. Validity questions whether or not the study investigates what was intended. It is paramount to "the extent to which our observations indeed reflect the phenomena or variables of interest to us" (Pervin, 1984, p. 48). Validity is "a process for developing sounder interpretations of observations (Cronbach, 1971, p. 433). In fact, a valid argument is powerful, convincing, well grounded, and justifiable. A valid inference is precisely derived from its premises (Kvale, 1995). Validity is also the researcher's mask of authority (Lather, 1993). Without it, there is no truth (Scheurich, 1992) because actions that lack validity "seem unable to occur in reality" (Todorov, 1977, p. 82). Reliability, on the other hand, is a concept that is more encountered when studying quantitative methods. It refers to the consistency of findings or results (Kirk & Miller, 1986). Qualitative researchers often refer to reliability as consistency. They see reliability as "dependability" and stress the importance of using multiple sources of information. Furthermore, reliability is affected by the quality of the questions and the fit to the group being studied.

The first factor confirming the validity and reliability of qualitative interviewing is that, although quantitative and qualitative research methods differ sharply in working,

both research designs look for valid and reliable results. With respect to qualitative interviewing, validity is socially constructed (Kvale, 1995), both by the field researcher and the participants, who collaborate in the same setting and situation. The field researcher "wants to provide an account that communicates with the reader the truth about the setting and situation" (Altheide & Johnson, 1994, p. 496). As a qualitative interviewer, I would not attempt to seek proof or some type of statistical correlation; I would strive for thick description: is the interpretation emerging from the participants' accounts convincing to the reader – does it ring true? (Altheide & Johnson, 1994). Validity of qualitative data is what is hoped for because the researcher wants data to be representative of a real and complete picture of phenomena under investigation. The ultimate question that the qualitative researcher asks is the following: "Are the representations in the text consistent with the real?" (Lincoln & Denzin, 1998, p. 416).

Another important factor is that, in my research, validity would be my loyalty and commitment to representing the people – i.e., computer security experts, university cyber forensics employees, IT analysts, law enforcement officials, and so on – being studied as fully as possible. Within such an all-embracing conception of validity, qualitative interviewing may, in principle, lead to valid scientific knowledge (Kvale, 1995) because qualitative interviewing means more than merely asking questions; the validity of in-depth interview data depends considerably on the methodological skill, understanding, and wholeness of the researcher. With regard to reliability, in order to ensure reliability in my type of research, examination of truthfulness and trustworthiness is also crucial. Seale (1999), by establishing good quality work through reliability in qualitative studies, asserts

that the trustworthiness of a qualitative research report lies at the heart of issues traditionally discussed as reliability.

The third factor is that the text – that is, the end-product written by the qualitative interviewer – is considered valid if it is sufficiently grounded, and "comprehensive in scope, credible in terms of member checks, logical, and truthful in terms of its reflection of the phenomenon in question" (Lincoln & Denzin, 1998, p. 414). In other words, validity becomes contingent upon the quality of "craftsmanship" in the qualitative investigation, which includes constantly checking, questioning, and theoretically interpreting the findings. In this "craftsmanship" approach to validation, the focus shifts from examination at the end of the production line to quality control during all the stages of knowledge production (Kvale, 1995). This means that validity in qualitative interviewing is dependent on meticulous "checking." As opposed to validity in quantitative research, validity in in-depth interviewing is not synonym with "control" or "verification" of a final product. Rather, verification in my study is built into the research process with frequent checks of the credibility, plausibility, reasonableness, and trustworthiness of the findings (Kvale, 1995). This is why I want to outline, in detail, the tactics formulated by Miles and Huberman (1994) for testing and substantiating qualitative interview findings. The tactics involve looking for negative evidence (and not just looking around the site), checking for representativeness and for researcher effects, weighing the evidence, eliminating rival explanations, and checking the meaning of outliers (this would occur if the interviewees in the organization give unusual responses that are far outside most of the rest of the responses in the data set) (Miles & Huberman, 1994).

A fourth factor is that systematic and rigorous observation involves far more than just the researcher's presence and his or her looking around the site. The approach in my study is to analyze the many sources of potential biases that may emerge in the research sites. These potential biases may invalidate observations and interpretations. This is why engaging multiple methods such as observation, interviews, and recordings yields more valid and reliable construction of realities (Johnson, 1997). Also part of the multi-method strategy involves employing extreme cases, following up surprises, replicating a finding (Miles & Huberman, 1994), and getting feedback from IT analysts, cyber forensics experts, and other specialists.

Generalizability of Qualitative Interview Findings

In the same line of reasoning, the goal of qualitative interviewing is to generalize from close study. Generalizability means that findings can be generalized; it refers to the extent to which an account can be further applied to situations or populations not directly studied. Lincoln and Guba (1985) stress that generalizability allows a semblance of prediction and control over similar phenomena, yet one should keep in mind that "any generalization is a working hypothesis, not a conclusion" (Cronbach, 1975, p. 125). The qualitative researcher "generalizes" his or her findings, but not with an approach that seeks to reach the scope of a universal law. Instead, the richness of the thick description, the particular elements that were detailed, recorded, and verified, and the patterns of themes that these elements exhibit, enable the researcher to make all those "generalizations." "Generalizability" in qualitative interviewing means that the findings are trustworthy, dependable, and transferable (Oberle, 2002). The ultimate objective is

that the qualitative results from my research serve as the foundation for future studies that will benefit from my observations.

However, I am also fully aware of the fact that generalizing in qualitative interviewing is more difficult. While in most quantitative research, generalizing is a relatively straightforward task – indeed, when the statistician collects the same variable from his or her subjects in the sample, all that needs to be done is generalize to the sample as a whole and compute values such as the mean or median – the data in qualitative interviewing are more raw and hardly ever pre-categorized. Accordingly, I, as the researcher, needed to take the time to sort out and "classify" that raw information. This shows that in-depth qualitative interviewing must be a rigorous methodology where the researcher detects participants who have closely experienced the phenomenon in question, observes them, and interviews them for hours. Then, the researcher edits the interviews profoundly so that he or she pictures the participants' life experiences in a way that makes the account different from what any of these participants has told. In the meanwhile, the researcher still addresses the question of interest. As one can see, even generalizing across a set of different accounts can become a labor (a labor of love nonetheless).

In contrast with quantitative research, where the researcher's findings are generalized beyond the sample from which the data was drawn, a qualitative interviewer provides a thick description of the study to the readers. Part of the goal of producing a thick description is to persuade readers that the interpretation of the findings is plausible. As far as this investigation of cyberterrorist networks and information security is concerned, there are undoubtedly a certain number of law enforcement agencies and

cyber forensics labs that have vast expertise in the matter and that exist in many areas of the Midwest and the Southwest. They can be found anywhere. Although there are clear differences between each of these organizations or agencies, they also share many similarities such as the way some of their structures or operations work (i.e., they rely on computer and Internet networks and have computer security experts). Although these are not statistical generalizations, anyone familiar with these twenty-first century organizations and agencies can recognize these standard elements. So, the reader can easily identify with these organizations and agencies.

What this means is that the generalizations of the findings might somewhat differ from what the reader expects, but, if we were to "look at the whole picture," a thick description provides the readers with ample information to evaluate the suitability of applying the findings to other settings. This enables the readers to determine if the situation described in the rich text (that has been meticulously crafted) applies to the situation of the reader himself or herself. By the same token, the investigator can ascertain the typicality of the case, that is, describe how typical a participant is in relation to others in the same class so that readers can make comparisons with their own situations (Merriam, 1988) and estimate whether or not the work of the researcher is generalizable to them and consistent with their perceptual reality. In this way, generalizability is a process of interaction; it is a conversation between the researcher and the researched, and between the reader and the text (Atkinson, Heath, & Chenail, 1991).

Finally, generalizability in qualitative interviewing is highly possible because this type of research is based on the principle that social actors co-create emergent social worlds, in a particular time and place. For this reason, the concept of generalizability for

qualitative interviewing involves social processes (i.e., insiders-outsiders) that might be relevant in more than a single setting or interaction. As a qualitative researcher, using the term "generalizability" does not refer to the statistical relation of a sample to the greater population, but to common patterns in social interaction and social life. What is useful, in order to generalize the findings of my study on information security systems, is to diversify the investigation as much as possible in order to determine whether or not the findings vary from one location to the next. For example, I could have attempted to interview members of large IT corporations in the upper Midwest and members of private industries in the lower Midwest (most of which have computer security experts working for them). In other words, I might have conducted a cross-case analysis, that is, an analysis across multiple potential targets of cyberterrorist networks that builds an integrated framework (Merriam, 1988). This could have shifted attention to other organizations in the research sites in order to further explore and modify the initial findings. Eventually, this could have improved the "generalizability" aspect of my qualitative study.

Chapter IV

Analysis of Research Question 1

In this chapter, the findings from accounts elicited from twenty-seven participants (mostly cyber forensics experts and law enforcement officials, but also other important individuals working with them) about their fight with cyberterrorists and their experiences of collaborating with other agencies are analyzed in detail. This analysis examines each of the four research questions separately. In order to answer **RQ1** (What do computer security experts' and law enforcement officials' accounts reveal about networks of cyberterrorists?), the following questions were asked in each interview: (1) What is cyberterrorism?; (2) What are the motivations to engage in cyberterrorism?; (3) What does a network of cyberterrorists look like?; (4) What do cyberterrorists do in those networks of terror?; (5) Describe the role of nodes and hubs [minor and important actors] in the networks of cyberterrorists; (6) Describe the degree of centrality in cyberterrorist networks; (7) Describe the culture or way of life of cyberterrorist networks. These questions were mostly driven by social network theory and do not include probing questions that were asked during each interview because, for each participant, the interviews progressed differently. Let us begin by analyzing the participants' perspectives on what cyberterrorism is.

What Is Cyberterrorism? The Participants' Perspectives

Although the interview questions for **RQ1** were mostly driven by social network theory, it would be wise to center the first question on the main issue of this study: cyberterrorism. For this reason, I asked the participants what their perspectives were on cyberterrorism. In other words, "what is cyberterrorism?" The participants' accounts are

consistent with the assumptions made about cyberterrorism in the literature review. The first excerpt was selected from an interview conducted with a forensics examiner. His main tasks and responsibilities are to examine and investigate any kind of intrusion or suspected illegal activity on any kind of digital medium. The participant described one of the components of cyberterrorism. For him, cyberterrorism is,

> any kind of threat that can come through any digital medium, such as network package injection, injected across software programs loaded on. It's also any kind of threat that can take down an infrastructure or network such as a power plant infrastructure, an IT infrastructure, or a law enforcement infrastructure.

The statements made by this participant are clear-cut. Cyberterrorism is "any kind of threat" via a digital medium. The scholarly literature says that "digital" includes, but is not limited to, systems related to computers, computerized items, and/or automated systems (both in terms of hardware and software) (i.e., Casey, 2004). Part of this definition embraces some statements made in the description above ("network package injection, injected across software programs loaded on"). This view of cyberterrorism is general and does not include the motivations behind cyberterrorism. Nevertheless, cyberterrorist threats, says our participant, could cripple infrastructures or networks "such as a power plant infrastructure, an IT infrastructure, or a law enforcement infrastructure." The excerpt below, selected from a computer crime specialist in the Southwest, is similar to the previous excerpt:

> It's some type of violation either through the use of a computer or with a computer against a network. So, it involves a computer mechanism of some sort. It is intentional and has to be done through a computer network or a computer

system, which may be an individual workstation or a more complex grid of computer systems or an application on various levels of what that means.

Here, however, the emphasis is not on digital media, but on computers themselves ("It has to be done through a computer network or a computer system"). The participant's statements relate very much with accounts of cyberterrorism in the scholarly literature. For instance, for Dunnigan (2003), cyberterrorism is the use of electronic networks and computer technology as weapons. Likewise, for Stone (2001), cyberterrorists frequently attempt to break into computers to contaminate them – and others – with viruses (i.e., what our participant calls "violation"). In addition, in this excerpt, there is mention of intention (i.e., "it is intentional") behind the cyber attacks. This corresponds with the description of cyberterrorism made by other scholars such as Arquilla, Rondfeltd, and Zanini (1999) and Conway (2002). For them, cyberterrorism is the intentional use of threatening and disruptive actions against computers, networks, and the Internet in order to cause harm or further ideological, political, or similar objectives, or to intimidate any person in furtherance of such objectives. The following excerpt, taken from an interview conducted with a computer crime specialist with the National White Collar Crime Center, adds something important to the previous descriptions of cyberterrorism. For this participant, cyberterrorism is,

> any means by which an information system can be used to cause some sort of harm. This could be harm to the information system itself or some sort of physical infrastructure. For example, a lot of dams are controlled by computers. That could be subverted to bad uses, like opening up the floodgates and drowning half the town. Theoretically, cyberterrorists could do it, but that hasn't happened yet.

First, this description highlights the effect of cyberterrorism, that is, harm (i.e., "to cause some sort of harm"). The two previous excerpts did not focus on harm. Cyberterrorism, Dunnigan (2003) says, can cause harm, even devastating harm. Second, this participant emphasizes the fact that cyberterrorists have not been successful in conducting a massive-scale attack ("that hasn't happened yet"). Nevertheless, our participant adds that, "theoretically, cyberterrorists could do it." Although the participant did not use a term such as "massive-scale," the idea that cyberterrorism could be "opening up the floodgates and drowning half the town," is, in itself, a massive attack and, theoretically, it could be done. The next excerpt, taken from a forensics examiner in the Southwest, takes a different angle on cyberterrorism:

> You've heard of the Nigerian scams? Those are basically people that exploit money; they would claim to be some person that has a lot of money. American and British banks are some of the most targeted. Once they start following into the ploy with you, they threaten you and your family, they have people come and harass you. They are definitely cybercriminals, but not cyberterrorists. They only threaten people. They use email communication.

Here, the description of cyberterrorism is that if it is only a threat via computers or the Internet (i.e., "email communication"), it is not an act of cyberterrorism. Rather, it would be cybercrime (i.e., "They are definitely cybercriminals"). Besides, as opposed to what was said in the very first excerpt, a threat, in and of itself, cannot "take down an infrastructure or network such as a power plant infrastructure, an IT infrastructure, or a law enforcement infrastructure" (see first excerpt of this sub-section). Open sources on cybercrime correspond with the statements made by the participant on the matter. A

cybercriminal, in essence, is a criminal who uses computers and/or the Internet to communicate, raise money, recruit new members willing to break the law, and commit other crimes such as threats (McQuade, 2005). Archick (2003) goes further when she says that a cybercriminal offense includes money laundering, as well "fraud and forgery, child pornography, copyright infringements, and security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability" (p. 2). The next excerpt concentrates on the difference between hacking and cyberterrorism. Asking a participant working in a cyber forensics lab if there was a difference between a hacker and a cyberterrorist, the participant responded with the following statement:

> Yes, there is. A lot of hackers do it for the fun of it or for notoriety, or for personal gain, whereas cyberterrorists usually do it to disrupt or to cause trouble to actually try to strike terror and fear into the general populace or into a certain company. Another difference is that hackers like to brag about being hackers, but cyberterrorists do not see themselves as cyberterrorists. They like to rationalize their actions.

This difference between hacking and cyberterrorism helps us understand the intent of both types of disruption and, to some extent, the effects of cyberterrorism. Based on the participant's description, the hacker does it just "for the fun of it or for notoriety, or for personal gain." From this, it can be inferred that hackers like to delve into computers with no intention to harm computers. A cyberterrorist, on the other hand, is an intentionally malicious hacker. Indeed, cyberterrorists "usually do it to disrupt or to cause trouble to actually try to strike terror and fear into the general populace or into a certain

company." This is a throwback to the definition of Vegh (2002) mentioned at the beginning of this study. For him, hackers with malicious intent are cyberterrorists. In line with these contentions, as explained in the literature review, just like terrorism is primarily a process of communication between terrorists and target audiences (Tuman, 2003), an important goal of cyberterrorists is to send a powerful signal, whose meaning is intended to frighten and coerce. The participant expresses it clearly: "to actually try to strike terror and fear into the general populace or into a certain company." Cyberterrorism is a semiotic act; it is a message, a symbol, and a new media image. Our modern western world is wrapped up with images, signs, and symbols (Miller et al., in press). Given this, there is a powerful semiotic dimension to cyberterrorism. Without a doubt, it can involve sending images of fear.

The participant makes another difference: "hackers like to brag about being hackers, but cyberterrorists do not see themselves as cyberterrorists." From this, it follows that cyberterrorists have different views than law enforcement agents as to what constitutes a cyberterrorist. This is an important matter because cyberterrorists, as they like to "rationalize their actions" (according to our participant), might not realize that the fact that they are damaging computer systems makes them cyberterrorists. In the cyberterrorists' community, do they even know that they are cyberterrorists if they conduct cyber attacks or cripple entire networks? The fact that they like to rationalize their actions demonstrates that part of their identity is to say "no" to the Internet rules enforced by law enforcement and the powers that be. Asking the same participant whether or not cyberterrorism is accidental, the participant responded that it was not:

> No, it's not accidental. You can't accidentally do it. I've seen people accidentally hack, but with cyberterrorism, you have to specifically have a target picked out and a method picked out that's going to be very specific for your purpose.

Cyberterrorism, says our participant, is "not accidental" because "you can't accidentally do it." From this, we can deduce that cyberterrorism is always intentional. A computer-whiz college student may break into a computer system for various reasons, but, as the point was made in the previous excerpt, these reasons are not necessary intentional. Hackers might just do it "for the fun of it or for notoriety, or for personal gain." They have no intention to cause harm. By extension, the participant's belief that hacking can be accidental ("I've seen people accidentally hack") refers precisely to the "I Love You" virus incident mentioned in the literature review. The "I Love You" virus was a hacking episode that resulted in more than $10 billion in damage around the world (*New York Times*, June 13, 2000). The twist is that the Filipino author of the virus was never prosecuted because in 2000, there were no cyber laws in the Philippines. Although the "I Love You" virus infected and harmed computer networks including those of the Pentagon, governmental establishments, parliaments, and corporations worldwide (Wehrfritz & Vitisca, 2000), nobody knows if the hacker sent that virus intentionally. It might have been an accident. For all these reasons, from a law enforcement perspective, the "I Love You" virus was an act of hacking, not cyberterrorism (*New York Times*, June 13, 2000) because, as the participant tells us, cyberterrorism has "to be very specific for your purpose." The next excerpt was, again, selected from the interview conducted with that same participant:

> They all come together with a common goal of wreaking havoc. Their main initiative is to find people that are like-minded because hacking, while it is traditionally seen as the one kid sitting down at 2 a.m. in front of his mom's computer, is not always like that. It can be highly organized in groups and individuals who are working together on a common goal, like the botnets out of the Netherlands. That was a group of people that came together for a group cause.

A botnet is a compilation of compromised machines that run malicious programs (i.e., worms, Trojan horses, or backdoors) under a common command and control infrastructure (Baker, 2005). The Dutch botnets were operated by a cyberterrorist group from the Netherlands of which the main goal was to cripple computer systems of various businesses (Knight, 2005). This demonstrates that this is a group of people who come together "for a group cause" and that it is composed of "individuals who are working together on a common goal." And the common goal of cyberterrorists is to wreak havoc ("They all come together with a common goal of wreaking havoc"). For this reason, "their main initiative is to find people that are like-minded." The participant also makes a reference to hacking as a traditional form of computer intrusion that has no intent to harm ("it is traditionally seen as the one kid sitting down at 2 a.m. in front of his mum's computer"). Nevertheless, it "is not always like that." Hacking can also be malicious hacking. Malicious hacking – if it is intentionally malicious – is cyberterrorism. The last excerpt of this sub-section, taken from a former CIA agent who specialized in computer crime, is interesting because it gives an overall perception of cyberterrorism as a threat to our society:

> I think cyberterrorism is a threat to our society. Some people say that cyberterrorism has never happened and that it never will, but that strikes me as naïve. Think about the computer intrusions that have been done out of the former Soviet block against banks. People stole millions. If you can do those intrusions for an economic gain, why couldn't cyberterrorists do that for a political gain? I agree that cyberterrorism on a massive-scale hasn't happened, but that doesn't mean we shouldn't protect against it.

Cyberterrorism, says this former CIA agent, is a threat to our society. Based on his statements, there have been cases of computer invasions for financial purposes. The intruders were from the ex-Soviet Union. Computer intrusions, he continues, are a threat to our society because if we can have intrusions for an economic gain, "why couldn't cyberterrorists do that for a political gain?" This excerpt is similar to the third excerpt in that both participants emphasize the very notion that cyberterrorists have the capabilities to cause serious problems. Yet, while in the third excerpt it was said that cyberterrorists could "theoretically" open up the floodgates and drown half the town, in this excerpt a different outlook of the potential of cyberterrorism is expressed in the following terms ("I agree that cyberterrorism on a massive-scale hasn't happened, but that doesn't mean we shouldn't protect against it"). Here, the participant recommends that we should protect ourselves against cyberterrorism, implying that it is dangerous.

All in all, these eight excerpts articulate the dangers of cyberterrorism and the similarities and differences it has with other forms of computer intrusion, particularly hacking. While both hacking and cyberterrorism are forms of intrusion, cyberterrorism has the distinctive characteristic of being intentional in wreaking havoc or causing harm.

A few examples were given to demonstrate the potential threat of cyberterrorism; it could flood a town, harm a power plant, cripple an entire infrastructure, or compromise computer systems. Although hacking could be a good means for threatening computers or make them more vulnerable, attacks through the Internet or against networks or systems need to have a terrorist component in order to be labeled "cyberterrorism." This is why the next sub-section purports itself to concentrate on the various motivations that cyberterrorists have for engaging in cyber attacks.

Cyberterrorism: Various Motivations

I asked the participants what the motivations to engage in cyberterrorism were. Most of the data I collected on this are consistent with the statements made in the literature review. For the purpose of this sub-section, I selected four relevant quotes that are representatives of many of the participants' accounts. For instance, asking a professor and executive director of an information security center at a Midwestern university what the motives of cyberterrorist acts are, he responded promptly with the following:

> Anything that would motivate someone to commit a terrorist act in the physical world could spawn an analog in the realm of digital information systems, computing, and the like. Cyberterrorism could be blowing up a chemical plant and disabling the phone systems. We don't protect our infrastructures as well as we should. Security and liability have not been at the forefront of those concerns up until recently.

The statements made by this participant are interesting because they give us an all-encompassing perspective of the motives of cyberterrorism. In essence, "anything that would motivate someone to commit a terrorist act in the physical world could spawn an

analog in the realm of digital information systems, computing, and the like." Based on this view, it follows that the motives of cyberterrorists are the same as those of conventional terrorists. What are the motives of conventional terrorists? There is a plethora of articles and books on the subject. For example, Der Derian (2005) maintains that terrorism is an act based on personal, political, social, ethnic, religious, ideological or similar motives. This goes directly to the assumptions made on cyberterrorism at the beginning of this literature review. Seventeen forms of cyberterrorism were given. In general, the motives are the same as those of conventional terrorists such as Al Qaeda. As such, a cyberterrorist act is any act committed for ideological, religious, political, or social reasons, or the threat thereof, via computers or the Internet. It could be destroying infrastructures; destroying the actual machinery of the information infrastructure, or the threat thereof; hacking into the controls of a nuclear power plant or a facility that handles hazardous materials, or the threat thereof, and so on. Regarding this last form of cyberterrorism, the statement made by the participant is almost identical (that is, "cyberterrorism could be blowing up a chemical plant and disabling the phone systems").

The following examples are an extension of the previous ones. Cyberterrorism could be shutting down power grids for ideological, religious, political, or social reasons (in the same way that conventional terrorists would), sabotaging operations; causing a fatal incident, coercing a government or a political faction, via computer technology, to modify, add, or subtract existing laws or rules; attacking a national, racial, religious, linguistic, or any social group or community, via computer technology, or the threat thereof. The point made here is that, whatever form of cyberterrorism it is, it resembles conventional terrorism because the motives are the same. The participant's account

corresponds with the assumptions made in this study. For this reason, terrorist motivations could spawn an analog in the digital realm. Asking another participant, who is the chair of a cyber forensics program in a department of computer and information technology at a Midwestern university (where he is also an associate professor), he responded with specific statements about the motives of cyberterrorists:

> They can have political, social, religious, ethnic, financial motives. They can have a mental illness too. Some of them can be state-sponsored, as it was the case for the defacement of Ariel Sharon's Web site. You've got individual motives. It all depends on their motives. It could be to cause fear of uncertainty. There's always the ability to impact financially. You make people uncertain or fearful of online transactions.

Again, it is very clear in those statements that they [cyberterrorists] can have political, social, religious, ethnic, or financial motives. The participant here even adds that defacing Web sites is a cyberterrorist act because it can be state-sponsored. Based on his belief about the defacement of Ariel Sharon's Web site, we can add that the purpose of cyberterrorism is also to spread political propaganda. No matter what, the ultimate goal is "to cause fear of uncertainty." Here, what is dealt with are not only the motives but also the effects of cyberterrorism on our society. The effects are based on the motives. The two concepts are highly correlated. This excerpt is also different from the previous one in that it also makes the point that the motives could be financial (i.e., "to impact financially" and to make people "uncertain or fearful of online transactions").

So, those who are likely to conduct cyber attacks are those who are socially, politically, financially, religiously, or ethnically motivated. Going back to the statement

made about Ariel Sharon's Web site, as we have seen in the literature review, in 2002 a cyberterrorist group known as the World Fantabulous Defacers (WFD), whose cultural practice is to wreak havoc on Web sites, delved into the Web site of Ariel Sharon, the Israeli Prime Minister, to deface it. They wrote, on his Web site, "The Face of the Biggest World's Murderer." According to Verton (2003), the WFD had strong political clashes with Sharon's administration. Those types of cyber attacks could pose serious threats. Another participant, a professor of social network theory, working closely with the FBI, made similar statements when he said that there have been Christian and Muslim Web sites defaced by each other:

> They [cyberterrorists] have many different motives, like political motives. If they have the mindset that a country shouldn't be acting the way they are, they can put pressure just like any traditional terrorist. We have been attacked multiple times, specifically United States Web sites, attacked and defaced, hosting companies taken down, uh, companies threatened of being taken down if they didn't stop supporting certain initiatives within the government. There have been quite a few different documented and probably even many more undocumented cases. Ideological motives would easily be the religious aspects. There have been Christian and Muslim Web sites defaced by each other, churches' and temples' Web sites defaced. Financial motives are not a big thing for cyberterrorists, but they have to be funded like every other group.

While the scholarly literature says that the defacement of Ariel Sharon's Web site was mainly politically motivated (Verton, 2003), here it seems that the "Christian and Muslim Web sites defaced by each other" are ideologically or religiously motivated (i.e.,

"Ideological motives would easily be the religious aspects"). Besides the Christian and Muslim Web sites defaced by each other, the participant says that churches' and temples' Web sites have been defaced as well. It is worth looking at the first statement ("They [cyberterrorists] have many different motives, like political motives. If they have the mindset that a country shouldn't be acting the way they are, they can put pressure just like any traditional terrorist"). A similarity can be drawn with the previous excerpt: their motives and acts can be applied in the digital realm ("just like any traditional terrorist").

Another important consideration is that cyberterrorists, as it is made clear by our participant, are not necessarily driven by financial motives ("Financial motives are not a big thing for cyberterrorists"). This goes back to the statement made about Nigerian scams in the previous sub-section; those scams are acts committed by cybercriminals because "those are basically people that exploit money." Nevertheless, based on the excerpt above, it seems that in order to be active and successful, they need financial resources ("they have to be funded like every other group"). Money, in this context, is used as a tool and not the ultimate objective of personal gain. The last excerpt of this sub-section focuses solely on one motive: political. It was selected from an interview conducted with a senior analyst engineer in forensics who also has an IT group. He and his group support the police of a Midwestern university (where that participant is employed), law enforcement investigations, and internal investigations for the Dean of Students and human resources:

> What will come in the next wave of cyberterrorism will be hugely destructive. The intent will be political; to bring down the politics of whatever you're opposed

to. The misconception of the cyber world is that we believe that cyberterrorists can't get us.

"The intent," says our participant, "will be political." A correlation can be made with statements written by scholars such as Anderson and Sloan (2002a) when they say that terrorism is primarily a political act. From this vantage point, just as it is for conventional terrorism, the intent of cyberterrorism is "to bring down the politics of whatever you're opposed to." So, based on the selected accounts, we can conclude that cyberterrorists have various motives that are identical to the motives of conventional terrorists. These motives can be social, ideological, religious, political or ethnic. As it turns out, the motive that emerges the most in these accounts is the political motive. By the same token, financial motives do not seem to be as prominent as the other motives. Nonetheless, in all cases, the intent is to cause harm via computer technology or the Internet, in the same way that the intent of terrorists is to cause harm by dropping bombs or engaging in similar types of action. The next few sub-sections will focus on issues and topics driven mostly by social network theory, the first of which pertains to what networks of cyberterrorists are.

Networks of Cyberterrorists: What Are They?

The data that pertain to this sub-section are mostly based on two interview questions, "What does a network of cyberterrorists look like?" and "What do cyberterrorists do in those networks of terror?" Nine excerpts were selected to illustrate that analyzing social networks of cyberterrorists is important because it helps us better understand how and why cyberterrorists interact with each other through those networks, and how the design of the network itself, especially in this day and age where the Internet

and computer technology play a central role, can facilitate their interactions. This analysis follows the premises of social network theory. Social network theory is the mapping and understanding of social networks (Lipnack & Stamps, 1986; Scott, 2000; Wasserman & Faust, 1994; Wellman & Berkowitz, 1988). The questions that pertain to the roles of hubs and depths of communication patterns are not dealt with in this sub-section, but will be in subsequent sub-sections. The first excerpt, taken from an interview conducted with a forensics examiner in the Southwest, gives a broad outlook of cyberterrorist networks:

> Usually, it's not just an individual. It's going to be a cyberterrorist joining a network. You get all these cyberterrorists that will go online and use IRC. They'll form kind of these loosely-knit groups. Then, um, they can communicate, transfer files, sharing information through IRC. They can share strategies and all those different things.

Based on these statements, the existence of networks among cyberterrorists is clear ("Usually, it's not just an individual. It's going to be a cyberterrorist joining a network"). Cyberterrorists, then, tend not to work alone; they feel the need to team up with others. Besides, when cyberterrorists network, they network with others via different channels of communication; what they do is "go online and use IRC." Note the emphasis on groups that are loosely knit ("They'll form kind of these loosely-knit groups"). As we will see later, the emergence of hubs is enabled by those groups that are loosely knit. The participant lists some of the activities that are done in those cyberterrorist networks ("they can communicate, transfer files, sharing information through IRC. They can share strategies and all those different things"). These practices reinforce the needs of the community of cyberterrorists without the necessity of creating a large-scale single

organization, like a massive conventional terrorist organization. The statements made by the participant are consistent with the descriptions of important issues in the scholarly literature. For instance, McKenzie (2004) argues that cyberterrorists have become involved in Internet social networks. Likewise, for Schwartau (1996), some cyberterrorist groups play the role of cybersurrogate groups in order to assist other cyberterrorists who are really in need of help (i.e., regarding the design of certain malicious software programs or, like the participant says, the sharing of information and strategies). The main goal is to increase their chances of successful cyberterrorist attacks against the Internet or computer networks. The creation of networks has been proven to be easy and advantageous (Schwartau, 1996). The following excerpt was taken from the account told by an IT Security Analyst II (an assistant forensics examiner) in the Southwest:

> You'll have two or three or four guys or girls in the cyberterrorist network. You'll never know if they've met before. They don't use their real identities. They're really smart; they understand how this works. They will write tools, scripts, um, programs that can harm your computer, and distribute them within that [cyberterrorist] network.

Cyberterrorist networks, as it transpires in the first statement, are composed of both "guys" and "girls." Interestingly enough, some of the literature mentions that those networks are composed of members of both gender (i.e., Levy, 2001). Another quote from a different participant says that "the average age of a cyberterrorist is twenty-eight years old." These demographics increase our knowledge somewhat, but what matters more is the fact that anybody can use the Internet to engage in cyber attacks and anybody can join a cyberterrorist network, regardless of gender or age. Speaking of gender, a

direct comparison can be drawn with conventional terrorist networks, where females have been known to commit terrorist acts, i.e., the Patty Hearst case (Holman, 2004). This exemplifies, again, that cyberterrorism is, in a lot of respects, terrorism in the digital realm. By the same token, the belief that the average age is twenty-eight years old shows that, in order to be a successful cyberterrorist, one needs to be very skilled with computers and spend a tremendous time online, learning all the tools and strategies to harm computer networks and systems. Can a twelve-year old hacker be as knowledgeable as a twenty-eight year old cyberterrorist? Levy (2001) mentions many non-cyberterrorist hackers whose ages range from twelve to nineteen. However, most of the members of the Chinese cyberterrorist group Titan Rain have a college degree, sometimes at the graduate level, or have done some military training (Schneier, 2005). So, it is no surprise that the average age of the cyberterrorist is in the late twenties. For all these reasons, it can be deduced that the previous statement that hackers, as opposed to cyberterrorists, "tend to be teenagers or computer-whiz kids" has some validity.

In a similar fashion, in the cyberterrorist network, the main actors might not know one another (as the participant says, "You'll never know if they've met before"). The fact that they might be unbeknownst to each other has been confirmed in scholarly pieces. McClure and Scambray (1999) maintain that the Internet can be used in such a way that the structure of cyberterrorist networks allows some groups to communicate with each other while they do not even know one another. Likewise, according to our participant, "they don't use their real identities." The postmodern nature of cyberspace is such that Web users can alter their identities within a few seconds. Postmodernism emphasizes fluidity and the immediate and constant re-referencing of identities. Identity becomes a

flux or, as Rheingold (1998) suggests, a "fluid" (p. 84) that enables Web users to be disembodied. In this sense, they can take a fluid role in the construction of identity through different levels and qualities of interaction. Anonymity works for cyberterrorists. This means that the self can be manipulated on the whims of its creator. It also entails fragmentation of the self, a term of postmodern identity construction (Matusitz, 2005c). While modernist notions of the self are based on the ideal of a stable, non-shifting identity, postmodernism conceives identity as continuously being shifting and reconstructed (Deibert, 1997). The next excerpt, taken from a cyber forensics specialist in the Midwest, also emphasizes the anonymous aspect of cyberspace, which makes the task easier for cyberterrorists:

> On the Internet, nobody knows you're a dog, which makes the task complicated for them [law enforcement]. It might even be the case that one federal agency is stalking the other agency. Who's part of a network of cyberterrorists? You don't know that until you catch one of them, and even if you catch one of them it's still gonna be hard to get the others.

Cyberterrorists protect themselves through the Internet. They can conceal specific parts of their identities: skin color, ethnicity, social status, sexual orientation, and so on. Sherry Turkle, in her book *Life on the Screen* (1995), shows how possible it is to alter our identities and how the intensive relationships Web users have with the Internet change the way they make their identities seem to be. Turkle describes the computer as a tool, a mirror, and as a gateway to the world through the looking glass of the screen. From this perspective, cyberterrorists use computers and the Internet as new media on which to project their new identities. The only way to bust them is to catch them in actual physical

space, a feature of modernism ("Who's part of a network of cyberterrorists? You don't know that until you catch one of them"). Cyberterrorists enter cyberspace as part of the routines of everyday life. Their concealed identities that turn into new or even multiple identities make their world ambiguous. A central tenet of postmodernism is the willingness to accept ambiguity (Kramer, 1997). It is so ambiguous that it confuses federal agencies ("It might even be the case that one federal agency is stalking the other agency"). From a social network theory standpoint, there cannot be mutual observable behavior between two nodes in a social network on the Internet, which is a direct contrast with dense networks in actual physical space, characterized by "network closure" (Coleman, 1990, p. 318). Network closure is the extent to which everyone knows everyone else in a network. The next excerpt, from the IT Security Analyst II mentioned earlier, underlines the formation of cyberterrorist networks through worldwide cooperation:

> There is cooperation among those groups around the globe that do try to help each other out. You're not only seeing U.S. cyberterrorists perpetrating against U.S. targets. It's global. It's gonna be someone in a country that has poor cybercrime laws or poor law enforcement that are willing to go after these targets there.

Again, based on the participant's words, cyberterrorists tend not to work alone. Instead, they cooperate and this can be done globally ("There is cooperation among those groups around the globe"). As the participant continues, cyberterrorists are not always geographically located at the same place ("You're not only seeing U.S. cyberterrorists perpetrating against U.S. targets. It's global"). From a social network theory perspective, the rapid evolution of global electronic networks such as the Internet points to the

potential of those networks to develop communication means that enable nodes to communicate and interact with other nodes in real time all over the world (Kettinger & Grover, 1997). In doing so, these nodes can easily create networks where they can collect information and transfer knowledge.

The last statements of this excerpt indicate specific areas where cyberterrorists might originate ("It's gonna be someone in a country that has poor cybercrime laws or poor law enforcement that are willing to go after these targets there"). Such was the case of Western European countries and former Soviet Union states a number of years ago. Recall what was said in the literature review; in the late 1980s, a German hacker group sold data to members of the ex-Soviet KGB. The German group accessed the information by hacking into computer systems in Departments of Energy and Defense, defense contractors, and NASA (Stohl, 1989). If they had been successful, the damage would have been colossal. Additionally, during the Persian Gulf War, a group of Dutch cyberterrorists who had intruded the Department of Defense systems attempted to sell their services to the Iraqis (General Accounting Office, 1991). These examples really demonstrate that cyberterrorist groups *do* try to create global networks in order to reach their outcomes. The next excerpt, selected from an interview conducted with a local law enforcement agent in the Midwest, deals specifically with the role of the Internet in the formation of cyberterrorist networks and the creation of sub-networks within the bigger network:

> I think that things are really easy for them [cyberterrorists] because of the nature of the Internet. It's all over the world and there are unimaginable ways to communicate with it within seconds. With that, you can create a network with

> tons of relationships, and it works for cyberterrorists. Once they have a network, they can also have other networks within that network, you know, like one small network under the big umbrella to recruit new potential cyberterrorists and another one to fundraise money for building new software programs.

Based on the participant's comments, it appears that the nature of the Internet can be an augmentation to the power of cyberterrorists to wage successful attacks ("I think that things are really easy for them [cyberterrorists] because of the nature of the Internet"). Besides, the Internet alters and defies the geometry of interrelations within networks ("It's all over the world and there are unimaginable ways to communicate with it"). This is a manifestation of the postmodern aspect of the Internet right there; the Internet, through "unimaginable ways to communicate," enables cyberterrorists to do things that would not be possible in the actual physical world of conventional terrorists. In addition, the Internet enables relationships to "transcend geographic boundaries into areas of the world" (Hecht, et al., 2005, p. 271) that Web users would not otherwise travel because the possibilities to transcend temporal boundaries are spectacular (i.e., communication can be done "within seconds").

In line with these arguments, the Internet offers cyberterrorists the possibility for creating networks with a significant number of relationships within a computer-mediated world ("you can create a network with tons of relationships"). More importantly, their networks can have sub-networks, like hybrids ("Once they have a network, they can also have other networks within that network"). In other words, cyberterrorists can create a combination of networks within networks or, simply, networks of networks. As such, one sub-network could be used "to recruit new potential cyberterrorists" and another one "to

"fundraise money for building new software programs." Sub-networks can break down what appears to be a single large network into smaller ones, which allows for numerous nodes to be linked in various ways, like in a spider's web (Barabasi, 2003). From all this, it appears that the design of a cyberterrorist network is the same as the design of a social network in that it is characterized by flexibility and a capacity to expand (through techniques like sub-networks) (Buchanan, 2002). The following excerpt, selected from an account told by a professor of social networks in the Midwest, builds on the previous excerpt with respect to the idea that the Internet modifies and challenges the geometry of interrelations within networks. It also brings information on the "all-channel" aspect of cyberterrorist networks:

> The way cyberterrorists communicate online is extremely fast and effective. Connections are made among all of them [cyberterrorists]. The Internet really helps a lot. Their networks are very heterogeneous. They have to be any way, otherwise they wouldn't be able to be loosely knit.

The way the participant describes the connections that are made possible among cyberterrorists thanks to the Internet illustrates the feature of an all-channel network (Bavelas, 1950; Leavitt, 1951), where any node in the network is linked to any other node ("Connections are made among all of them [cyberterrorists]"). The all-channel is collaborative, quick, and effective ("The way cyberterrorists communicate online is extremely fast and effective"), but can be difficult to maintain due to the significant need of exchange of information required. Nevertheless, it is the network of the information age and, when organized by cyberterrorists, it can be very effective (i.e., it can launch multiple, repeated attacks from different points) and very difficult to destroy in its

entirety (nodes are redundant). By extension, in such a postmodern social network, nodes – as trivial and innocent as they look – can be very powerful; the high number of nodes in a social network makes it a non-homogeneous entity ("Their networks are very heterogeneous"). A heterogeneous network consists of a mix of nodes that makes them loosely knit and, therefore, very difficult to identify. Plus, a non-homogeneous network has another advantage; failures are likely to occur on relatively small nodes (Faloutsos, Faloutsos, & Faloutsos, 1999; Matlis, 2002). On the other hand, a homogenous network is composed of closely-knit nodes, which makes the network more vulnerable and easier to identify (since all the nodes are very similar and follow the same pattern). The next excerpt, taken from an account told by an IT Analyst II, describes the absence of leadership in cyberterrorist networks:

> There is no leadership. If anything, it's more of a "lead by agreement." They might be the most experienced and skilled, but if you don't like what they do, they just go out or you get rid of that person. There's no hierarchy. You can usually tell in some that there is a natural order that works out between the younger hackers and the more experienced hackers, just like any pack of wolves or wild animals. The order is based on knowledge, skills, and experience. When their name is in the news, they put themselves above the other guys.

The first four words of this excerpt sum it all up: "There is no leadership." This assumption is very consistent with the findings of the study conducted by Arquilla, Ronfeldt, and Zanini (1999), where the three scholars argue that Internet-based intergroup networks of cyberterrorist cells symbolize the postmodern type of structure, that is, a move away from the traditionally organized, hierarchical design to the

decentralized and flexible horizontal structure. As such, the communication pattern and the flow of information in cyberterrorist networks move horizontally, non-linearly, and through many sub-networks. In other words, instead of operating through a central command structure – as it is the case in traditional terrorist organizations – in which information filters down from the top in a vertical and linear manner, information in cyberterrorist networks moves laterally from node to node. This non-hierarchical structure makes the nature of operations work asymmetrically and in an all-channel manner (Bavelas, 1950, Leavitt, 1951). So, as the participant says, "there's no hierarchy." The cyberterrorists who stand out in their networks are the ones who have more experience ("natural order that works out between the younger hackers and the more experienced hackers"). This also implies that they have more notoriety. However, they are not the leaders *per se*. Instead, our participant continues, "the order is based on knowledge, skills, and experience."

In line with these contentions, since cyberterrorist networks are organized on a non-hierarchical basis, they tend to be more nimble and flexible than hierarchies. As a result, their networks are more adaptable to changing circumstances. By the same token, they are not fixed but very malleable (Barabasi, 2002; Buchanan, 2002). They are mostly unplanned, emergent systems whose ties end up being disproportionately and unequally distributed, with some areas of the network sparsely connected. The next excerpt, selected from an interview conducted with the manager of an information security team at a Midwestern university, also emphasizes the lack of leadership in cyberterrorist networks:

> I think there is a bog underground network that exists because they have to communicate with one another. Cyberterrorism is not a one-man effort. I think that it's a group of individuals who are working together. That's where they conglomerate and get all this data in one area. They have different factions spread all over. I do not believe they have a leader because you will see internal fights within these groups, arguments between two members. It's almost who can show up the other.

"Cyberterrorism," says our manager of the information security team, "is not a one-man effort." Given this, they do have to collaborate or, at least, communicate with one another ("they have to communicate with one another"). Arquilla & Ronfeldt (2001) maintain that cyberterrorist groups, what the participant calls "factions," are likely to be composed of small units that communicate and plan their activities in an internetted manner. This is a break from the past when groups and units depended on a state sponsor for physical location and financing. Cyberterrorists, in contrast, can take actions without the need for a purported or outward commander ("I do not believe they have a leader"). The last excerpt of this sub-section draws attention to the importance of collaboration and interaction for their networks to survive:

> Typically, there's no hierarchy or structure. It's more like anarchy. There is no supreme god. They're independent, but they also have to collaborate, otherwise their network wouldn't survive. So, I think there must be some kind of interaction to make their network viable.

Again, their networks are not hierarchical ("there's no hierarchy"). Our participant goes even further by contending that their structures are more like anarchies

because, he says, “there is no supreme god.” The other statements highlight the importance of collaboration (“they also have to collaborate”) and interaction (“there must be some kind of interaction”) for their networks to remain viable (that is, “otherwise their network wouldn’t survive” and “to make their network viable”). This is a direct throwback to Hegel’s systems theory (Beiser, 1993; Kojève, 1969), upon which some of the main tenets of social network theory rest. Systems theory is based on the premise that, for a system to function, there must be interaction among its parts. In other words, networks cannot survive, let alone exist, without interaction or interconnection among nodes. Besides, parts (or nodes or individuals) cannot be understood in isolation from the whole (Banathy, 1996). For this reason, in this day and age, cyberterrorist networks model that design. They create complex systems of interconnections that have differentiated themselves horizontally into networks of interconnected social sub-systems (i.e., sub-networks or hybrids).

In summary, social network theory helps understand how cyberterrorist networks operate. Put simply, cyberterrorists are nodes in a network of rapidly expanding networks; they can be male or female with an average age of twenty-eight years old. Cyberterrorist networks are so flexible, nimble, and rapid that they can have sub-networks or hybrids. They are also characterized by a decentralized structure that is composed of cells. Given this, cyberterrorists do not communicate or collaborate among each other in traditional hierarchies (as opposed to armies and traditional terrorist organizations) (Barabasi, 2002). Because of the absence of leadership and the postmodern nature of the Internet, collaboration and communication in their networks

tend to be horizontal, in an all-channel manner (Bavelas, 1950; Leavitt, 1951), and anonymous.

Hubs as Humans with High Degrees of Centrality

In this sub-section, as well as the following two sub-sections, an analysis of the role of hubs is provided, based on social network theory. Hubs are those important nodes in the network of cyberterrorists that are so powerful that they connect a great number of other nodes [cyberterrorists]. The end-result of the analysis is that any type of network is much stronger when its hubs are active. Three types of hubs are identified in this study: (1) hubs as humans with high degrees of centrality, (2) hubs as go-betweens, and (3) hubs as central locations. The main questions that generated relevant data on this matter are the following: "Describe the role of nodes and hubs [minor and important actors] in the networks of cyberterrorists" and "Describe the degree of centrality in cyberterrorist networks." This first sub-section particularly examines hubs as humans with high degrees of centrality. Two quotes from accounts told by an IT Analyst II in the Southwest and a professor at a Midwestern university, respectively, serve to illustrate that hubs as humans have high degrees of centrality; they are givers/receivers and central locations for the other nodes. They also have great power in the network through their transfer and exchange of knowledge:

> I don't think they have a leader *per se*. I don't think they go through an election process. Generally, in a network of cyberterrorists, the person with the most skills or resources is the one that seems to be "running the show." A lot of times, that is the person that has the highest resources and connections.

We saw at the beginning of this study that a vast majority of nodes are connected to the network by way of just one link: fewer have two, even fewer have three, and so down the line (Barabasi, 2002). Unlike an exponential network, a cyberterrorist network has small but significant numbers of nodes that have many connections. Consequently, a cyberterrorist network exemplifies an uneven distribution of connectedness. Rather than having a random pattern of connections, some nodes act as very connected hubs, while many other nodes do not (Johnson, 2000; Keller, 2005). The role of hubs considerably influences how their network operates. The excerpt above portrays the hub as a human, more precisely as a person who is not a designated leader, but who has an effect on the other actors in the network through his or her highest skills, resources, and connections. The hub, in this context, is the one who seems to be "running the show." From this, it follows that, while many cyberterrorists are simple nodes, that is, cyberterrorists who do things and who have all kinds of skills or expertise, other fewer cyberterrorists are hubs. These hubs act as directors, that is, people with the highest power and who appear to be charismatic, influential, and motivating. More importantly, they are the ones who have the most connections. Given this, they are hubs who have high degrees of centrality; they are givers/receivers and central locations for the other nodes. They impact the flow of information and activity (Arquilla & Ronfeldt, 2001). The next excerpt is similar to the previous one, but focuses more on the value of hubs through the transfer and exchange of knowledge:

> What we are trying to understand here is how cyberterrorists congregate and transfer knowledge. They live in small circle networks that overlap to a certain extent. These networks have, indeed, hubs, but the hubs, in my view, are central

> individuals. They are not places necessarily. They are individuals that know more and are known by more people. They are essential for exchanging this knowledge; they are the people with the highest degree of centrality. And it goes very fast.

Hubs, our participant says, "are not places necessarily." From his statements, it follows that they are humans. These humans are important because they are "central individuals." This degree of centrality points to the notion that their networks have a number of direct connections to a human who acts as a router node (Lott & Taylor, 2005). Wigand (1997) argues that central individuals in a network enable quick communication with the nodes connected to them. From this vantage point, communication between simple nodes and hubs [central individuals] is mostly done through quick exchanges, meaning that relationships among the less important nodes in the network are not as fast. This is not a postmodern transformation because what makes communication among nodes vastly quicker in the network is the presence of a human hub. Our participant expresses it clearly: "And it goes very fast." This paves the way for innovative interactions among individuals greedy for wreaking havoc against computers and systems. By the same token, this is an addition to the main premise of systems theory, that is, that a system is the sum of all its parts plus the effects of interconnection and interdependency among those parts (Lilienfeld, 1978; Weinberg, 1975). Put another way, while systems theory rests on the principle that interrelations among all the parts of a system are vital [which implies that the system is more than the mere sum of its parts], the theory does not take into account the role of the important parts – which would be the hubs in the network – as social network theory does.

In a similar vein, what this excerpt illustrates is not only the importance of centrality, but also the importance of knowledge transfer and exchange ("They are essential for exchanging this knowledge"). What can be inferred is that exchange among cyberterrorists must pass through a hub that is a central node. Hubs can afford to be the ones in charge of transferring knowledge in the network because, as our participant says, "they are individuals that know more and are known by more people." This shows the importance of being a hub. This is crucial for cyberterrorists because a hub can provide the network the ability to communicate with other nodes one-to-many within seconds. And the Internet helps. What the Internet does is enable the development of communication patterns that did not exist before IT systems were implemented in social networks. The use of central individuals in conventional terrorist organizations was not as efficient as that of present-day cyberterrorist networks (Arquilla & Ronfeldt, 2001). Since relationships through hubs are the shortest and the most efficient, social network theory assumes the existence of a network characterized by sporadic but extremely fast exchanges that require neither prolonged human contact nor a social contract in order to persist.

So, this great timeliness of knowledge exchange through rapid communication between hubs and nodes enables cyberterrorist networks to be founded on unprecedentedly quick relationships with a wide range of actors. As it was recounted by some participants in previous sub-sections of this study, cyberterrorist networks span the globe. Their postmodern type of network is the opposite of dense networks. Dense networks lay emphasis on organizational cohesiveness with a central location to store information (Renzulli & Aldrich, 2005). The problem with centralization of information

is that the exchange of knowledge is not as fast, efficient, and resourceful. Besides, it is not as readily transferable to other actors. Given this, centralization of information does not allow for quick decisions. For cyberterrorists, knowledge is not something that can be stored in a central container. They need hubs, what our participant calls "people with the highest degree of centrality" and "individuals that know more and are known by more people."

Hubs as Go-Betweens

So far, the types of hubs that have been described were the hubs as humans with high degrees of centrality. The type of hub analyzed in this sub-section is similar to the previous except that it focuses more on the role of brokering or, simply put, the "go-between." To corroborate the arguments about the importance for cyberterrorist networks to have go-betweens, three quotes were selected from the interviews and one quote was selected from the scholarly literature. The first quote was taken from an interview conducted with a professor at a Midwestern university:

> These networks are kind of small, but they have go-betweens, individuals that contact multiple groups. These are the people that are more respected, that have greater fame if you want, individuals that have been there for some time. They're like a switch, like a switchboard if you want. And it's all on the Internet.

A go-between is a mediator who acts as a link between multiple actors (Pearson & Hobbs, 2004). A hub has a similar meaning: it is a place of convergence that links multiple actors (Greenie, 2005). For this professor at a Midwestern university, a go-between is someone who contacts multiple groups. They have the privilege to act as go-betweens because they are "more respected," they have "greater fame," and they "have

been there for some time." This view resembles the statements made by two previous participants, respectively, that the cyberterrorists with high degrees of centrality are the ones with the highest "skills, resources, and connections" and the ones who "know more and are known by more people." A go-between, our participant adds, is like a switchboard. From this statement, we can deduce that, just as the switchboard is an interface that connects lines and trunks, the go-between is an interface that connects nodes. The following excerpt was selected from an account told by the chief information security officer at a Midwestern university and its regional campuses:

> The cyberterrorists' market is like the mafia or the mob. They're getting into middlemen or the brokers of information. They're not only doing the hacking, they're also doing the selling. They want to make sure they cannot be found. They're not only doing the stealing of the data; they're also brokering; they're getting something off the top.

Based on this participant's statements, the go-between is the middleperson or the broker. The term "brokerage" has been defined as the occupancy of a structural position that links unconnected actors (Fernandez & Gould, 1994). A broker is a middleperson, a mediator, a go-between, or, as Granovetter (1973) would call it, a "local bridge." As a local bridge, he or she performs the role of a gatekeeper, whether it is between nodes that are already parts of a cyberterrorist network or nodes that are not yet part of the network, but that might be potential members. They might be very different in nature. In the excerpt above, the nodes that might get into contact with the cyberterrorist/broker can also be the ones that are being sold something. As the participant puts it, "the cyberterrorists' market is like the mafia or the mob;" "they're also doing the selling." The

selling of what? Dunnigan (2003) contends that it is not unusual for cyberterrorists to sell malicious software programs to nodes that are not part of their network, such as suspicious organizations. The brokering role of the cyberterrorist also implies that he or she "screens" outside resources (i.e., "stealing of the data") and communicates or exchanges them with other nodes. Fernandez and Gould (1994) maintain that brokerage involves the very notion that the broker finds himself or herself in a position where he or she is tied to nodes that are not necessarily interconnected. For Raider (1998), being a go-between in a network is very advantageous because,

> this brokerage or gatekeeping location in the social structure is a position of competitive advantage because it offers the opportunity to access diverse information, to control the transfer of information between disconnected parties, and to identify and broker transactions between otherwise disconnected parties (p. 5).

So, to have go-betweens is very crucial to the interconnectedness of the cyberterrorist network. Although few in numbers, go-betweens are not random; rather, they are so powerful that they connect a great number of other nodes. For Simmel (1950), the go-between becomes "the third who benefits," a.k.a. *tertius gaudens*, that is, the third who benefits from exchanging information with, say, two other nodes that do not necessarily know each other. Through the use of the Internet, information, secrets, ideas, knowledge, and even orders and assignments are transmitted by this hub, this central messenger, or this virtual master who maintains contact and communication. The last excerpt of this sub-section, selected from an interview conducted with the chair of a cyber forensics program in the department of computer and information technology at a

Midwestern university (where he is also an associate professor), also highlights the importance of having a go-between:

> In some of these social networks, some have a gatekeeper or a go-between, others don't. Those social networks that have a very loose structure have a go-between because it makes things easier for them, I mean, for the social networks. It's also much faster.

This quote, again, illustrates that a cyberterrorist can take advantage of the Internet in order to use it for communicating knowledge effectively to any other cyberterrorist in the network. In doing so, the cyberterrorist/go-between occupies a pivotal position in the network. The main benefit is that "it makes things easier" for the social network of cyberterrorists. As the participant continues, "it's also much faster." Barabasi (2002) maintains that the use of a go-between implies that the nodes in the network are not necessarily connected to one another; they might not even know about the existence of one another. Any node, however, can be connected to the go-between. By adopting this method, each node can obtain superior information due to the go-between's privileged position through his or her high degree of centrality. Truly, the important gain to all this is that greater connectivity through the cyberterrorist/go-between can tremendously improve and, ultimately, accelerate communication in the network. In turn, it will also enhance the performance of the cyberterrorist network overall (Arquilla & Ronfeldt, 2001).

Hubs as Central Locations

A third type of hub identified in the accounts told by the interviewees is the hub that acts as a central location. In this context, the hub acts as a place of convergence in

the network, that is, a central location where any cyberterrorist can meet. In fact, Zepp (1999) asserts that cyberterrorists need a "location" where they can meet, exchange ideas, trade insights, and share tools and software programs, all of which provide the means, knowledge, and incentives they need to wage cyber attacks. The first excerpt was selected from an interview with the same IT Analyst II mentioned previously:

> The university, for the most part, seems to be kind of a pass-through point to do other things. Universities are generally at the top of the list for cyberterrorists. Universities have a lot of IP addresses out there. So, they [cyberterrorists] start with the universities first because they are less secure. There are academic reasons for that. You know, a university has to be somewhat open.

The university is the central location here because, as the IT Analyst II expresses it, it is a "pass-through point." Cyberterrorists use universities for transit, for making a passage to other locations. As a result, universities are big hubs for cyberterrorists. What makes things easier for them is that, as the participant confers to us, "a university has to be somewhat open." How is it open? Through its huge number of IP addresses ("Universities have a lot of IP addresses out there"). IP stands for "Internet protocol." An IP address is a unique number that devices use to identify and communicate with one other through a network utilizing the Internet protocol standard (Kozeriok, 2005). Any participating network device – which includes, but is not limited to, routers, computers, Web servers, and internet fax machines – must have its own unique address (Matthews, 2005). The problem is that universities are so open that it is easier for cyberterrorists to delve into these IP devices that enable them "to do other things" such as hacking into computer networks that are related to these university IP addresses. The next excerpt,

from the same participant, discusses another type of hub as central location: the Internet Relay Chat (IRC). As the participant expresses it,

> I would say that probably 90% of all the machines that I've looked at use IRC to communicate. It's one of the first things we look at to see suspicious activities from a machine. We'll go out and see if it's doing IRC traffic because they will go back and use that communication path. It's definitely where they meet.

It would be wise to begin with a definition of Internet Relay Chat (IRC). IRC is a tool for instant communication over the Internet. In essence, it is designed for group (many-to-many) communication in channels or discussion forums; it also allows one-to-one communication (Charalabidis, 1999). The Internet Relay Chat is a big hub for cyberterrorists because this central location is factually a worldwide network where everybody can join. As our participant remarks, "they will go back and use that communication path" and "it's definitely where they meet." From this, it follows that millions of Web users the world over can use that communication path to chat with friends, discuss any subject, and collaborate on projects (Mutton, 2004). Yet, it is also a forum where cyberterrorists can recruit new potential members, share malicious software programs, and, of course, create networks. With a simple, well defined protocol, the Internet Relay Chat has become one of the hottest central locations. It is more than just a basic chat system; it is also a network of intercommunicating servers, allowing thousands of Web users to get connected from anywhere in the world using the IRC protocol (Mutton, 2004). As our security analyst declares, perhaps 90% of all the computer machines he looks at "use IRC to communicate." The last excerpt of this sub-section,

selected from the account told by the supervisor of a computer forensics unit in the Southwest, also focuses on chat rooms as central locations:

> Chat rooms are hubs for cyberterrorists. The Internet itself would be a huge hub, but if you think of individual nodes being one guy at this computer; the chat rooms and IRC are big areas where they meet. The reason is that it's flexible. They can be very anonymous there. They don't have to be discovered for who they are, for their true identities. So they can meet there and share information. The Internet is still kind of the Wild Wild West. Now, the new frontier is not policed *per se*. There are no cops walking on the Internet. So, it's an easy place to share criminal types of information.

His first sentence is clear: "Chat rooms are hubs for cyberterrorists." From a social network theory perspective, the chat room is a hub, a central location with a vast number of highly connected nodes. In this excerpt, it is also plainly stated that "the chat rooms and IRC are big areas where they meet." What this also means is that the larger the hub, the greater the number of links to it. And the higher the capacity of the hub, the faster its growth. There are countless chat rooms where cyberterrorists can communicate and network with one other. The reason they meet in these central locations, says our participant, lies in the fact that they are "flexible." Cyberterrorists, he continues, "can be very anonymous there." Zepp (1999) observes that in these chat rooms, cyberterrorists can ask others how to wage a cyber attack and get almost instant feedback. By the same token, this enables them not to waste time searching what they need on the World Wide Web or through newsgroups. For all these reasons, we can deduce that the "scale-free network" theory mentioned at the beginning of this long study can be applied here. As a

reminder, a scale-free network is recognized by its centrally located, highly connected hubs, which considerably influences the way the Internet operates (Dorogovtsev & Mendes, 2003).

Of equal importance is the principle that cyberterrorists function in an "all-channel" type of network, as it has been mentioned before (see Bavelas, 1950; Leavitt, 1951). The "all-channel" network is a network where all dispersed nodes can be connected to each other for simultaneous dissemination of information and instant coordination (Barabasi, 2002). This is precisely how the chat room works: simultaneous dissemination of information and immediate coordination. The chat room is a very good example of an Internet hub because it has decentralized command and control; it also has extremely fast communication flow between numerous nodes in the network. The participant goes even further when he says that the Internet itself is a huge hub. After all, cyberterrorism would be meaningless without the Internet because the literature shows that cyber attacks are mostly waged through the Internet (see Dunnigan, 2002; Verton, 2002a, 2003a). So, the Internet itself is a central location for those postmodern reapers of terror. Because this central location is so flexible, it turns out to be a form of "new frontier" or, as the participant puts it, "the Wild Wild West." A major difference from actual physical space is that the Internet is not "policed *per se*." As the participant continues, "there are no cops walking on the Internet." This, again, is a manifestation of postmodernism.

Networks of Cyberterrorists: Communities of Practice

This sub-section is an analysis of a set of data selected from the participants' views on the culture and practices of cyberterrorists' networks. As such, the question in

the interview protocol was the following: "Describe the culture or way of life of cyberterrorist networks." Based on six excerpts, it was found that a cyberterrorist network constitutes a culture in itself because it has its own distinctive "community of practice" that enables cyberterrorists to create and maintain their network. It was also found that part of their communities of practice involves a way of life that uses "leet" speak, a jargonized lingo used by cyberterrorists in order to reinforce their culture and avoid detection by law enforcement. Finally, it was also assumed that cyberterrorists tend to be emotional communicators via online media (i.e., the Internet).

The concept of community of practice is important in our effort to understand the complex relationships between cyberterrorists in cyberspace. Communities, unlike other types of structures, need to invite interaction to make them alive (Wenger, McDermott, & Snyder, 2002). Communities develop because of ongoing human interaction, regardless of time or place. The same happens on the Internet. Just as communities develop in cities and tropical forests, Web users can create cultures by exchanging ideas, collaborating on tasks, and developing relationships. Software programs and other sophisticated tools allow individuals to process and interpret information, construct meaning, and engage in social interaction with other individuals. The first excerpt, selected from an account told by a professor at a Midwestern university, discusses the role of knowledge in the cyberterrorists' communities of practice:

> I think cyberterrorist networks are the best example that we have of communities of practice. Basically, their knowledge is practical knowledge, embedded knowledge, and this knowledge is transferred from one individual to another

within these communities. They are rarely written down and very rarely systematized.

According to Wenger (1998), a community of practice refers to the process of social learning that occurs when individuals with a common interest in some areas collaborate over a certain period of time to share knowledge (i.e., ideas, solutions) and build innovations. Communities of practice have become associated with knowledge management as people increasingly see them as ways of developing social capital, feeding new knowledge, promoting innovation, and sharing existing information within a system (Saint-Onge & Wallace, 2003). Based on this participant's comments, it follows that, because "their knowledge is practical knowledge, embedded knowledge," cyberterrorist networks form "the best example that we have of communities of practice." This statement is very consistent with observations made in the scholarly literature on the subject. For instance, Hildreth and Kimble (2004) state that communities of practice are knowledge networks.

In the same train of thought, for the participant, embedded knowledge is knowledge that "is transferred from one individual to another within these communities." Leonard and Sensiper (1998) corroborate this idea when they say that embedded knowledge is subjective, experiential, and developed in the "here and now." As they continue, it is "semiconscious and unconscious knowledge held in peoples' heads and bodies" (p. 113). For these reasons, embedded knowledge is not much quantifiable and cannot be simply captured, codified, and stored (Hildreth & Kimble, 2002). Winograd and Flores (1986) describe embedded knowledge as lost in the unfathomable depths of

personal experience. The same professor at a Midwestern university adds another interesting quote on the subject:

> Cyberterrorist knowledge is tacit knowledge; it is embedded knowledge. It's not explicit, it's implicit. It's built in what they do and what they try to achieve, which is subversion. What they do is engage in subversive activities. From this perspective, they are very uninterested in the theoretical aspect of what they do. They are more interested in the broader implications of the technologies they use and the broader issues to build and maintain these infrastructures.

"Cyberterrorist knowledge," he says, "is tacit knowledge; it is embedded knowledge. It's not explicit, it's implicit." From this vantage point, communities of practice seem to offer a way to make tacit knowledge valuable, despite the fact that tacit knowledge cannot be easily captured, codified, and stored (Hildreth & Kimble, 2002). In the context of knowledge management (KM), Polanyi (1966, 1975) describes two types of knowledge: tacit knowledge and explicit knowledge. Tacit knowledge is embedded, unsystematic, personal, informal, and subjective knowledge, while explicit knowledge is codified, theoretical, communicated in the form of symbols, systematic, formal, and easier to exchange. Tacit knowledge is what the knower knows; it is gained through experience in a specific context (Flanagin, 2002) and it embodies beliefs and values (Nonaka & Takeuchi, 1995). Explicit knowledge is represented by some artifact (i.e., document or video) typically created with the goal of communicating with another person.

So, knowledge management (KM) is a strategy to capitalize on what a network knows (Knapp, 1998). The main goal is to acquire, coordinate, and communicate

knowledge of actors so that other actors can use it in order to be more efficient and productive in their endeavors (Alavi & Leidner, 1999). "Knowledge" here means both the experience and understanding of the network actors and the information available within the network (Marwick, 2001) and among the nodes that are interconnected. Sources of knowledge that come from outside a network are crucial to social learning in the network, the development of the network's abilities, and the innovation process. For these reasons, cyberterrorists are mostly interested in what they gain and learn from their own experience (i.e., "It's built in what they do and what they try to achieve"). They are not concerned with symbols and theories. Our participant expresses it clearly: "From this perspective, they are very uninterested in the theoretical aspect of what they do."

The next excerpt was selected from the captain of a Midwestern County Sheriff's Department. This captain also oversees IT operations for that Sheriff's Department, as well as the 911 systems of the county and its public safety network. This excerpt focuses a little bit more on cyberterrorists' cultural practice and identity formation in their networks and communities of practice:

> They do have a culture, that's why you have all these funky names that these cyberterrorists… these groups have online. The Internet is a great source of identity formation and education. Cyberterrorists do all these things because they can. They also like to send codes or leave like, you know, an impressionable signature about what their work is, whether it'd be a backward "7" or a different character that they type. It's some sort of identifiable thing that says, "I've been here." It's like the Da Vinci code.

This excerpt has several implications. First, as the participant suggests, "they do have a culture;" "the Internet is a great source of identity formation and education;" and they have "these funky names." These assumptions go along with the comments made by Poster (2001) that cyberterrorists' communities of practice are manifested through the interplay of cultural identity, the interaction among each other, and a strong motivation to wreak havoc on computers and networks. Since interaction among cyberterrorists is done anonymously, it allows them to engage in what our participant calls "identity formation." In other words, cyberspace allows them to create new identities; attributes of identity such as name, gender, class, race, physiognomy, and nationality are no longer at stake. The performance of identity, then, becomes less of a critical element of communicative practice in cyberspace (Wright, 2005). Cyberterrorists cannot locate and identify their identities through historically-established relation to physical phenomena like the body, land, physical environment, and social or political systems. Rather, cultural identities on the Internet are fluid and are a fleeting linkage to an ever-evolving and creative process of cultural construction (Frederick, 2005; Poster, 2001). Part of their identity is also to leave "an impressionable signature."

In addition, to create a community of practice is the ability to connect with people who have similar interests and may well be the key to cyberterrorists' networks. In that respect, based on what the captain calls "education," cyberterrorists appear to be interested in social learning (Bandura, 1977). Social learning is a process in which individuals are not only the active members in the community of practice, but also one through which they build their own identities *vis-à-vis* that community (Hildreth & Kimble, 2002). Members of communities of practice recognize that networking among

them is important for participation because actors in a network need to see themselves through each other and through communication (Wenger, 1998). Any community of practice like that of cyberterrorists will produce cultural practices such as tools, procedures, stories, and, of course, codes and languages (Hildreth & Kimble, 2002).

Speaking of languages, the next two excerpts were selected from participants who claim that cyberterrorists have come up with a new type of lingo that is peculiar to them and that aims at excluding "outsiders." This lingo or language code is called "leet speak" (Crystal, 2001). Leet speak is an online language code used in the Internet population, including cyberterrorists (Kee, 2005). More precisely, leet speak is a meta-textual system of symbols distinguished by complex layers of signification (Crystal, 2001). The quote below was told by an IT Security Analyst II in the Southwest:

> They [cyberterrorists] have this term called "leet speak," in which they have their lingo. "Leet" comes from "elite." You use character substitution. So, instead of using "elite," they will change to "leet." They'll do character substitution and do "l33t." It used to be a good way you communicated online to show how good your leet speak skills were. Now, cyberterrorists use it a lot, which makes it difficult for us, and law enforcement as well.

From this excerpt, it follows that cyberterrorists have their own community's lingo with specific categories and with changes in semantics, not only to hide meanings from the outsider world, but also to give it metaphorical beauty (i.e., "l33t" for "leet"). Phonetically, says our participant, the word "leet" comes from the word "elite." For Verhoeven (2000), "leet" is a cipher, or cryptic form of spelling that replaces letters with numbers (i.e., "h4cker"), symbols, and other letters that sound or look alike. Leet speak

originates from incorrect spelling due to speed of typing; then, it is intentionally and repeatedly used as incorrect (Carooso, 2004). What can be also inferred in this excerpt is that "leet" helps reinforce cyberterrorists' communities. It gives them a unique identity. Philipsen (1992) asserts that a community, in any society, can be established in a particular time and location, whether this time and location be recognized or not, which sets itself apart as a group of individuals with a common language [here, it is leet speak] as a method of communication and cultural bonding between its members.

This excerpt also states that because cyberterrorists use leet speak a lot, the task becomes difficult for cyber forensics experts – what the participant refers to as "us" – and law enforcement. For Carooso (2004), the goal of using leet speak is to prevent law enforcement agents from deciphering specific meanings. Davis (1997) predicted the need for culturally diverse groups such as cyberterrorists to develop their own systems of communication in order to mislead law enforcement and "cope with the new diversity" (p. 267). This can imply that part of the effort of law enforcement agents to understand the nature of cyberterrorists' communities (and the underlying reasons which may shed light as to why they engage in cyber attacks) is to concentrate not only on the technical skills of cyberterrorists (i.e., their abilities to develop malicious software programs), but also their codes and lingo.

The next excerpt, from the same participant, points out the use of leet speak in cyberterrorist networks. Yet, it also assumes that, while the language used by cyberterrorists is oftentimes English, it can become a language barrier if cyberterrorists come from foreign countries. This view is also supported by Barber (1995). Below is the quote from the participant:

> Of course, cyberterrorists sometimes face language barriers. You have Portuguese, French, German groups. But when they use leet speak, a jargonized lingo, they seem to understand one another better. What they'll do is change characters of important words and turn them into numbers. For example, symbols like "1337" are common to all cyberterrorist groups.

This excerpt corroborates the belief that leet speak has become a popular phenomenon among cyberterrorists. Leet speakers constitute a cultural group characterized by the secrecy and thrill of a specialized lingo (i.e., "What they'll do is change characters of important words and turn them into numbers") that excludes nodes that are not part of their networks (Crystal, 2001). Based on the first two sentences, it can be interpreted that those who want to engage in cyberterrorist activities had best read English if they want to reach maximized outcomes. However, "when they use leet speak," says our participant, "they seem to understand one another better." The last excerpt of this sub-section, selected from an account told by an assistant professor at a Midwestern university who is also involved in cyber forensics, rests on the main idea that in order to reinforce their messages, cyberterrorists have to find some common ground through emotions:

> I used to work with deaf students. Sign language is very limited; it's a representative language based on emotions. When you say, "This is my friend," you see the sign for "friend," which is my two fingers crossed, almost like a handshake. But if I were to tell you, "This is my *best* friend," you would see the emotions, not only through my finger gestures, but also my face. It's an emotional language. I think the same can be said, to some degree, about the communication

> styles in cyberterrorist networks. Whether it's the use of directed language, specific language, diatribes of intent or mission, or why they're doing this, or if it's for short statements such as "Today's the day," the statements are usually very long diatribes about how Americans are the infidels. Yet, when the statements are related to a specific point that's going to happen or issues that they are going to make, they are very much more specific. Email is nothing without the emotions. On the Internet, cyberterrorists have to be emotional communicators.

The general description of this long quote is that email communication, just like sign language, is very limited because it is a representative language that needs the expression of emotions for the message to be produced and understood to its fullest extent. For deaf students to say, "This is my *best* friend," they need to show the emotions, not only through their finger gestures, but also their face. Likewise, when cyberterrorists need to express statements related to specific events that will happen (or "issues that they are going to make"), they need to be much more specific. For this reason, email, an important means of communication for cyberterrorists (Dunnigan, 2003), is "nothing without the emotions." "On the Internet," our participant adds, "cyberterrorists have to be emotional communicators," in the same way that deaf students have to be emotional conveyers of message if they want to let their feelings come across in the most effective way.

So, in order to reinforce their messages, cyberterrorists have to find some common ties through emotions. Emotional communication is the ability to send emotional signals. This might be an additional reason that explains why cyberterrorist networks are communities of practice. Ekman (2003) argues that emotional

communicators allow people to communicate an expression. The purpose of emotional communication is to give one's feelings stronger about particular goals or reinforce a bond. The signal transmitted by the sender is transformed into a stimulus to cause a change (Hunter-Carsch & Cooper, 2006). The outcomes derived from emotional communication are the main basis for the goals to be achieved. For emotional communication to be understood via email, the receiver must be highly knowledgeable with the culture of the cyberterrorist networks and all their practices. Although it is known that sending text messages can be enhanced with emotional content (Longueuil, 2002), cyberterrorists must use a sort of universal language – leet speak is one – in order to be able to communicate their emotions in the most effective manner.

Communication between cyberterrorists, after all, is communication between humans. Communication happens not only in the cold and distant method of digits, but also in the emotionally direct and powerful language of images and sounds (Salem, Anne Bogat, & Reid, 1997). With this ability emerges a new, previously undreamed of possibility of using the computer as a means for conveying emotional communication. As the participant confers to us, cyberterrorists can do it too. From all this, it is reasonable to say that cyberterrorist networks enable affectionate, emotional communication. Yet, as Kee (2005) contends, it primarily depends on the culture of their communities of practice or even on the social context (i.e., the expectations, norms, and values of the members of the cyberterrorist networks).

Networks of Cyberterrorists: Networks of Trust

The very nature of cyberspace is paradoxical, liberating, empowering, fragmenting, and very changeable (Jordan, 1999; Lévy, 2000; Poster, 2001). Cyberspace

is so flexible that it yields a sensation of informational risk that can only be conquered through trust development (Nissenbaum, 2001). Leat speak is accounted for the way in which cyberterrorists attempt to not only keep law enforcement out of their network premises, but also to build trust among each other. Trust is the belief that, within a community of shared behaviors, honesty and cooperative behavior are expected on the part of all the members of that community (Fukuyama, 1996). Bucher (2002) explores the phenomenon of "trust development" in cyberspace as a key characteristic of online communication in networks of Web users. The postmodern, disembodied nature of communication in cyberspace seems to call for innovative ways of building trust. Yet, based on the quotes selected from two participants, it appears that trust is based on chaining (that is, following connections from one friend to the next), a practice that has been used since the birth of civilization. The first quote comes from an interview conducted with a forensics examiner who also happens to be a graduate student at a Southwestern university:

> In a network of cyberterrorists, a friend of a friend introduces you. Again, it's all a network of trust. Somebody has to introduce you first or you have to make a name for yourself in your own right so that you get someone's attention, someone who can contact their friends to let you in.

This quote illustrates that trust is important in networks of cyberterrorists. Misztal (1996) remarks that trust makes outcomes more predictable, creates a sense of community, and makes it easier for people to collaborate on tasks and projects. These assumptions seem to work perfectly for cyberterrorists: by working with other cyberterrorists that they trust, outcomes will likely be more predictable, their

communities will be reinforced, and they will be more able to work on tasks and projects. So, how is trust built then? Based on the participant's statements, "somebody has to introduce you first." This notion of trust resembles that of the community of practice described previously in that both involve relationships between inviduals. By introducing "a friend of a friend," there is an implied belief by one person that another's motivations towards them are well-intended and honest. This practice of using a friend to gain more people in the network is called chaining (Madorsky Elman & Kennedy-Moore, 2003). From a social network theory perspective, chaining implies following connections from one node to the next.

It is important to note that this quote stresses that reputation alone can help a cyberterrorist gain trust from a cyberterrorist network. As the participant puts it, "you get someone's attention, someone who can contact their friends to let you in." Nevertheless, the process of "getting in" the network is still done through chaining ("someone who can contact their friends to let you in"). The second quote, told by a professor at a Midwestern university, compares cyberterrorist communities with conspiratorial communities of the past, which is his account for how trust is developed in their networks:

> Cyberterrorist communities are very much like your typical conspiratorial communities of war from the 19th century, like the Carbonari of Italy or the masons, where trust is important. They congregate enough people that they kind of know. Those people only get in if somebody kinda knows them, not that people know each other personally, but they know each other from online identities.

They are let in as more and more people are willing to vouch for their name and reputation.

The first statement is worth to be analyzed: cyberterrorist communities are very much like the Carbonari in Italy and the (Free)masons. The Carbonari (which means "coalminers") were a group of secret revolutionary societies created in Italy in the 19th century. They were very good at orchestrating revolutions not only in Italy, but also in countries like Spain (Frost, 2005). They were organized in the fashion of cyberterrorists, broken into small cells scattered across Italy. Freemasonry, still existing today, is a fraternal organization where members are united by shared ideals (Hodapp, 2005). While certain aspects of Freemasons' networks and practices are not disclosed to the public, Freemasons have become notorious worldwide for their lodges (Mackey, 1996), that is, their locations for meetings and congregations. The Freemasons have been accused of creating conspiracies against certain governments (Davis & Preiss, 2006). Both the Carbonari's and Freemasons' organizational structure, as opposed to the design of cyberterrorist networks, is very hierarchical.

What characterizes both societies is the value of trust ("where trust is important"). After all, what is conspiracy? It is a secret agreement between individuals to commit a malicious act. For conspiracy to succeed, trust is essential (Vankin & Walen, 2004). How is trust built? Based on the participant's statements, it can be inferred that it comes from chaining ("They congregate enough people that they kind of know. Those people only get in if somebody kinda knows them, not that people know each other personally"). Chaining is a series of connections that start with a trustworthy node. This node will

contact another node to make nodes connect with another. The ultimate goal is to create a flexible, trustworthy network.

Networks of Cyberterrorists: The Individualism-Collectivism Dimension

The analysis of cyberterrorist networks can be articulated upon the individualism-collectivism dimension as well. When designing the questionnaire, I did not anticipate to collect any data that would pertain to the individualism-collectivism dimension. Yet, two strong quotes, selected from the answers to the question that was analyzed earlier ("Describe the culture or way of life of cyberterrorist networks"), reveal that cyberterrorists tend to be individualistic, even if they are part of a cyberterrorist network and even if they come from collectivistic cultures. The analysis of the motivations of cyberterrorists to engage in attacks against computers and networks was done earlier. However, there was no mention of individualistic or collectivistic motivations behind the cyber attacks. So, it might prove interesting to do an analysis of the issue. Let us begin with a definition of collectivism and individualism. Collectivism is defined as a social pattern consisting of individuals who see themselves as part of one or more collectives. This worldview demonstrates measurement of dependency between one another (Hofstede, 1991). Individualism is a social pattern that consists of individuals who view themselves as independent of collectives (Triandis, 1995).

However, it is important to note that some scholars have called into question the value of the individualism-collectivism dimension. For instance, Voronov and Singer (2002) claim that a whole culture or civilization cannot be pigeonholed in a dichotomous category such as individualism-collectivism. For these two scholars, individualism and collectivism are descriptive labels that evoke "unduly fixed and caricature-like mental

impressions of cultures" (Voronov & Singer, 2002, p. 461). Likewise, for Sinha and Tripathi, 1994), this worldview is too "black or white." For them, presenting cultures in those terms "not only clouds one's understanding of them, but inevitably leads to good-bad comparisons" (p. 123). Nevertheless, the dimension of individualism-collectivism is not always a "catchcall default explanation for cultural differences in human behavior" (Kagitcibasi, 1994, p. 55). The dimension still holds value in specific contexts. The first quote reinforces the arguments made by Triandis. The quote was taken from an interview conducted with a chief information security officer in the upper Midwest. He has a degree in law and said that he lived overseas for a certain period of time. In his excerpt, he says that,

> cyberterrorists come from all over the world. They come from the U.S., from China, from Korea, from all over. Regardless of where they come from, if they want to compromise your network, sometimes they'll work together on that. You know, the culture of cyberterrorists tend to be similar in many places. You sit in front of the screen and you try to get software programs out to cripple networks. If an Asian cyberterrorist hacks into your computer, most of the time I don't think he'll do it for the benefit of the collective. He's a cyberterrorist. He knows he's taking risks.

The last statement of this quote exemplifies elements of individualism: "He's a cyberterrorist. He knows he's taking risks." One of the variables used to understand the differences between collectivism and individualism is the variable of risk. While collectivists tend to be risk-avoidant (Sinha, 1997), individualists support risk taking (Ohbuchi, Fukushima, & Tedeschi, 1999). In a similar fashion, the statement, "I don't

think he'll [an Asian cyberterrorist] do it for the benefit of the collective," also depicts major tenets of individualism. Kling and Carmel (1997) note that, in the context of cyberterrorism, malicious computer hackers tend to be individualistic. The individualistic cyberterrorist's mindset and his or her risk-taking computer ethos, that is, being innovative in targeting computer systems or delving into networks where nobody has dared going before (Kling & Carmel, 1997), have led to the conclusion that individualists have the best flexibility and adaptability in dealing with the unexpected; they are also among the least likely to be overpowered by cyber attacks (MacNulty, 1999). The second quote was selected from an account told by a computer analyst in a Midwestern university:

> I don't know that cyberterrorists are state-sponsored. It's hard to tell. I've read before that Titan Rain was being backed up by the Chinese government, but that's just speculation. Even if that's true, I think that cyberterrorists are people that start as individualistic hackers in their teens. At the beginning, they do it to show off, and then they become nastier as they get better.

Again, the belief that cyberterrorists are individualists is evident ("I think that cyberterrorists are people that start as individualistic hackers"). Our participant also mentions Titan Rain, a group of Chinese cyberterrorists. He doubts that Titan Rain is supported by the Chinese government. No matter what the situation is, we can deduce, based on these two quotes, that, although the thinking pattern most prevalent in a dominant culture is typically the most highly valued in that culture, a risk-taking cyberterrorist tends to be individualistic, even if he or she is a Chinese cyberterrorist hired by the Chinese government to attack an American computer system. As a matter of

fact, the literature says that it is the case of Titan Rain; they are stealing U.S. secrets (Thornburgh et al., 2005). Titan Rain is thought to be highly risk-taking and among the most pervasive threats that U.S. computer networks have ever faced. They engage in malicious hacking to such a large degree that they fall into the category of "extreme individualism" (Hay, 2000, p. 39). Drawing upon the individualism-collectivism dimension, this means that even in collectivistic cultures there are people who are idiocentric, that is, who believe, feel, and act like other individualists around the world (Triandis, 1995).

Another important consideration is that individualistic cyberterrorists' concept of themselves is contingent upon their ability to compare themselves with others ("they do it to show off"). To strengthen this statement, Kling and Carmel (1997) found that their self-esteem is contingent upon finding themselves to be "better off." Display of their hacking talents, and particularly the display of potential successes (i.e., disrupting a large computer network like a university computer network, even for just fifteen minutes, is considered a major success by many hackers), is a necessary element in establishing their worth or "name" in the cyber world. What comes next is an account of cyberterrorism and intercultural differences on privacy.

Cyberterrorism and Intercultural Differences on Privacy

The question of privacy in cyberspace has already been studied by scholars such as Capurro (2005) and Nakada and Tamura (2005). Yet, no scholarly work has ever been published on the conception of privacy in the cyberterrorist's culture. The data provided in this sub-section come from two excerpts selected from interviews conducted with the same upper Midwestern chief information security officer mentioned earlier and a law

enforcement agent in the Midwest. Privacy, defined as the condition of being concealed or hidden, can be achieved by "the management of interaction and information" (Laufer & Wolfe, 1977, p. 23). Privacy is a cultural universal, but the conceptions thereof vary from culture to culture (Altman, 1977). Concern over privacy has been associated with cultural values. Specifically, individuals in individualistic cultures as measured by Hofstede's (1991) individualism-collectivism index are more concerned about privacy than collectivists (Milberg, Smith, & Burke, 2000; Smith, 2001).

One aspect of privacy that is specifically analyzed in this sub-section is private space on the Internet. Space is a major standard by which a culture designates who has privilege (Wood, 1994). With regard to the conception of privacy in the cyberterrorist's culture, the degree of file penetration is culturally based (Debrix, 2001). The level of file protection is culturally based too; it depends on the concern for invasion of privacy. One way of grasping the importance attached to private space on the Internet is the extent to which disclosure of information is deliberately kept private. Tran (1996) argues that "in intercultural communication there is often an overlap, where what is personal for one culture is considered public in another, and vice versa. It is in this area of overlap where communication problems occur" (p. 214). To illustrate these postulations, let us analyze the first quote:

> We tend to see the development of software as being an intellectual property of values. In our country, we value individual creation and we're trying to protect it, even on the Internet. Not everybody in the world sees it that way. Some network intruders see software and hardware as being opportunities for advancement. They don't see something like software as something you can't really touch.

The chief information security officer comes from the American upper Midwest. He is no Asian and was probably not raised in a strongly collectivistic family as many Asians are. As he made it obvious in his quote, "we value individual creation and we're trying to protect it, even on the Internet." Private space is a major standard by which our participant designates who has privilege. For our participant, because "the development of software" is "an intellectual property of values," nobody else can invade his private property, even if it is on the Internet. For this reason, he will try to protect it. With respect to the individualism-collectivism dimension, Triandis (1995) asserts that individualists are mainly motivated by their own preferences, needs, and rights. Individualists are more aware of their rights to privacy (and to a greater extent). The debate is complicated by intercultural dimensions on privacy today; what is viewed as freedom in some cultures is perceived as taboo in other cultures.

Nevertheless, our participant seems to be aware of intercultural differences when he says that "not everybody in the world sees it that way." He contends that "some network intruders see software and hardware as being opportunities for advancement." What it all boils down to saying is that, based on the individualism-collectivism worldview, mindsets and thinking patterns (i.e., reasoning) are valued differently from culture to culture (Johari, 2005) and this has an impact on the way cyberterrorist operations are conducted. From this vantage point, some cyberterrorists "don't see something like software as something you can't really touch." The second quote, taken from an account told by a law enforcement agent in the Midwest, also attributes online invasions of privacy and cyber attacks to cyberterrorists with a different culture, particularly a collectivistic culture. As he explains it,

> if a cyberterrorist steals your data, they might not see it as stealing. Opposition of values causes a big problem. I tend to think that somebody coming around on my network without coming to the front door snooping is improper. But it might be normal for them to nose around somebody else's property. So, some of it is cultural. If they come from a culture that values collective property, then it might be normal for them to delve into my network.

While individualists hold that people should mind their own business and that private space should be respected (Triandis, 1995), collectivists believe that the space of the collective is also one's space (as the participant remarks, "if they [cyberterrorists] come from a culture that values collective property, then it might be normal for them to delve into my network"). According to the collectivists, people should be concerned with each other's personal matters (i.e., "it might be normal for them to nose around somebody else's property"). "Putting one's nose in another person's business" is absolutely reasonable and expected. The collective is entitled to know, even regulate, what others do privately (Hofstede, 1991). As a result, cyberterrorists from collectivistic cultures see the Internet as a place where they can access any Web site they want, log into others' accounts, and penetrate anybody's private cyber "space." Conversely, individualist Web users will try to protect their files by having two layers of password protection, by changing their password every month, and by installing firewalls and anti-virus software. Their goal is to make sure that no other Web user invades or even knows "what is going on" in their private space. As the participant contends, invading one's space is improper (i.e., "I tend to think that somebody coming around on my network without coming to the front door snooping is improper").

However, as it was argued in the previous sub-section, the small fractions of highly skilled computer and Internet users worldwide may share the same levels of individualistic privacy preferences and concerns (Smith & Bond, 1993), regardless of the fact that they belong to individualistic or collectivistic cultures. For this reason, even in collectivistic cultures, there are idiocentric people; they believe, feel, and act like other individualists around the world (Triandis, 1995). Now that we have seen the participants' [computer security experts' and law enforcement officials'] perspectives on what cyberterrorism is, what the motivations of cyberterrorists are, what the social networks of cyberterrorists are, what actions and practices are accomplished in these networks, the manners in which they create these networks, the roles of nodes and hubs [minor and important actors] in the networks, the degree of centrality in cyberterrorist networks, and the culture and way of life of these networks, let us move on to the analysis of **RQ2**, that is, the analysis of the accounts told by computer security experts and law enforcement officials about their own networks.

Chapter V

Analysis of Research Question 2

In order to answer **RQ2** (What do computer security experts' and law enforcement officials' accounts reveal about their own networks?), the following questions were asked in each interview: (1) What types of networks do you use to combat cyberterrorism?; (2) What do you do in those networks?; (3) Is it necessary to create networks against networks? Explain; (4) Describe the downsides to networking with other agencies; (5) Are those networks formal or informal? Explain; (6) Describe the role of nodes and hubs [minor and important actors] in your networks; (7) Describe the degree of centrality in your networks. As it was for the analysis of **RQ1**, these questions were mostly driven by social network theory and do not include probing questions that were asked during each interview because, for each participant, the interviews progressed differently. Let us begin by analyzing the participants' accounts of what networks of cyber forensics experts and law enforcement agents are.

Networks of Cyber Forensics Experts and Law Enforcement Agents: What Are They?

This sub-section is based on accounts solicited by two questions, "What types of networks do you use to combat cyberterrorism?" and "What do you do in those networks?" The participants' accounts in this context are broad and touch a little bit on specific concepts of social network theory like structures, nodes, hubs, and degrees of centrality. These concepts will be subject to an in-depth analysis later. Nevertheless, the quotes selected here are consistent with the statements made by various scholars about networks between law enforcement agencies and cyber forensics laboratories. Not only do the accounts focus on what networking designs and strategies are used in order to stop,

or at least, understand social networks of terror, but they also explain how networks are created at all levels: local, federal, national, and international. Four excerpts were selected to illustrate all this. The first excerpt was taken from an account told by an IT Security Analyst in the Southwest and illustrates that networking against cyberterrorism is done at the global level:

> You're talking about an international network. The FBI and different groups cooperate with other governments. You can go to the German equivalent of the FBI and say, "We're looking at this case; we think there's a cyberterrorist group here." Here is the evidence; help us prosecute these people.

In the same way that cyberterrorists collaborate worldwide thanks to the rapid evolution of global electronic networks and anonymity on the Internet, law enforcement agencies also join forces internationally ("You're talking about an international network"). Our participant gives a few examples (i.e., "You can go to the German equivalent of the FBI and say, 'We're looking at this case; we think there's a cyberterrorist group here'"). If the cyberterrorist is in Germany, American federal agencies will be more able to prosecute him or her if they already have connections with the proper authorities in Germany ("Here is the evidence; help us prosecute these people"). The next quote, from an assistant professor at a Midwestern university, reinforces the same belief that these networks are international:

> Computer forensics labs work together with local police departments. It depends on the crime, the level of the scene, or the escalation of the crime. Mostly, it is LE to LE [law enforcement]. It's global. Sometimes, differences in U.S. laws and international laws create difficulties. So, we'll need the UK, Germany, France, all

collaborating with the U.S. We would tell them, "Go to this computer, you'll find this, this, and this on it."

From this excerpt, it follows that collaboration occurs on many levels: (1) computer forensics labs with local police departments; (2) LE to LE [law enforcement]; and (3) globally ("Sometimes, we'll need the UK, Germany, France, all collaborating with the U.S."). With respect to the third point, because cyberterrorism is a problem that is very international, the need of networks to counter this problem almost goes without saying. The statements made by this participant are in harmony with studies found in recent scholarly articles on the matter. For instance, as Hutton and Mydlarz (2003) contend, Diplomatic Security (DS) trains foreign law enforcement officers in the reduction of cyber threats and repercussions of cyberterrorism throughout the world. Most of these training sessions are in Europe. In a similar vein, the U.S. National White Collar Crime Center is teaming up with counter-cyberterrorism agencies in Russia and Eastern Europe to help prosecute online intruders (Kshetri, 2005).

The necessity to create networks also stems from the fact that American cyber laws cannot be applied the same way everywhere. As Aeilts (2005) remarks, cyberterrorism incidents can cross regional, state, and even international jurisdictional boundaries, to the point where traditional jurisdictions and boundaries do not apply. For this reason, American federal agencies need to network with foreign agencies that would be willing to go after the identified cyberterrorists and prosecute them. As the participant tells us, directions on how to recognize a cyberthreat can be given from the U.S. itself (i.e., "We would tell them [foreign countries], "Go to this computer, you'll find this, this, and this on it"). Besides, going back to the legal barriers, language problems, as Cutler

(1999) remarks, constitute many obstacles to U.S. investigations abroad. Pacts and treaties date from as far back as the 1800s and their requirements vary from country to country. Because of this, "courts face the complicated task of applying constitutional protections from the eighteenth century to today's computerized world (Ziff, 2005, p. 841). As the participant expresses it, "differences in U.S. laws and international laws create difficulties." For this reason, U.S. federal agencies have started to create networks with countries like the UK, Germany, and France. Some countries allow U.S. officials to interrogate potential cyber attackers and obtain documents from cooperative individuals or organizations. Other countries do not, as they view it as a violation of their sovereignty (Cutler, 1999).

As it has been mentioned several times, cyberspace's very design dispenses with national borders. In fact, the postmodern nature of the Net is such that the Net really is a computer system on a global scale (Cangemi, 2004). However, still today, under the long-standing principles of international law, countries have jurisdiction only on the territory upon which they exercise their national sovereignty. Thus, a conflict exists between cyberterrorism, global in scale, and criminal activities confined to national borders (Cangemi, 2004). Considering these facts, it is no surprise that American federal agencies have started to create networks with foreign agencies that have specialties in computer forensics. Our participant expresses it clearly ("It's global"). Any law enforcement approach has to face with the reality that virus authorship is a highly international phenomenon. Any action based on law enforcement or legislatively mandated authentication would likely raise some eye-brows in some countries or even leave the entire Internet vulnerable to virus attacks in other countries. For these reasons,

international collaboration has been intensified for the past couple of years (Barnes, 2004).

The following excerpt does not deal with international cooperation among federal agencies, but pertains to a model of social network design based on the description of how computer forensics experts collaborate with other agencies, some of which collaborate among themselves as well:

> I have two positions. My first position is within an IT group where I am the senior analyst engineer in forensics and I do forensics for that IT group. I also have a position as an assistant professor with the college of technology, where I teach computer forensics at the graduate and undergraduate level. I have a very strong relationship with local law enforcement. I work fairly regularly with the state police. I have a relationship with the Department of Justice as well. Then, there is the entire network of the Big 10 universities. We get together in person four times a year. We work in circles. Sometimes, our state police will collaborate with agencies from other Big 10 states and local enforcement will be contacted by the Department of Justice. Those agencies don't always go through me. We try to share the cyberterrorists' signatures that we found after they committed their attacks. We just ask one another, "Are you seeing this?" If they see the same signatures, I can tell them other things to look for.

Figure 5 on the next page illustrates a social network design where interagency connections are done in an all-channel manner (Bavelas, 1950; Leavitt, 1951). Any node in the network, mainly composed of law enforcement agencies, can connect with any other node. As opposed to the "star" or "wheel" network (Bavelas, 1950), there is no

central point that shows a hub to which all the nodes of the network are connected. Rather, this network does not have a node with a high degree of centrality.

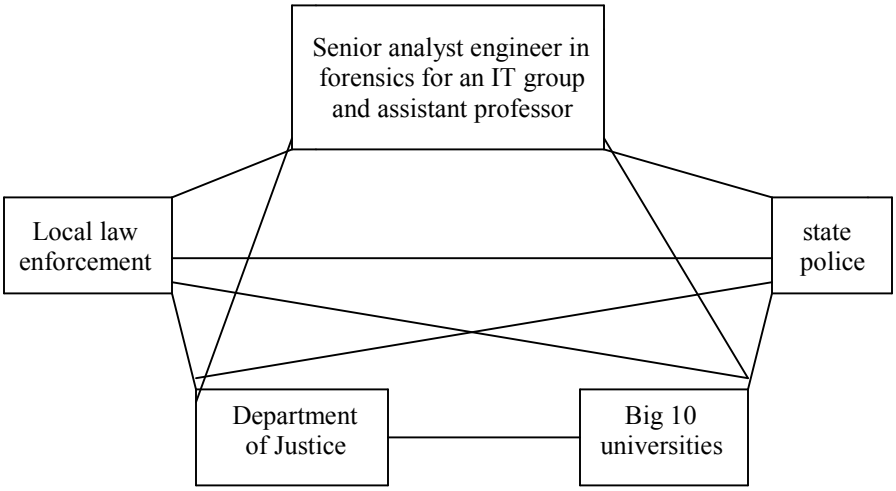

Figure 5 *Example of five nodes composing an all-channel network. There is no central node or high degree of centrality.*

Indeed, there is no prominent individual or group that stands at the center of the network and that has influence on its environment (i.e., in terms of decision-making, etc.). As the participant explains it, "we work in circles. Sometimes, our state police will collaborate with agencies from other Big 10 states and local enforcement will be contacted by the Department of Justice. Those agencies don't always go through me." This means that the all-channel network above is collaborative and multi-directional. There is no central commander. In other words, it is a full-matrix networks, where every cell is connected to one another and can communicate directly with every other cell (Evan, 1972). In the all-channel network, the measure of visibility is the number of links (Barabasi, 2003). The last excerpt of this sub-section, from a local officer in the

Southwest, is more an account of the fact that, in some cases, there is a jurisdictional hierarchy between law enforcement agencies:

> Homeland Security, in conjunction with various information-sharing analysis centers (ISACs), is finally starting to share information with all sorts of cyber forensics agencies, even the local ones, across state lines. They also try to get people within the states to understand that they need to share information with county governments. If a cyberterrorist case goes to federal agencies, they have jurisdictional power over us [the local police department].

This excerpt points to the collaboration between the Department of Homeland Security and "all sorts of cyber forensics agencies, even the local ones, across state lines." This act of working jointly goes even further as the participant says that "they [Homeland Security, in conjunction with various information-sharing analysis centers (ISACs)] also try to get people within the states to understand that they need to share information with county governments." However, as opposed to the design of cyberterrorist networks, there is a clear hierarchical structure that a cyberterrorist case must go through. Based on the participant's last statements in this quote, "if a cyberterrorist case goes to federal agencies, they have jurisdictional power over us [the local police department]," the Department of Homeland Security has supremacy over other agencies when a cyberterrorist case has to be investigated.

From a social network perspective, while it is reported that cyberterrorists consider hierarchies as clumsy techniques to use in their networks (Arquilla & Rondfeldt, 2001), it appears from this excerpt that some law enforcement agencies follow a design where there is a jurisdictional hierarchy between them, especially when it comes to

investigating specific cases of cyberterrorism. This contrasts with the social network design portrayed in the previous excerpt, where connections among all agencies are made in an all-channel manner. No matter what, both cyberterrorists' and law enforcement's networks are similar overall, but they also have a few differences. The next excerpt, taken from an interview conducted with a lady who does strategic relations and communications between different agencies in the Midwest, deals with ethical issues based on the actions taken by law enforcement agents:

> I'm really glad you're doing a study on that. Cyberterrorism needs to be explored, but I think it's important to explore the role of law enforcement agents too. I mean, if they network among each other to monitor our private email, do their actions fall on the ethical side, even if their ultimate goal is to catch the bad guys?

It was explained in the literature review that the FBI has authorization from any Internet Service Provider to use Carnivore, a machine that observes and reads email, and that monitors other online communications (Mansfield, 2000). Yet, the participant expresses some concerns about the fact that the actions of the network of law enforcement agents are to monitor our private email. From this, it can be interpreted that we – that is, the average citizens – have a right to privacy. How can the line be drawn? For the participant, "even if their ultimate goal is to catch the bad guys," does a law enforcement agency have the right to take those actions? In other words, what she is asking is the following: is computerized surveillance acceptable from an ethical standpoint, even if the objective is to protect society as a whole? Those issues are interesting because they pertain to many of us, computer users. The next sub-section

deals with the necessity for law enforcement agents and cyber forensics experts to create networks.

Networks of Cyber Forensics Experts and Law Enforcement Agents: A Necessity

Recall the six words used by Arquilla and Rondfeldt (2001) in the literature review: it takes networks to fight networks. Many participants reveal that it is necessary to join forces, through networking, in order to fight, let alone understand, cyberterrorist networks. As it turns out, it is also very advantageous for cyber forensics labs to do so. This sub-section is based on accounts mainly solicited by the following question, "Is it necessary to create networks against networks? Explain." The participants' accounts are consistent with reports made in the literature review and scholarly publications about the importance for cyber forensics experts and law enforcement officials to create networks. The first quote, selected from an interview conducted with a former FBI agent who worked as a computer forensics expert (now an assistant professor at a Southwestern university), emphasizes the need to network because of jurisdictional reasons:

> Now, certainly, in the area of cyberterrorism, it's a necessity that you network with state, federal, and other state agencies within inter-states because most of these types of crimes cross jurisdictional boundaries. So, oftentimes you have to collaborate in order to solve these kinds of things.

From this quote, it appears that networking is necessary "because most of these types of crimes [of cyberterrorism] cross jurisdictional boundaries." This statement is consistent with the observation made by Sadler (2005) that, since 2001, local agencies such as small-town police departments do not have the same mandates for investigating computer crime cases as a federal agency such as the FBI would. In fact, Mansfield

(2000) comments that the FBI is allowed to investigate any Internet Service Provider in order to observe and read email, as well as monitor other online communications. As far as state agencies, they need a prosecutor's certification, such as a mandate (Dekker, 2002), in order to investigate any case of cyberterrorism (Berkman & Shumway, 2003). What it all boils down to saying is that, a local or state agency might not be able to perform a counter-cyberterrorism operation based on the fact that there are some jurisdictional barriers. Consequently, it takes networks to fight networks. As our participant says, "oftentimes you have to collaborate in order to solve these kinds of things." The next quote was selected from an interview conducted with a police officer in the Southwest.

> It's necessary to work with cyber forensics labs. What I've found is that the more people are involved, the better collaboration you have. It's like teamwork. Instead of working home on an investigation, if I've got three or four people, it usually comes out better because they have different specialties and skills they can bring to the investigation. You're gonna get a better work product if you have a team doing it.

While the previous participant highlights the importance for networks between agencies at all levels to rely heavily on multi-jurisdictional collaboration, this participant, a local police officer, stresses the need to collaborate with experts in cyber forensics because "they have different specialties and skills they can bring to the investigation." Cyber forensics experts are computer experts who have superior technical skills. For this reason, says our police officer, "it's necessary to work with cyber forensics labs." According to Thilmany (2004), cyber forensics labs improve investigation into an ever-

growing era of crimes that uses computers, computer-aided terrorism, cyberterrorism, espionage, bank and business fraud, and identity theft. Teamwork makes dream work (i.e., "the more people are involved, the better collaboration you have" and "you're gonna get a better work product if you have a team doing it"). The next excerpt, taken from an interview conducted with the commander of an investigation division in a Midwestern state (who also supervises computer crime experts), supports the statements made in the previous quote when he says that,

> it's necessary to network because there are so many kinds of computer systems; you've got servers. You only have three people in our department and they will not have expertise in all domains of cyber forensics. You have to specialize in certain areas, to do things that other people don't do. It's nice to reach out to somebody else who doesn't have the expertise in that field.

"It's necessary to network," says our division commander, and "there are so many kinds of computer systems." To illustrate that this statement is true, it is worth mentioning that cyber forensics is not a term that can be applied broadly because there are several types of computer forensics expertise. Generally, cyber forensics applies to the retrieving and analyzing of evidence from computer systems, including small bits of computer hardware and electronic data online (Delio, 2005; Holsapple, 2005; Roberts, 2005; Smith, 2000). A parallel definition of cyber forensics is that it refers to the identification, examination, and rebuilding of evidence extracted from any element of computer systems, computer networks, computer media, and computer peripherals that enable forensics analysts to solve a computer-related crime (Hosmer et al., 2000). Although cyber forensics experts usually have solid knowledge in a wide range of

computer/networking hardware, software, and operating systems, there are other types of cyber forensics experts who only specialize in areas that others would have no knowledge about. For instance, there are only a handful of cyber forensics experts worldwide who specialize in analyzing attacks waged against computers via cell phones (McCullough, 2004). Although this might be trivial or inconsequential, cell phones have the power to download malicious data as much as certain computers do. For this reason, the participant says that "it's nice to reach out to somebody else who doesn't have the expertise in that field."

Rist and Chee (2004) state that it is necessary for law enforcement, in their tracking down of cyberterrorists or recovery of seized and frozen data, to consult with cyber forensics labs in order to maximize the outcomes of their investigations. Part of this necessity to network lies in the fact that, as Bhaskar (2006) notes, knowledge of cyber forensics within the law enforcement community is still limited. For Hesalroad (2001), cyberterrorism investigation is a fairly new area in law enforcement. Our participant shares similar views ("You only have three people in our department and they will not have expertise in all domains of cyber forensics"). The network of computer security experts and other important agents is enabled by cyber forensics experts involved in team projects that start at the level of local police departments. These projects include immediate incident responses, and high-rate security analysis tools (Rist & Chee, 2004). Because cyber forensics experts have the required knowledge, skills, and expertise to resist cyber attacks, most cyberterrorist attempts have not been successful (Dunnigan, 2003). The next excerpt was taken from an account told by an ex-CIA agent whose last position was head of an overseas operation. As he states,

there are some dangers to networking with other agencies because you're exposing a system. So, isolationism is good in the sense that nobody knows what you're doing. But, on the other hand, you don't know what anyone else is doing. So, networking is a necessity.

To begin with, the participant expresses concerns about networking with others ("There are some dangers to networking with other agencies because you're exposing a system"). In fact, Goldsborough (2006) notes that, because of the advent of the Internet and networks, collaboration among agencies is not always safe as it exposes computers to various security threats. To corroborate his statement about the dangers to networking, the participant mentions isolationism ("isolationism is good in the sense that nobody knows what you're doing"). Isolationism is a type of foreign policy based on the principle that political leaders should not entangle alliances with other nations. Thomas Paine is generally credited with instilling the idea of avoiding the creation of alliances (Liell, 2003). Isolationism also implies that legal barriers should be imposed to avoid trade and cultural exchange with people in other nations (Nordlinger, 1995). In the context of this study, what this could mean is that American federal agencies should not exchange their software programs with other agencies across the world or share their anti-cyberterrorist tactics with them.

However, as our participant states, when agencies do not network with others, they do not know what anyone else is doing ("on the other hand, you don't know what anyone else is doing"). From this perspective, isolationism can also be criticized for being an "ostrich policy," where people hide from danger by burying their heads in the sand (Kandell, 1995). In other words, agencies cannot conduct an ostrich policy because

the endurance of networks and, above all, their increased intercollaboration are vital for their success against cyberterrorism. For this reason, as our participant expresses it, "networking is a necessity." The next excerpt, from an assistant professor at a Midwestern university, includes several attention-grabbing statements that strengthen this study:

> I think that no man is an island. I'm nothing without the network. I can sit in front of my computer all day long. What would I gain? I can sit in front of the TV and learn, but my interaction would be limited to what I'm being fed through the Internet. If I have no feedback mechanism, communication is useless. Communication is based on feedback. I can sit and talk all day to the wall. For example, we're building a database currently, which comprises of over 500 high-tech agencies dealing with computers. Me, sitting in my office, analyzing over 500 agencies? Impossible. I couldn't do it. I don't have enough money and I don't have the time.

Let us start with the first statement: "I think that no man is an island." These words come from a quote by English poet John Donne, who wrote that "no man is an island; every man is a piece of the continent" (cited in Nutt, 1999). The idea is that people cannot be isolated from one another, but should be interconnected. As the participant continues, "I'm nothing without the network." For this reason, networking is important, otherwise, as the participant indicates, there is nothing to gain ("What would I gain?"). It is also impossible to solve all network-related problems by oneself ("Me, sitting in my office, analyzing over 500 agencies? Impossible. I couldn't do it. I don't have enough money and I don't have the time").

Another important concept in this excerpt is that of feedback mechanism ("If I have no feedback mechanism, communication is useless"). It is an accepted principle that one of the crucial elements needed for effective communication is feedback (Mory, 2003). Feedback is the foundation of all communication (Franklin, Powell, & Emami-Naeini, 2005). The participant's assumptions are consistent with the fact that positive outcomes in the fight against cyberterrorists can only be achieved, not by working alone, but by being involved in a social network that relies on a feedback mechanism. As a result, developing a feedback mechanism is a crucial function of the communication process. According to Wiener (1961), feedback mechanism is circular mechanism. It is a mechanism that is organized by receptors that either initiate or inhibit a reaction. Feedback mechanisms are necessary to maintain stable conditions and achieve a dynamic equilibrium in a network (McFarland, 1971). When there is a continuous feedback mechanism, there is an ongoing flow of communication between humans, and as the network seeks to increase its performance, feedback helps the network make essential adjustments.

As one can see, our participant encourages feedback mechanisms. Because "no man is an island," it is worth collaborating with others. Can one person analyze five hundred companies by him- or herself? The participant says he could not ("Impossible. I couldn't do it. I don't have enough money and I don't have the time"). As Mory (2003) notes, collective problem-solving is required to assess progress, correct errors, and improve performance. By the same token, adjustments can be made on a continuous basis when he or she makes mistakes. An honest feedback mechanism can accurately tell what the problem is. Intergroup network feedback can be given in the form of

recommendations or through a process whereby questions and needs can be heard, analyzed, and ultimately acted upon (Franklin, Powell, & Emami-Naeini, 2005). Therefore, a continuous communication loop between cyber forensics experts and/or law enforcement agents is necessary. Not only does it help reinforce the existence of a community of practice among them, but it also helps weigh up their direction and areas for improvement.

Champagne (2002) remarks that networks can break down if they lack the feedback mechanisms that would allow them to control their growth and achieve a dynamic equilibrium with their environment. When the participant says, "I can sit in front of my computer all day long," it implies that no feedback would be possible because there are no humans involved. When the cyber forensics expert, locked to him- or herself through the junctions of screen, mouse, and keyboard, interacts alone, that individual becomes his or her own sender and receiver, providing feedback to him- or herself in an ongoing internal process. What would the expert gain? Nothing. As the participant expresses it, "What would I gain? I can sit in front of the TV and learn, but my interaction would be limited to what I'm being fed through the Internet." Some of the excerpts mentioned in the previous sub-section also highlight, indirectly, the importance of feedback mechanism. Collaborating with federal agencies from other countries form a basis for future collaboration by sharing information and providing a feedback mechanism for information shared.

Cyber Forensics Experts and Law Enforcement Agents: Networks of Trust

This sub-section drives on the analysis of some of the participants' answers to the following question: "Are those networks formal or informal? Explain." Trust is at the

core of relationships between humans. The boundaries of trust are often personal, and, thus, decentralization is the nature of trust because each individual will have a unique trusting relationship with another individual (Fukuyama, 1996). The sense of what it means to trust someone can also be applied in the realm of counter-cyberterrorism. As expressed in six different interview excerpts, trust depends on "who is proven in the field," "whom we should have faith in," and "who knows whom" in the network. Defeating cyberterrorism is a priority that drives not only military action to subdue individual terrorists and deter their state supporters, but also multilateral cooperation in law enforcement and intelligence sharing. The first quote comes from an interview conducted with a forensics examiner in the Southwest:

> That's more of a matter of whom you know because the FBI, Secret Service, or the NSA won't work with you if they don't trust you. You have to be proven in the field, you have to know each other. It's a network of trust. You're not out to just network with any forensics program. There are some in the state that we specifically won't work with because we don't trust them. But, generally, agencies like the FBI and local departments will collaborate with each other without any reservations.

Based on the first statement, in order to be part of the network of federal agencies, one should have earned their trust beforehand ("the FBI, Secret Service, or the NSA won't work with you if they don't trust you"). The result is that "it's a network of trust. You're not out to just network with any forensics program." In fact, as the participant continues, "there are some [forensics programs] in the state that we specifically won't work with because we don't trust them." Therefore, just as it is the case for cyberterrorist

networks, this practice of using someone whom we know to gain more people in the network is called chaining (Madorsky, Elman, & Kennedy-Moore, 2003). From a social network theory standpoint, chaining involves following connections from one node to the next. So, in this context too, chaining is used in order to recruit the "right" people in the network (as the participant says, "That's more of a matter of whom you know"). By introducing someone "whom you know," it is implied that the third person who is trusted will be honest and have good intentions.

The last statement, "generally, agencies like the FBI and local departments will collaborate with each other without any reservations," is interesting. "Without any reservations" implies that some agencies trust one another and do not have doubts that prevent them from accepting to work together without conducting some sort of background check. McNamara (2003) notes that the collaboration between computer crime units of the Federal Bureau of Investigation, the Secret Service, the NSA and other state and local agencies shows that law enforcement agencies trust one another and recognize the significance of networking with each other. As McNamara (2003) continues, with the rapid proliferation of cyber attacks, the FBI has created trust networks like the National Infrastructure Protection Center in order to provide safety measures to governments and industries.

In a similar fashion, the FBI has created networks of trust such as Computer Crime Squads across the nation, and the National Infrastructure Protection Center in Washington. They also have Computer Analysis and Response Teams to do computer forensics investigations on magnetic media. Those networks of trust make certain that cyberterrorist cases are investigated by the proper parties (Prosise & Mandia, 2001).

Additionally, analysts like Diamond et al. (2003) say foreign governments have increased cooperation with U.S. law enforcement authorities primarily because they trust these authorities. This is exactly what the participant means when he says that "you have to be proven in the field" for people to trust you. They recognize that their people and infrastructures have become targets of cyberterrorists. All these examples show that some agencies "will collaborate with each other without any reservations." Note, however, that one of the points made in the analysis of **RQ4** is that the FBI and the CIA, though being two immense U.S. federal agencies, still oppose each other on different mission goals and tend not to trust one another (Riebling, 2002). The following excerpt, selected from an interview conducted with an IT Security Analyst in the Southwest, also emphasizes the importance of trust in networks between law enforcement agents:

> Most of it is a matter of whom you know because you can't get in a lot of these places without already knowing somebody there. Security officers go to presentations on cyber security; they go to agencies and conferences and give presentations. After your presentations, people hear your ideas and your theories. They might agree or disagree, but you get the idea of whoever talked. That's where a lot of the trust is built and that's how networks form.

This excerpt resembles the previous one for two main reasons. First, in order to get *entrée* to those networks, one must already have a foot in the door by knowing someone who can let that person in ("Most of it is a matter of whom you know"). As the participant continues, "you can't get in a lot of these places without already knowing somebody there." Consequently, it can be deduced that trust is built from chaining. Chaining refers to a chain of connections that start with a trustworthy node. This node,

then, contacts another node that will make nodes connect with each other. The ultimate goal is to create a network of trust. The principle is the same as that of cyberterrorist networks. Plus, this notion of trust resembles that of the community of practice because both concepts involve relationships between inviduals.

Another similarity between this excerpt and the previous one lies in the idea that, in order to be seen as trustworthy, one has to be established in the domain. While the previous participant said, "You have to be proven in the field," this participant argues that security officers will go to agencies and conferences to "hear your ideas and your theories." So, one has to be seen and considered credible. In doing so, the participant continues, "you get the idea of whoever talked. That's where a lot of the trust is built and that's how networks form." From a social network perspective, this tactic of creating networks of trust follows a Peer-to-Peer (P2P) model. The P2P model is a model where users can see where trustworthy information arrives from and which peers are at the source of this information (Oram, 2001). When the personal views (what the participant calls "ideas" and "theories") are collected and evaluated, they can be used as guidelines for recommending the information to other sources, hence creating personalized webs of trust (Moore & Hebeler, 2001). The next excerpt, selected from an account told by the chair of a cyber forensics program in a department of computer and information technology of a Midwestern university, where he is also an associate professor, describes networks of trust through the transitive trust model:

> We rely on technology for the networking. I only know 50% of the people I network with face-to-face. Our community is still a virtual community. It's a transitive trust model. I know Jim face-to-face and if Jim told me that this person

is OK, then my trust in this person is to the extent that I have a good relationship with Jim. So, the trust becomes a transitive trust model.

As this chair of a cyber forensics program expresses it, because the cyber forensics community "is still a virtual community," trust is done through "a transitive trust model." The transitive trust model is a model whereby trust is transitive, that is, transmitted through another party. As shown in Figure 6, based on the main tenets of social network theory, node A validates and trusts node B; node B validates and trusts node C; node A trusts but does not need to validate node C. For example, node A trusts node C, but does not engage in checking anything related to node C. As a result, for A to trust C, A needs to trust B that he or she [B] has validated C by the same standards that A validates B (Hermann, Issarny, & Shiu, 2005).

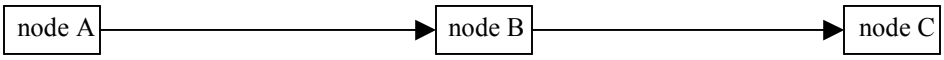

Figure 6 *The transitive trust model is a model where node A validates and trusts node B; node B validates and trusts node C. Yet, node A trusts but does not need to validate node C.*

So, a transitive trust model portrays trust as being a two-relationship model between three nodes. Indeed, node B has two relationships; one with node A and one with node C. From this, it is implied that node A automatically trusts node C due to the extent that node A trusts node B. As the participant explains it, "I know Jim face-to-face and if Jim told me that this person is OK, then my trust in this person is to the extent that I have a good relationship with Jim." This pattern resembles the chain network coined by

Bavelas (1950) and Leavitt (1951), where information moves in a sequential manner through a series of nodes. The use of trust in both the chain network and the transitive trust model requires the existence of a common purpose (Jøsang, Gray, & Kinateder, 2003), which needs somehow to be derived from or given by a specific transitive chain. This has either to be modeled from relevant evidence or, one way or another, the trusting nodes must be enabled to derive it from past experiences. The advantage of the transitive trust model is that it enables the connection of different nodes while reducing the credential validation (i.e., background check) effort (Demaio, 2001). The following interview excerpt, from an assistant professor at a Midwestern university, adds interesting points about the importance of trust in networks:

> In my world (the world of cell phone forensics), the network is composed of a small group. Worldwide, it's less than 50. For example, the Secret Service only has one. The FBI has a couple. In computer forensics, it's the same; you know the names of those who are trusted. You earn that trust of the node through their experiences, their abilities. You learn by watching others' actions; this is how the network forms.

The excerpt does not discuss a chain network or the transitive trust model. The point that the participant is making is that the world of cell phone forensics, a branch of study that is part of cyber forensics overall, is so small that "you learn by watching others' actions; this is how the network forms." Trust, here, comes from the benefit of having increased frequency of communication and more intimate connections between cell phone forensics experts (i.e., "the network is composed of a small group;" "worldwide, it's less than 50"). In fact, the network is so small that "the Secret Service

only has one. The FBI has a couple." So, how can trust be created in these circumstances? According to the participant, "you earn that trust of the node through their experiences, their abilities." In developing strong ties this way, as Larson (1992) puts it, nodes in the network learn about one another, become more dependent on each other, and develop relational trust ("you know the names of those who are trusted"). The next excerpt, selected from a former CIA agent, stresses the importance of having formal networks:

> I like formal networks better because you know whom you're dealing with, somebody you trust. I'd rather deal with the German Minister of Defense than some shady German informant. I have a lot more faith in the official guys. They're not going to try to screw you because they know you're gonna come back and say, "What did you do that for?" Going through an informal network, say, working with a little hacker, can save you a problem, but give you a couple of more besides.

Based on this former CIA agent's statements, in a formal social network, an actor will be less tempted to cheat another because "you know whom you're dealing with." In other words, in a formal network, nodes will know of one another's actions. In fact, Thornburgh et al (2005) observe that one of the formal rules in social networks is that law enforcement agents are supposed to check another's behavior. For this reason, the participant believes, "I'd rather deal with the German Minister of Defense than some shady German informant." It would be very difficult to do a background check on a shady German informant. Mutual observable behavior between each actor in the network provides more security to the network itself (Roson, 2001). That monitored behavior in

question must be consistent with the exchanged information between those actors. Hence, the participant has "more faith in the official guys." Because of such mutual monitoring of behavior, our participant continues, "they're not going to try to screw you because they know you're gonna come back and say, 'What did you do that for?'"

Such behavior control is exerted through repeated interaction, leading to dyadic expectations of reciprocity between each actor (both of whom are strongly connected). Rutten (2004) remarks that being part of a formal network is judicious because the actors can share information in a way that establishes conjoint trust regarding the protection of the actors themselves (i.e. through a secure link). Our participant opposes informal networks ("Going through an informal network, say, working with a little hacker, can save you a problem, but give you a couple of more besides"). From this viewpoint, a formal network provides more security [to the network] because dyadic reciprocity reinforces mutual expectations which, in turn, yield to trust. Trust and security are almost synonyms here. The last excerpt, selected from an FBI agent, contrasts with the previous one in that this excerpt underscores networks of trust that are informal:

> The network is fairly informal and it's based on mutual trust. It's not like somebody in the administration and the FBI says, "You will work with the University." Over a period of time, law enforcement agents and experts in cyber forensics have had so much interaction that there has been a level of trust. We do not have informants; we depend only on assets that we can control. The danger is when you don't know the other party well. That's why mutual trust is very important. For this reason, you need to know the background and the level of integrity.

A network of counter-cyberterrorism officials, involving FBI agents and cyber forensics experts, "is fairly informal and it's based on mutual trust." The network is created through repeated interaction over a period of time ("law enforcement agents and experts in cyber forensics have had so much interaction that there has been a level of trust"). According to the participant, trust depends on nodes that can be monitored ("we do not have informants; we depend only on assets that we can control"). Because it is difficult to know who the node is, mutual trust is very necessary ("when you don't know the other party well. That's why mutual trust is very important."). This is a throwback to Coleman (1988) when he contends that mutual trust through strong interconnections guides or controls actions in a network and fosters cooperative behavior. This type of trust model also leads to more commitment. Therefore, norms of cooperation are quickly established because network actors that have faith in the idea that strong ties lead to better collective monitoring and sanctioning create an effective incentive for mutual trust (Coleman, 1988). This, in turn, facilitates the spreading of norms across the network. Consequently, a higher number of actors established in highly interconnected, dense networks develop shared behavioral expectations (Meyer & Rowan, 1977; Oliver, 1991; Rowley, 1997).

The difference between this view and the transitive trust model lies in the fact that the latter does not involve verifying the background or level of integrity of a node. Put another way, node A does not engage in authentification and verification of node C because node A trusts node B. This is how the transitive trust model works. However, our participant here suggests that mutual trust be supported by knowing the background and level of integrity of anybody in the network. As he says, "you need to know the

background and the level of integrity." The subsequent part of this analysis describes the downsides to networking with others.

Downsides to Networking

This section is an analysis of the data based on the participants' answers to the following question: "Describe the downsides to networking with other agencies." Although federal agencies have developed networks among each other for the past couple of years, it appears that not all networks can be trustworthy or dependable for keeping information secret. Three interview excerpts were selected in this sub-section to demonstrate that there are downsides to networking. The first of these excerpts, from an interview conducted with a visiting faculty at a Midwestern university, who is also a computer crime specialist with the National White Collar Crime Center, stresses that there is leaking of important data to the press:

> People working in law enforcement want to put cyberterrorists in jail; people working in academia also want to put them in jail. That is one of the reasons why we create all these social networks against cyber attackers. Yet, you also have a certain level of distrust between some agencies and other agencies, based on past experience. If I share this information with agency X, Y, or Z, they leak it to the press while my investigation is going on. As soon as I leak it to another agency, I lose control of that information. I've done all this work for the past six months, and agency A, B, or C is going to take it away from me and get all the credit for it.

The first few statements of this excerpt are worth mentioning because they explain why social networks are created against cyber attackers. The reason those social

networks exist lies in the fact that "people working in law enforcement want to put cyberterrorists in jail," in the same way that "people working in academia also want to put them in jail." Yet, the participant continues, "you also have a certain level of distrust between some agencies and other agencies." The source of distrust can be blamed on one single node, which takes a connection path other than the one officially blessed by the network. One leak to the press and secret information is made public. As the participant describes it, "if I share this information with agency X, Y, or Z, they leak it to the press while my investigation is going on." The result is a loss of information on the part of the National White Collar Crime Center ("As soon as I leak it to another agency, I lose control of that information"). The distrust with nodes in the network is even amplified as the node that gets all the credit for doing all the counter-cyberterrorist network is another agency ("I've done all this work for the past six months, and agency A, B, or C is going to take it away from me and get all the credit for it"). The next excerpt, selected from a participant who does strategic relations and communications with different cyber crime agencies in a Midwestern state, also emphasizes the downside to networking with other agencies:

> I trust the people that I know in the network but not their friends, because I don't know how far that chain goes. I don't know how many nodes belong to the network. I can go to a guy who is brilliant in the area of cyber forensics (and I trust him) and ask him, "What do you think of this?" But there are still some dangers of networking with others even with those whom we trust. There can always be a bad actor. That is human nature. Every time you network with others, you expose yourself to risks and to somebody else with power over you.

The first important point of this excerpt is that no one knows how many nodes belong to a network ("I don't know how many nodes belong to the network"). As a result, our participant thinks one cannot know "how far that chain goes." Thornburgh et al. (2005) argue that one of the formal rules in social networks is that law enforcement agents are supposed to do a background check on every node in the network. Yet, their social networks consist of nodes across the nation and across the globe. As a result, it is not always possible to know every node. Besides, agents sometimes network with informants who are not official members of networks of agents and cyber forensics experts. As the participant explains it, "I can go to a guy who is brilliant in the area of cyber forensics (and I trust him) and ask him, 'What do you think of this?'" Because the FBI does not have enough top-notch computer experts to recruit for cyber forensics, they will tend to rely on freelance cyber experts (Thornburgh et al., 2005). The downside to this type of networking is that "there can always be a bad actor." The participant goes further when she says that every time we network with others, we expose ourselves to risks and to others with power over us. The last excerpt of this sub-section, from an assistant professor at a Midwestern university, points to the problem of ethical hacking as part of the practice of social networks:

> One of the phenomena in our networks is that technical people have vigilantism; they really want to try to clean this up. In that fervor to do good, the temptation to do bad is huge. I think that ethical hacking is a huge challenge nowadays. Ethical hackers are hired to penetrate your sites, your network, your system to expose your vulnerabilities. They violate laws and try to cut corners in order to reach outcomes. It is never appropriate to break a law while investigating a problem. In

> our state, we have computer-trespassing and computer-tampering laws, which we often quote to our technical communities. If you change without permission, that's tampering.

The participant condemns the practice of ethical hacking as it represents a challenge nowadays. Britt (2005) explains that ethical hacking is a type of authorized network intrusion where the intruder employs the same tools and techniques as a cyberterrorist would. Ethical hackers are paid to hack into your network in order to check if everything is alright. Yet, as opposed to cyberterrorists, ethical hackers would neither damage the target systems nor steal information (Fadia, 2005). As the participant expresses it, "they are hired to penetrate your sites, your network, your system to expose your vulnerabilities." The problem, says the same participant, is that it is a law-breaking practice ("They violate laws and try to cut corners in order to reach outcomes. It is never appropriate to break a law while investigating a problem"). Referring to the comments made about the previous excerpt, we could interpret that an ethical hacker represents a potential node that cannot be trusted in the network. First and foremost, they are not completely trustworthy. The reason, says Palmer (2001), is that ethical hackers may discover information about an organization that should have been kept secret. In many cases, this information, if publicized, could enable real cyberterrorists to break into the systems, possibly leading to significant damage.

Another problem related to ethical hacking is that, during a paid intrusion, the ethical hacker usually holds the keys to the organization, and therefore can hurt the system with just a few keystrokes (Palmer, 2001). It is very difficult to hold absolute trust in such a node in the network because they could exercise total control over any

information about a target. That control, of course, could easily be misused. Although there is a contract between the client and the ethical hacker (Simpson, 2005), it has been known that wicked humans violate pacts and treaties for their own benefits. In fact, Swartz (2003) notes that ethical hackers often sneak in through Internet access points. All in all, although this study reveals that there are many benefits to networking with other agencies or groups in their fight against cyberterrorism, there are also downsides to networking with particular nodes. The following sub-section focuses on informal networks, calling attention to the strength of weak ties.

Informal Networks: The Strength of Weak Ties

This sub-section derives from the data obtained from the participants who answered the following question: "Are those networks formal or informal? Explain." It discusses Granovetter's (1973) theory of the strength of weak ties in informal networks of law enforcement agencies. The basic tenet of Granovetter's theory is that a weak tie represents a bridge (Granovetter, 1973) between nodes in a social network. Weak ties lead to more flexibility. Two excerpts were selected from the participants' interviews to illustrate that having weak ties presents benefits. The main benefit is the extreme facility of information flow, that is, the ample diffusion of information among actors in the network. The first of these excerpts was taken from an account told by a professor of communication at a Midwestern university who has worked with the FBI:

> You like to ask about social networks a lot. You know, in my experience, many of the ties we have developed with computer crime analysts working for the FBI have become strong. And that's when the network becomes formal because, over time, we end up having a set of definite rules and habits for conducting our

investigations. But we also have weak ties with other computer crime analysts too. That way, it's more informal, you're freer to exchange information, and things get more flexible, you can cut corners, you get more opportunities.

Based on these statements, it is obvious that formal networks with strong ties make collaboration between law enforcement officials possible ("many of the ties we have developed with computer crime analysts working for the FBI have become strong"). The advantage of a formal network is that rules and practices are fixed, settled, and clear-cut ("that's when the network becomes formal because, over time, we end up having a set of definite rules and habits for conducting our investigations"). Yet, many scholars argue that using networks with strong ties can trap the highly connected nodes into one particular area of knowledge and lock them out of external opportunities (Cohen & Levinthal, 1990; Leonard-Barton, 1995; Poppo & Zenger, 1998; Young-Ybarra & Wiersema, 1999). Nodes connected through strong formal ties may be reluctant to pursuing better opportunities.

However, our participant explains that he and his team also use weak ties because, "that way, it's more informal." As he continues, "we also have weak ties with other computer crime analysts too." Granovetter (1973) contends that informal networks contribute to greater mobility and autonomy. This is where the importance of his theory of the strength of weak ties comes into play. Having weak ties is advantageous. The main advantage is the flexibility of information flow between the nodes ("you're freer to exchange information, and things get more flexible"). By having an informal network with weak ties, law enforcement agents do not become isolated from receiving new information from outside circles. Rather, they can act as bridges between different

agencies. They see themselves in situations where they receive information that they can share with any actor they want (Granovetter, 1982; Haythornthwaite, 2000). The second excerpt was taken from an interview conducted with a computer crime analyst working for a local police department:

> Not all our networks are formal. Sometimes, we work with informants. When we go for informants, at that point, they're working with us and that's how we get the bigger fish. Most of the time, if they're working with us, they have hacked, they have a track record. So, we kind of direct them in a way that we need to go in the investigation. So, if they are willing to work with us, they can play the part.

The first six words are clear: "Not all our networks are formal." "Sometimes," the police officer continues, "we work with informants." By definition, an informant is a person who supplies information to law enforcement agencies (Eichenwald, 2001). Having ties with informants can be beneficial for law enforcement agents in that they can flexibly communicate and cooperate with them, as they might possess specialized knowledge and capabilities. What it also comes down to saying is that informal networks are valuable when law enforcement agents use them as conduits to unfamiliar nodes that own novel and potentially unique information. As the participant says, "they're working with us and that's how we get the bigger fish." What weak ties do is locate or embed nodes [informants] in distant regions of the social network. Likewise, weak ties can make law enforcement investigations improve as agents are freer to use informants the way they want. As the participant explains it, "we kind of direct them in a way that we need to go in the investigation."

Adler and Kwon (2002), Greif (1997), and Uzzi (1996) argue that formal networks are not good for using informants. Plus, constant interaction with the same actors in the network limits the network's exposure to new ideas and information. It also weakens the diversity of knowledge available in the social network, thus diminishing its value (Dussauge, Garrette, & Mitchell, 2000; Hamel, 1991; Nakamura, Shaver, & Yeung, 1996). The next sub-section also analyzes informal networks, but, this time, it stresses the importance of structural holes.

Informal Networks: Structural Holes

This sub-section builds directly on the previous section. In the previous section, Granovetter's theory of the strength of weak ties highlighted weak ties through the description of their meaningful roles for the diffusion of information within social networks of law enforcement agents. As part of the analysis of **RQ2**, this sub-section shows that Granovetter's theory also provides the groundwork from which important emerging perspectives on informal networks can be made. One of these perspectives is Burt's (1992) structural holes theory. Burt's ideas stem directly from Granovetter's theory in that, for Burt, individuals with whom a person has weak ties are less likely to be connected to one another. In other words, the person is embedded in a structural hole. The first excerpt, selected from an account told by the chair of a cyber forensics program in a department of computer and information technology of a Midwestern university, where he is also an associate professor, mentions those structural holes:

> The majority of what gets done on a daily basis probably gets done on the informal level. At the formal level, you have a compressed time frame for law enforcement investigations. What ends up happening is that investigators will use

informal networks because they are faster and allows people to be in structural holes.

Note the criticism of formal networks again ("At the formal level, you have a compressed time frame for law enforcement investigations"). By having an informal network, by having a grasp on who knows whom and who knows what, law enforcement agents can easily manage their networks because it is assumed that they provide or feed relationships that they see fit. Indeed, for the participant, informal networks "are faster." What ends up happening is that the investigators find themselves to be in "structural holes." The participant does not explain it further. For Burt (1993), when actors in a network are kept discrete, a succession of holes in the network starts to develop, to such a point that an important actor can become the bridge between different actors. This is what is called "structural holes" (Burt, 1993). Burt (1992) argues that being embedded in a structural hole allows actors to be more efficient in obtaining information. This is where Burt meticulously revisits Granovetter's ideas. For Burt, the benefits of the strength of weak ties are increased for a gatekeeper, or what Granovetter (1973) refers to as a "local bridge," connected to different groups that have no other bridging connection.

More importantly, the structural hole is a knot in the social network that gives access to missing knowledge. Therefore, an individual who is the only one linking a group to another is at a significant advantage. Not only does the individual gain from having access to a different set of information that is unavailable in a dense network of strong ties, but, also, he or she has the power to control what aspects of this information can be shared with the different groups to which they belong (Burt, 1992). This is very

important for communication among network actors because the less dense and formal the networks are, the more structural holes emerge and develop in those networks. By the same token, what those actors do is taking advantage of *le vide* (literally, *emptiness*; conceptually, structural holes) (Stewart, 1996), considered as necessary in network-based relationships. The second excerpt takes a different angle on the matter:

> With respect to Internet regulation, we have a private safety network, maintained by Verizon, and a public safety network, which is actually owned and maintained by us. The two never really directly mesh. They're not directly interconnected. We use a key player, like a router, for the communication between the two.

From this excerpt, the key player ("like a router") finds him- or herself in a structural hole because the private safety network and the public safety network "never really directly mesh." As a result, the key player is a link "for the communication between the two." So, the key player is in a structural hole in the social network because it acts as a bridge between the "private safety network, maintained by Verizon, and a public safety network." It empowers that network by enabling important actors to get indirectly interconnected. Here, the two networks are forms of sub-networks being part of a gigantic network for Internet regulation against cyber attacks. Managing the flow of information to a great extent is vital for communication between network actors because these actors need to acquire as much information as possible in order to maximize profits and benefits of all kinds. For this reason, by acting as a local bridge between these actors, the key player strengthens his or her abilities to gain and control information. The next sub-section describes the hubs in their networks. Analyzing their hubs is important because hubs are nodes in a social network that have many connections with other nodes.

Hubs in Their Networks

This is the last sub-section in the analysis of **RQ2**. The data selected here are answers to the two following questions: "Describe the role of nodes and hubs [minor and important actors] in your networks" and "Describe the degree of centrality in your networks." An analysis of the role of hubs in social networks of law enforcement agencies is provided, based on social network theory. Particularly examined are hubs as humans with high degrees of centrality. As a reminder, hubs are nodes in a social network that are so important that they connect a great number of other nodes. The outcome of this analysis is that any type of network is much stronger when its hubs are active. The first excerpt was selected from the captain of a Midwestern County Sheriff's Department. This captain also oversees IT operations for that Sheriff's Department, as well as the 911 systems of the county and its public safety network:

> We have key players at different agencies that we can call who can provide a certain level of assistance. They can remotely connect. So, we do share files; they can give us access; we can give them access, or we can each deny mutual access to each other.

A vast majority of nodes are connected to a social network by way of just one link: fewer have two, even fewer have three, and so down the line (Barabasi, 2002). However, some nodes become hubs because they are very important through their higher visibility or the amount of help they can provide (Johnson, 2000; Keller, 2005). Here, in this excerpt, the hubs are key players. As the captain describes it, "we have key players at different agencies that we can call who can provide a certain level of assistance." The role of hubs considerably influences how the network operates. The excerpt above

portrays the hub as a human, more precisely as a person who has an effect on the other actors in the network through his or her assistance and location ("They can remotely connect"). The next excerpt, from the same participant, highlights the role of specialists who are important actors in the network:

> There are various investigators with each agency who have a skills set that allows them to research cyber threats, whether they are terrorist-related or larceny-related or some sort of theft-related. Aside from that, there are specialists that I know are very good in cyber forensics technology, in terms of recovering data, and also investigating network issues.

These hubs act as key actors, that is, people with the highest skills. As the captain explains it, "there are various investigators with each agency who have a skills set that allows them to research cyber threats." As he continues, "there are specialists that I know are very good in cyber forensics technology, in terms of recovering data, and also investigating network issues." By pointing to their being "very good in cyber forensics technology," they must be special nodes in the network and, hence, hubs. Removing these hubs might pose a problem. This shows the importance of being a hub. This is crucial for law enforcement agents because hubs can provide the network the ability to understand and fight cyberterrorism in the most effective way. This does not mean that relationships through these particular hubs are the shortest and the most efficient, but this means that those hubs have the skills and knowledge necessary to counter cyber attacks. They can provide special assistance when it comes to "recovering data, and also investigating network issues." The subsequent excerpt emphasizes the role of hubs as humans with high degrees of centrality in social networks:

> I do strategic relations and communications. Basically, I am the interface between this agency and other folks across campus here in terms of putting together teams or proposals or to see how they can work together and do research with other colleges, break through still pipes. I am also the interface between state government and some federal agencies, as well as between local agencies and corporations. So, I am the front facing people.

Based on the statements made in this excerpt, the participant seems to be a hub where she acts as "the interface" between different agencies. As she describes it, she is "the interface between state government and some federal agencies, as well as between local agencies and corporations." And she does "strategic relations and communications." In this case, she is a hub with a high degree of centrality. She has many connections with different actors in the network. Given this, she is the giver/receiver of information. She also impacts the flow of information and activity (Arquilla & Ronfeldt, 2001). This degree of centrality calls to mind that the network has a number of direct connections to a human who acts as a router node (Lott & Taylor, 2005). Wigand (1997) argues that central individuals in a network enable quick communication with the nodes connected to them. This is a beneficial method for improving the network because what makes communication among nodes easier in the network is the presence of a human hub.

In line with these contentions, it can also be inferred that the participant acts as a go-between, that is, a mediator or a link between multiple actors (Pearson & Hobbs, 2004). A hub has a similar meaning: it is a place of convergence that links multiple actors (Greenie, 2005). For this person who does strategic relations and communications, a go-between is someone who is at the interface between multiple agencies. Barabasi (2002)

maintains that the use of a go-between implies that the nodes in the network are not necessarily connected to one another. As she expresses it, she breaks "through still pipes." Any node, however, can be connected to the go-between. By adopting this method, each node can obtain superior information due to the go-between's privileged position through his or her high degree of centrality. Let us have a look at the last excerpt, selected from an account told by a forensics examiner:

> We work with law enforcement directly. We have direct physical network contact with them; we work with the law enforcement on a personal level. In a lot of ways, it's better when I work with actual investigators in the agency. Now, my directors, they work with chiefs of police at different states and different areas. Once they've got their relationships set up, and agree on whatever services, then they bring their investigators and I actually talk to the investigators.

What this excerpt is telling us is that, in order for the forensics examiner to work and talk with the investigators from the law enforcement agency, he has to obtain the agreement from his directors ("my directors") that the investigators be allowed to work with him (once they "agree on whatever services"). This shows that collaboration between key actors in the network has to go through go-betweens, that is, the directors. The go-betweens are the directors because they are the middlepersons. A comparison can be made with the previous excerpt where the middleperson occupies a structural position where she is the interface between different agencies. Here, the middleperson [director] links unconnected actors (Fernandez & Gould, 1994). In this context, the director stands between the investigators and the forensics examiners. Again, Granovetter (1973) would call it a "local bridge." As a local bridge, he or she performs the role of a gatekeeper,

whether it is between nodes that are already parts of a cyberterrorist network or nodes that are not yet part of the network, but that might be potential members. Fernandez and Gould (1994) maintain that brokerage involves the very notion that the broker finds himself or herself in a position where he or she is tied to nodes that are not necessarily connected in the network.

Now that we have an in-depth understanding of what social networks of both cyberterrorists and cyber forensics experts (and law enforcement officials) are, let us move on to the next step of this study: the analysis of **RQ3**. This analysis looks at how networks function against and *vis-à-vis* other networks, that is, how the two sides conflict and interact with each other, based to a little extent on social network theory and to a great extent on game theory.

Chapter VI

Analysis of Research Question 3

Except for the first two interview questions (that is, "What is cyberterrorism?" and "What are the motivations to engage in cyberterrorism?"), all the interview questions in **RQ1** and **RQ2** pertain to social network theory. The main goal was to understand how both cyberterrorists and cyber security experts (and law enforcement officials) create networks. The questions were both broad and technical (about nodes, hubs, degrees of centrality, etc.). The analysis of **RQ3** is not an analysis of networks *per se*. Rather, this section looks at how networks of cyber security experts (and law enforcement officials) operate against and *vis-à-vis* networks of cyberterrorists, that is, how the two sides conflict and interact with each other, based slightly on social network theory and mostly on game theory. The reason game theory is very much emphasized in this section lies in the fact that game theory is well applied in direct interactional and conflicting situations that involve two players (Fent, Feichtinger, & Tragler, 2002), as it is the case in this study.

In order to analyze **RQ3** (How can the conflict and interaction between cyberterrorists and computer security experts [and law enforcement officials] be explained through the use of social network theory and game theory?), both theories are used. The arrangement of this interpretation is structured in three different parts. Each is independent from one another. The first part is exclusively a social network theory approach; the second part is exclusively a game theory approach; and the third part is an intersection of the two approaches. The following questions were asked in each interview: (1) Describe a direct interaction or conflict between cyberterrorist networks

and cyber forensics experts' (and law enforcement agents') networks?; (2) How can a network knock down another network? (3) What game or strategy do cyberterrorists use?; (4) What game or strategy do cyber security experts and law enforcement officials use?; (5) Could you give me an example of a collaborative game strategy between the two sides?; (6) Could you give me an example of a non-collaborative game strategy between the two sides?; and (7) Do cyberterrorists make the rules of the game or do they go along? These questions do not include probing questions that were asked during each interview because, for each participant, the interviews progressed differently. Let us begin by analyzing the participants' perspectives, from a social network theory approach, of the conflict and interaction between cyberterrorists and computer security experts (and law enforcement officials).

Part I: A Social Network Theory Approach

Although the heading of this sub-section is "Part I: A Social Network Theory Approach," it does not analyze social networks *per se*. This was the purpose of the analysis of the two previous research questions (**RQ_1** and **RQ_2**). Instead, this sub-section specifically analyzes the conflict and interaction between cyberterrorists and computer security experts (and law enforcement officials). The data were driven by the two following questions: "Describe a direct interaction or conflict between cyberterrorist networks and cyber forensics experts' (and law enforcement agents') networks?" and "How can a network knock down another network?" The data are very consistent with the scholarly literature on the matter. The first excerpt was selected from an interview conducted with a local police officer in the Midwest:

> Sometimes our agents will go online and act as scouts. What they'll do is interact with cyberterrorists for a while. They're trying to get more information on them. They know they're dealing with a whole network of those guys because they recognize them by their nicknames. But the agents don't know for sure if the people behind those nicknames are the real cyberterrorists. They have to abide by the law. So, they won't investigate their computers unless they have a warrant. And the cyberterrorists will do the same; they'll interact with our agents to get more information on our network infrastructure, but that doesn't mean they will cooperate with them.

From a social network theory viewpoint, this excerpt, in essence, describes the interaction of a network with another network. Overall, it appears that law enforcement agents do not always engage in battle with cyberterrorists. They will try to interact with them in order to obtain more information about their networks (and vice versa). For this reason, our participant says that the "agents will go online and act as scouts," in the same way that cyberterrorists will interact with them ("they'll interact with our agents"). Nevertheless, the last statement clearly distinguishes interaction from cooperation ("that doesn't mean they will cooperate with them"). The word "interact" in this context can be interpreted as "interface" or "having some type of communication" online. As far as the nature of interaction, unfortunately, it is not made clear in this excerpt. Diani and McAdam (2003) argue that interface between networks can increase knowledge about each other's network. Interface here does not mean collaboration in itself. Rather, the more interactive the network, the more open the network, and the more open the network, the more chances to obtain new information and ideas about the enemy than closed

networks that have no interaction whatsoever. In other words, nodes that only interact within their network already share the same knowledge; the network, in this case, is not bound to make progress (Kalathil & Boas, 2003).

For this reason, law enforcement agents interact with their enemies (and vice versa) in order to know them better. A whole theme entitled "Know Thy Enemy" is analyzed in the next chapter (the analysis of the themes for **RQ_4**). However, the danger of interacting with the enemy is exposing one's network to the enemy. In fact, Bannister (2005) notes that, because of the advent of the Internet, interaction with another network of actors can be risky because it exposes the nature of the network such as the size of the network, the frequency of online use of the different actors, the depth of communication between the actors in the network, their specific type of language (including the number of keystrokes per minute, the accent, and the spelling mistakes), and other various components. The next excerpt, from an account told by a law enforcement officer in the Southwest, focuses more on how networks of cyberterrorists clash with networks of law enforcement agents:

> Those networks [of cyberterrorists], they always go after our soft spots, you know, like a weak link in our chain. If that soft spot is inside a critical infrastructure like ours, the other networks and systems that are connected to it could be severely compromised. What's gonna happen is a ripple effect. Law enforcement would have trouble taking actions, their communications systems would go down, basically we could be vulnerable. So, what do we do to prevent that? We try to dirupt their networks first.

Here, there is no interaction involved. Instead, it is conflict between two networks. Our participant makes it clear that the goal of each network is to disrupt the network: "Those networks [of cyberterrorists], they always go after our soft spots, you know, like a weak link in our chain" and "what do we do to prevent that? We try to dirupt their networks first." The motivations seem to be different on each side. On the one hand, the cyberterrorists seem to be trying to cripple the networks of law enforcement for the sake of crippling them. On the other hand, law enforcement agents disrupt cyberterrorists networks in order to prevent them from waging cyber attacks. From this excerpt, it follows that the fight between the two opposing networks seems to be offensive on the cyberterrorist side and preemptive on the law enforcement side.

What this excerpt is also telling us is that cyberterrorists are trying to find the hubs of their enemies' networks ("If that soft spot is inside a critical infrastructure like ours, the other networks and systems that are connected to it could be severely compromised"). A critical infrastructure like "theirs" (what the participant refers to as "ours") is certainly a hub because nodes are attached to it ("the other networks and systems that are connected to it"). The consequence, the participant continues, would be a "ripple effect." Based on the main tenets of social network theory, a ripple effect is a gradually spreading effect of one node on the other nodes (Johnson & Levin, 2002). If that node is an important node, and if it gets damaged, the other nodes connected to it will be damaged as well. If it were to happen to a critical infrastructure such as a law enforcement agency, the results would be devastating. As our participant explains it, "law enforcement would have trouble taking actions, their communications systems would go down, basically we could be vulnerable." A "ripple effect" is the same as a "cascading

failure," a detailed analysis of which is given in the next chapter on the themes (**RQ4**). The theme under which "cascading failures" fall is called "Postmodern State of Chaos." The next excerpt, from a chief information security officer at a Midwestern university, also emphasizes the networks that cyberterrorists are trying to target:

> If the cyberterrorists are trying to attack a community, and we have a documented case of it, or if they were trying to take down the city of Los Angeles, for instance, they probably are going to do it in little bits and pieces. They're gonna be testing the police department's network, they're gonna test the state government's network.

This excerpt illustrates networks against networks again. The network of cyberterrorists is attacking the law enforcement network "in little bits and pieces." This time, it is not a large hub that is targeted at once, but smaller hubs after smaller hubs ("the police department's network" and "the state government's network"). They would follow this method, for instance, "if they were trying to take down the city of Los Angeles." These views expressed by the chief information security officer are slightly different than other descriptions of what cyberterrorists are trying to achieve. Other participants said that it takes large hubs down to cripple a network. Faloutsos, Faloutsos, and Faloutsos (1999) and Matlis (2002) corroborate this too. Nevertheless, in the case presented by the participant above, the impact would still be devastating because a network like the police department's network is a hub in itself, and people's lives depend on it. Imagine the fear of having no police available. Now that we have seen examples of what a network of cyberterrorists could do to a network of law enforcement agents, let us analyze what the

latter could do to their opponents. The next excerpt was taken from an account told by a professor of social networks at a Midwestern university:

> You need to cripple the network of cyberterrorists before they attack. In order to disable their network, what you need to do is to disable its go-betweens, like in any other network, these cyberterrorists that mediate contact between a number of localized networks; they contact multiple groups because it makes things easier for the network.

Just as cyberterrorists try to target the hubs of their enemies' networks, so do law enforcement agents; they attempt to cripple the big actors in cyberterrorists' networks. Who are these big actors? They are the go-betweens ("to disable its go-betweens"). What do these go-betweens do? They "mediate contact between a number of localized networks; they contact multiple groups because it makes things easier for the network." After all, as Pearson and Hobbs (2004) put it, a go-between is a mediator who acts as a link between multiple actors ("they contact multiple groups because it makes things easier for the network"). So, law enforcement would strike the node that links unconnected actors (Fernandez & Gould, 1994), that is, the middleperson or, as Granovetter (1973) would call it, a "local bridge." As a reminder, a local bridge is a gatekeeper. Go-betweens, then, are very crucial to the interconnectedness of the cyberterrorist network. Getting rid of these go-betweens would be as destructive to their network as destroying the gas reserve of the German infantry in WWII. In line with these contentions, as the point was made in a previous excerpt, this participant stresses that the fight between the two opposing networks seems to be offensive on the cyberterrorist side and preemptive on the law enforcement side ("You need to cripple the network of

cyberterrorists before they attack"). The following excerpt, taken from an interview conducted with an IT Security Analyst II, underscores that the IRC server is a hub for cyberterrorists that law enforcement is trying to knock down:

> From a law enforcement perspective, you generally want to go for an IRC server. The first thing to do is to find out where that server is. You knock out the hubs. You have to knock out the heads off and hope that everything falls by the wayside. It's time-consuming to go after the smaller ones. Go after the servers that are the commanding control channels.

So, according to our participant, the hub that law enforcement agents try to target is a communication channel like an IRC server. He even gives us the steps to follow ("The first thing to do is to find out where that server is. You knock out the hubs"). If we "knock out the heads off," he continues, everything will fall "by the wayside." The reason to do this is that "it's time-consuming to go after the smaller ones." Here, the statements reinforce the idea that small nodes are only drops in the ocean. The "heads" in this excerpt are not go-betweens, but important channels like IRC servers. A cyberterrorist network is a typical example of a scale-free network; it will not be destroyed if the small nodes are removed and the large nodes are still there. A network like that can cope with about 80% of random node failures (Faloutsos, Faloutsos, & Faloutsos, 1999; Matlis, 2002). Only when the hubs are wiped out will the network stop working (Matlis, 2002). This is exactly what our participant says ("Go after the servers that are the commanding control channels"). The last excerpt, from another forensics examiner, follows a similar train of thought:

> The chat room is another place to get cyberterrorist networks. Like any kind of undercover action or like a drug undercover investigation in order to infiltrate a ring, the same thing happens on the Internet because anybody can go into these chat rooms and IRC. You can basically be anybody you want. It's a good place for law enforcement agents to gain intelligence and get information.

Like an IRC server, a chat room is considered a hub by law enforcement agents as they try to target it ("The chat room is another place to get cyberterrorist networks"). Now, "to get cyberterrorist networks" is a little vague, but the point here is that, whether or not the intent is to get rid of the chat room, it is obviously an important objective for law enforcement agents. Interaction between the networks of the two opposing sides is more subtle. Our participant suggests that agents "infiltrate a ring" by going "into these chat rooms and IRC." The situation in this excerpt is about networks going after networks. The incentive is that "it's a good place for law enforcement agents to gain intelligence and get information." Of equal importance is that, in those virtual channels, "you can basically be anybody you want." A similarity can be found with the first excerpt of this sub-section. The participant of that section said that law enforcement agents interact with their enemies (and vice versa) in order to know them better; our forensics examiner here also points to the agents' opportunity for infiltration so that they can "gain intelligence and get information." The procedure seems to be the same: to approach the enemy (and, by the same token, to know them), to get them, and to destabilize their network.

So far, the analysis of the interaction and conflict between cyberterrorists and law enforcement agents has been driven by social network theory. Now, let us analyze the same issue based on game theory.

Part II: A Game Theory Approach

This section includes the highest number of excerpts in this study. The goal is to illustrate the importance of game theory in the understanding of the complexity of the interaction and conflict between cyberterrorists and cyber forensics experts (and law enforcement officials). The data analyzed in this section are driven by the participants' answers to the following interview questions: "What game or strategy do cyberterrorists use?" "What game or strategy do cyber security experts and law enforcement officials use?" "Could you give me an example of a collaborative game strategy between the two sides?" "Could you give me an example of a non-collaborative game strategy between the two sides?" and "Do cyberterrorists make the rules of the game or do they go along?" The data are very consistent with the basic tenets of game theory.

Before getting into the analysis *proper*, let us reexamine in one paragraph what game theory is. Game theory studies the relationships between individuals, using models with clear statements of consequences (i.e., payoffs) that depend on the actions taken by those individuals (Aumann & Hart, 1992; Fudenberg & Tirole, 1991; von Neumann & Morgenstern, 1944). Game theory also studies how those very individuals behave when they are placed in situations that require them to interact with each other. This theory is about power and control. It deals with two-person decision-making situations (with opposing or joined interests). One important tenet of game theory is that each person "must first know the decision of the other agents before knowing which decision is best

for himself or herself" (Jehle & Reny, 2001, p. 267). As such, each person is a player in the game, as well as a decision maker, choosing how he or she acts. Because each player wants the best possible consequence or outcome to his or her preference, every decision made by each player will have an impact – whether positive or negative – on the outcome of the game. Put another way, each outcome is the result of particular moves made by the players at a given point in the game (Rapoport, 1974). The outcome can be a Nash equilibrium, a zero-sum game, a positive-sum game, or a negative-sum game (see literature review). The players have also the choice to engage in collaborative games or non-collaborative games.

The essential characteristic of game theory is the notion that players are rational and intelligent in strategic reasoning. Consequently, they look for the maximization of the difference between their own costs and benefits when considering an action they want to take. The first excerpt, taken from an interview conducted with a visiting faculty at a Midwestern university, who is also a computer crime specialist with the National White Collar Crime Center, illustrates those aspects of rationality and intelligence in strategic reasoning:

> Cyberterrorists' victory is based on law enforcement's defeat. I'll give you an example. Some of the really smart cyberterrorists have figured out that law enforcement agents use special software tools to examine hard drives and pull evidence off. They know what these products are and they try to find ways to disrupt these products. For example, if law enforcement agents run into a compressed file, very often they want to open up that file to see what was in it. While some hackers insert pornographic files in these compressed files, other

> clever cyberterrorists can set the compressed file as a logic bomb. What happens is that when the law enforcement software decompresses it, that file crashes the officer's computer. They have to start all over. Sometimes, they may not even realize what's causing that crash, except that when they open the compressed file, it goes to a certain process where to crashes their computer again.

The very first statement, "Cyberterrorists' victory is based on law enforcement's defeat," is a very good example of a zero-sum game (von Neumann & Morgenstern, 1944). It was described in the literature review that a zero-sum game is a game where, no matter what the outcome of the game is, the victory of one player is exactly balanced by the defeat of the other player. In other words, each of the payoffs must be the negative of the other (Fudenberg & Tirole, 1991). "Zero-sum" occurs when a player adds up his or her total gains and subtracts the total losses of the other; they will sum to zero. So, in this conflict between cyberterrorists and law enforcement agents, the cyberterrorist will win only at the expenses of the law enforcement agent, but the benefits and losses to both players amount to the same value. For this reason, it is a zero-sum game.

As far as the strategies, game theory postulates that strategies are available to each player. On the one hand, a strategy used by law enforcement, based on the excerpt above, is to create special software tools "to examine hard drives and pull evidence off." On the other hand, a strategy used by cyberterrorists is "to find ways to disrupt these products." So, this is the first step of a chess game going on here. The next action of the cyberterrorists is to insert a logic bomb in a compressed file that they think law enforcement will open up. The action of the law enforcement agent, according to our participant, is to open up that file. In this situation, the payoff of the cyberterrorists is to

see the agent's computer crashed ("when the law enforcement software decompresses it, that file crashes the officer's computer"). Payoffs are the "gains" that each player receives as a consequence of each possible outcome. The payoffs of the cyberterrorists are balanced by a loss of their opponents. Game theory also postulates that every possible strategy pursued by each player leads to a defined end-state. As we have seen, the end-state, or outcome, here, is a zero-sum game. The next excerpt, selected from an account told by an ex-CIA agent, explains how law enforcement agents, this time, win against cyberterrorists:

> If the target is a law enforcement agent that is a real computer user storing everything he or she has, as some people do, the reward for the cyberterrorist could be very high because the agent's life is on their machine. It could be the equivalent of taking their entire filing cabinet and carrying it off. At least, potentially, the rewards of a computer attack could be very high. That's both the good news and the bad news because if you download a lot of gigabytes and data, you have to go through it, which means that the task for the cyberterrorist can be very difficult. And if it's tons of garbage and pictures of the agent's family, and all these kinds of things, you may find it's very hard to process it. There are some risks of downloading data, especially if the files have viruses on them. The agent might do that on purpose. That's what can happen to the cyberterrorist if they don't know what they're after. In that case, they'd lose.

Here, we have an excerpt explaining two opposing situations. On the one hand, the cyberterrorist's victory would be diametrically opposed to the law enforcement agent's loss. If the cyberterrorist steals what the agent has on his or her computer (which

can be his or her entire life, that is, "the equivalent of taking their entire filing cabinet and carrying it off"), the cyberterrorist would win and the agent would lose something vital ("the rewards of a computer attack could be very high"). The outcome, again, would be a zero-sum game because the victory of the cyberterrorist is exactly balanced by the defeat of the agent.

However, the opposite can also happen ("That's both the good news and the bad news"), that is, there could be a situation where, this time, it is the cyberterrorist who loses against the law enforcement agent. First, as the participant explains it, "if you download a lot of gigabytes and data, you have to go through it, which means that the task for the cyberterrorist can be very difficult." We saw earlier that every decision made by each player has an impact on the outcome of the game. Yet, if the decision taken by the cyberterrorist hurts him- or herself, the opponent already has an advantage in the game. As the participant continues, "there are some risks of downloading data, especially if the files have viruses on them. The agent might do that on purpose." The basic assumption here is that the law enforcement agent follows specific objectives and takes into account both the skills and expectations of the other player (the cyberterrorist). This is what the participant means when he says that "the agent might do that on purpose." If the cyberterrorist does not know that what he or she is downloading is actually a set of files that are intentionally stuffed with viruses, they would lose the game ("if they don't know what they're after. In that case, they'd lose"). The end-result, or outcome, would be a zero-sum game in this situation because, in this battle between the cyberterrorist and the law enforcement agent, the latter would win at the expenses of the former.

What these two examples demonstrate is that the dangerous game played by cyberterrorists and law enforcement agents is a strategies-versus-counterstrategies game, like a chess game, where the players who prevail are those who possess the structural advantage. One might think that to disrupt is structurally less difficult than to protect, but as the second scenario tells us, the agent can create a situation where the cyberterrorist's defeat equals that of a scorpion killing itself with its sting. In other words, the cyberterrorist uses his or her usual tactics (stealing and downloading files) that eventually hurt him or her (those files were intentionally replete with viruses). The next excerpt, taken from an interview conducted with the computer crime specialist with the National White Collar Crime Center mentioned earlier, does not exemplify a zero-sum game, but a Nash equilibrium:

> In some situations, all of those guys [cyberterrorists and law enforcement agents] use their own strategies and don't change them. One such example occurs in the Internet chat room. The law enforcement agent pretends to be a safe Web user or a certain target-type victim online. A good portion of the cyberterrorists is wise to that. They do things like asking the same questions three times over a four-hour period to see if they get the same answer. If they get the same answer every time within a four-hour period, that's a cue to them that there are talking to a real person. However, if they ask the same question to a fake user and if they get different answers, which happens sometimes because two hours later the person does not remember that that question was asked and they don't remember what that answer was, the cyberterrorists will be probing for undercover law enforcement that way. Of course, law enforcement agents are wise to people

doing that. So, they keep a log of questions that have been asked and answers that have been given. In fact, they anticipate the common questions and they will actually write down a list of important elements, such as "these are my preferences, these are the groups I like, these are the groups I don't like," and so forth.

This situation suggests a Nash equilibrium as the outcome of the interaction between cyberterrorists and law enforcement agents in the chat room for several reasons. First, one of the tenets of the Nash equilibrium is that each player takes his or her opponent's current strategies as given (Nash, 1950). As such, a player has nothing to gain by changing only his or her own strategy. If a player has selected a tactic and if he or she cannot benefit by changing that tactic, while the other player keeps his or hers unchanged as well, then the current set of tactics and the payoffs that result from the outcome of the game constitute a Nash equilibrium (Fudenberg & Tirole, 1991). The participant clearly expresses these assumptions in the first statements he uses: "In some situations, all of those guys [cyberterrorists and law enforcement agents] use their own strategies and don't change them." To be more precise, the participant gives us a clear example. Many cyberterrorists know that "the law enforcement agent pretends to be a safe Web user or a certain target-type victim online." Because of this, the tactic that cyberterrorists usually use is "asking the same questions three times over a four-hour period to see if they get the same answer" from the Web user. However, if they get different answers from the same Web user, "the cyberterrorists will be probing for undercover law enforcement that way." So, there is no reason for cyberterrorists to change their strategies.

What gives the Nash equilibrium all its legitimacy in this excerpt is that law enforcement agents use counter-strategies ("they keep a log of questions that have been asked and answers that have been given") and use the same strategies over and over again. As the participant argues, "they anticipate the common questions." For this reason, "they will actually write down a list of important elements, such as 'these are my preferences, these are the groups I like, these are the groups I don't like,' and so forth." In the Nash equilibrium, both players perform their dominant strategies. None of the two players changes his or her strategy when they are offered the chance to do so at the end of the game. So, each player takes the actions of his or her opponent as given (Mehlmann, 2000). The end-result, or the outcome, is an equilibrium of strategies between the two players. In other words, it is a Nash equilibrium. Both cyberterrorists and law enforcement agents can maximize their outcomes that way. There is no reason to change their strategies in that type of situation. The next excerpt, taken from an interview conducted with a senior analyst engineer in forensics who has an IT group and who supports the police of a Midwestern university, does not exemplify any type of outcome but focuses on the postmodern aspect of game theory in cyberspace:

> Our friends at Iowa State had a break-in last week. Here's the quote from the chief information security officer from Iowa State: "Analysis of both computers indicated the intruders were not looking for personal data, but for space to distribute pirated movies." Well, that's what they believe. The problem here is if I were an intruder looking for personal data, I would masquerade as someone distributing pirated movies. The people at Iowa State are missing the point. These cyberterrorists know that they might accidentally be found out. When they're

found out, they want to have a cover story. So, load up your kit, put some fake movies in it. When cyber forensics experts do their analysis, they'll hit the pirated movies. It's incredibly naïve on the part of the players. And you're talking about a chief information security officer.

As it was mentioned earlier, game theory studies how players behave when they are placed in situations that require them to interact with one another. Game theory, as it appears, is about power and control. A cyber forensics expert who notices something unusual in the network will suspect that an attack has occurred and that action must be taken on that very moment. This implies that the players are in the same context: one player wants to attack a computer system, while the other wants to protect it. The context involves short-term strategies on the part of both players. However, in the excerpt above, the participant makes the point that the cyber forensics experts at Iowa State got deceived by cyberterrorists who masqueraded themselves as intruders "distributing pirated movies." Because of the postmodern nature of the Internet, and because of the absence of spatiality, the Web user can make any moves that would not be possible in actual physical space. When interacting with anything in cyberspace, cyberterrorists find themselves in situations that are aperspectival (Gebser, 1985). If "they want to have a cover story," they can do it however they want.

That is the postmodern aspect of game theory in cyberspace. As opposed to conventional war techniques, game theory in cyberspace allows for the use of grand strategies aiming at fast and easy deception of the respective opponent. The Internet allows players to change their moves more quickly and more frequently than in actual physical space (Carmel & Frequently, 1996). For this reason, our participant says "the

people at Iowa State are missing the point." It would not be fair to say that the outcome is a zero-sum game where the cyberterrorists' victory is contingent upon the law enforcement's defeat, because deception is not the same as defeat. The case here is a situation where the "good" side is being misled by the "bad" side. From what it appears, there is no damage or financial loss involved. Yet, there is a big deal of deception. Deception is part of game theory. Our participant extends this view in the excerpt below:

> The other aspect is that we don't understand our enemy. They can pretend to be just distributing pirated movies. They [the people at Iowa State] will believe that and they will stop their investigation. I got a gamble going on over here and I'm keeping you busy, while I'm really taking your data in the back while you're not looking. It's like a chess game. It's exactly game theory and they're good at it. They're the bad ones; they don't have to be fair. That's not part of the deal.

One of the goals of the players in game theory is to make sure that one player does not understand the other. The problem, our participant argues, seems to be on the cyber forensics/law enforcement side ("we don't understand our enemy"). What he means is that the cyber forensics/law enforcement side at Iowa State will stop at a certain end-state in the game, that is, when they see pirated movies downloaded on their files and when they stop the investigation at that point ("They [the people at Iowa State] will believe that and they will stop their investigation"). Yet, the participant says that they do not seem to understand that cyberterrorists are playing a chess game ("It's like a chess game"). Moreover, the participant continues, "it's exactly game theory and they're good at it." Again, this is a situation where the cyberterrorists know their true strength, but the targeted sources cannot estimate the true cyberterrorist actions behind the intrusion

attempts. The next excerpt, from our same participant, corroborates the assumptions made so far:

> Cyberterrorists are culturally very savvy. They know what the current script kiddies are doing. Sometimes, the talented guys, while bashing the script kiddies, use them as their cover, because if law enforcement agents look at a script kiddie, then they instantly assume that it's some copycat, but the agents don't realize that the true danger has been masked by this copycat. So, cyberterrorists are clever.

The problem here is the same. Law enforcement agents will stop investigating when they come across what they think is a script kiddie. "Script kiddie" is a pejorative term for inexperienced hackers who use programs developed by others, without knowing what these programs are or how they work (Tanaka, 2001). The intent is to compromise computer accounts and files (Verton, 2001a). Our cyberterrorists seem to play a cunning game ("while bashing the script kiddies, [they] use them as their cover") where they capitalize on their enemies' ignorance ("if law enforcement agents look at a script kiddie, then they instantly assume that it's some copycat"). According to Rapoport (1974), an expert on game theory, the player seeks to follow the best strategy that will help him or her accomplish the most beneficial goal in every situation. The strategy here is deception of law enforcement and, based on our participant's comments, it seems to work. For this reason, our participant says that "cyberterrorists are clever."

The following five excerpts depict the conflict between cyberterrorists and law enforcement agents (and cyber forensics experts) as an evolutionary game. The first of those excerpts was taken from an interview conducted with an IT Security Analyst II in the Southwest:

> Technologies are only a means to an end. It has never changed throughout the course of human history and there has always been some type of conflict. Cyberterrorists find new ways in order to exploit someone's vulnerabilities. Technology only makes that attack vector easier. When we find a new way to protect something, they [cyberterrorists] always find a new way to exploit it. There are always continuous patches and changes in technology. We are developing technology so quickly that security is sometimes not built into it. So, there are always going to be holes that people can take advantage of. I see that being a continuous struggle. It's going to get worse before it gets better.

To begin with, the third sentence of this excerpt is interesting. Based on the participant's statement that "cyberterrorists find new ways in order to exploit someone's vulnerabilities," the goal of the cyberterrorists is to create tactics and weapons that continually change in an effort to defeat their opponents' networks and systems. Besides, "when we find a new way to protect something, they [cyberterrorists] always find a new way to exploit it." From this vantage point, it does not seem that, in this dangerous game, any of the players loses. On the part of the cyberterrorists, there is no re-machining. If the cyberterrorists lose today, they will not disappear. Rather, they will learn what did not work and use it against their enemies tomorrow. The reason is that "there are always continuous patches and changes in technology." On the part of the cyber forensics experts and law enforcement agents, they will choose the option for the highest expected payoff by having the latest technological measures to protect their networks. Yet, in turn, cyberterrorists also select the option for the highest expected payoff for their digital attacks; as such, they manage to find out the probability of their opponents' failure on

their computer networks. It is an evolutionary game because it is based on situations where the players know their own strengths, but they can only estimate their opponents' power (as well as their resources and capabilities) based on the level of their moves (that is, their actions, tactics, and attacks or defensive measures). For this reason, our participant sees it as a "continuous struggle."

Based on the excerpt above, if cyber security is a game then cyberterrorists are the ones who make the rules. Indeed, protective measures like anti-virus software programs and firewalls are measures taken by cyber forensics experts and law enforcement as a reaction to cyberterrorists attacks. When the latter ones launch a new computer virus, the target side has to adapt to it. When the cyberterrorists manage to find a hole in the new adapted technology that has just been used against the virus, the target side has to adapt again. This evolutionary game seems to be a ping-pong match where the target has to play by the cyberterrorists' rules. Moreover, their very rules may change during the game, based on new cyber weapons, new tactics, new tools, all of which can be acquired a few mouse clicks away. Any cyber forensics or law enforcement agent who is unable to handle that is at a critical disadvantage. The last statement of this excerpt, "it's going to get worse before it gets better," can be opened to a solid interpretation. The cyberterrorists may be able to design programs that will get a computer network in trouble. Yet, the target can learn from his or her defeats and mistakes. The idea of losing the game against the cyberterrorists is not always a bad idea; computer security agents can learn from mistakes. This is where game theory perfectly fits (Littman, 1994). Yet, this game never ends; rather, it is continuously evolving. The next excerpt is from the same participant:

> The Internet allows the possibility for no ending in this conflict. Because of this, there is increased motivation to do anything to exploit it. Cyberterrorists will always find a way. Essentially, they are finding new methods every day. It's a moving target because the cyberterrorists' methods are always gonna be changing. They're gonna become more sophisticated.

Just as it is the case in the previous excerpt, the conflict between cyberterrorists and their opponents is an evolutionary game because new methods are constantly invented (i.e., "Cyberterrorists will always find a way. Essentially, they are finding new methods every day"). Also interesting are the first few statements ("The Internet allows the possibility for no ending in this conflict. Because of this, there is increased motivation to do anything to exploit it"). The postmodern nature of the Internet is such that the players in cyberspace are under no space or time control constraints (Carmel & Markovtich, 1996). Therefore, there is the possibility for no end of anything, not even the end of cyberwar ("no ending in this conflict"). Because timing for move and state updates is not fixed in cyberspace, it is no surprise that "the cyberterrorists' methods are always gonna be changing." For example, as we have seen in the literature review, not only can a player make multiple moves at the same time, but, also, both players can make multiple simultaneous moves as well. While in most conventional games players alternate moves, in cyberspace this is not true anymore. An opponent can launch multiple simultaneous attacks easily and quickly (Littman, 1994). For this reason, the participant argues that cyberterrorists will become "more sophisticated." The next excerpt was taken from an interview conducted with a chief information security officer at a Midwestern university:

> With cyberterrorists, you always have to think ahead. I'm trying to work within a construct of a game or a set of rules. Remember 9/11; we were not thinking about planes crashing into buildings. We were thinking of car bombs, an Oklahoma City bombing kind of thing. So, now, instead of looking at the hundred-year flood, consider it. It's not absurd now. The rules of the game keep changing.

Because "the rules of the game keep changing," it seems that anything is possible. As the participant explains it, nobody had really thought about planes crashing into buildings. On September 11, 2001, the rules of terrorism had changed. Would cyberterrorists be capable to flood an entire city by opening up a dam through its computer system? Well, the participant would say, "consider it. It's not absurd now." In most games, the rules are known by all players beforehand. These rules govern each player's behavior and, assumedly, each player has full knowledge of the rules. In the situation of cyberterrorism, however, "the rules of the game keep changing." Anything evolves. As a result, changing the rules leads to an outcome that would have been different had one or all players followed them. They are inventing new rules as they play the game. Or it might even be the case that the rules have changed by themselves, to the point of leading Web users with the sense that there are actually no rules. The rule of the game is that the game has no rules. After all, as Lyotard (1984) puts it, postmodernism means working without rules. So, in the postmodern multidimensional cyberspace, anything goes with anything, like a game with no rules. The next excerpt was taken from an interview conducted with a visiting faculty at a Midwestern university, where he is also a computer crime specialist with the National White Collar Crime Center:

> Anything that you can do to try to identify the cyberterrorist can be done by them to identify you. Most of them know not to use a law enforcement information system because it will bite back at them. There is some escalation in that cyberterrorists get wise to law enforcement measures and, in turn, law enforcement agents get wise that cyberterrorists are getting wise to this angle, so they find counter-measures. There is somewhat of an escalation taking place.

The word "escalation" is used twice here and feeds the thought that the game between the two opponents is an evolutionary game. Escalation is a phenomenon whereby a situation evolves step by step (Shukla-Mehta & Albin, 2003). The players do learn from each other as they are fighting on a daily basis. How do they learn from each other? Our participant explains that, while "cyberterrorists get wise to law enforcement measures," "law enforcement agents get wise that cyberterrorists are getting wise to this angle." From this, it follows that one never knows when the game is over. There is no outcome. This is essentially a postmodern fight. The next excerpt comes from the chief information security officer mentioned previously:

> They have to play a chess game in order to accomplish what they want to accomplish. I don't think one knows for sure what the other's gonna do. Professional cyberterrorists will try to stay abreast of defense mechanisms so they can always develop a means of exploiting known vulnerabilities or getting around the defense that's there.

The concept of "chess game" is mentioned here. The game of chess is a reflection of the ongoing events in the battle that takes place between cyberterrorists and law enforcement agents. Just like in a chess game, the computer security agent does not know

the next move of the cyberterrorist, and vice versa ("I don't think one knows for sure what the other's gonna do"). It is fair to assume that both players know what each other is capable of doing. Yet, they do not know what each other's next move will be. For this reason, cyberterrorists try to have the upper-hand against their enemies ("Professional cyberterrorists will try to stay abreast of defense mechanisms so they can always develop a means of exploiting known vulnerabilities"). To complete this short excerpt, law enforcement agents respond when an attack on the computer network is suspected or has actually happened. So, this battle is a chess game, where each player does not know what moves the opponent will take. Therefore, each of the players will find a strategy to examine the possible actions of each other in the situation. The ultimate goal is to determine the best course of action for him- or herself (Jehle & Reny, 2001). No matter what, the game is evolutionary. The next excerpt was selected from an interview conducted with a forensics examiner in the Southwest:

> A lot of it is intelligence. We watch what's going on in the rest of the world. We run what we call "honey pots" and we sniff traffic, trying to see things developing in advance, we try to head it off. We set up firewalls. A lot of it is preemptive, just to try to know what cyberterrorists do on the outside, to keep up with vulnerabilities as we see their new techniques coming out on the honey wall side and from all the security companies. We start patching against it internally so that cyberterrorists cannot use that vulnerability against us. That's the main goal, to stay one step ahead of them.

The phrases "to head it off," "preemptive," and "to stay one step ahead of them" are basic tenets of game theory. Just like a chess game, the cyber conflict is not a game of

chance. It is based exclusively on tactics and strategies. The outcome of the game is not influenced by some randomizing device. For this reason, forensics examiners have to "head it off," "just to try to know what cyberterrorists do on the outside." They go to access control lists to determine what does and does not belong to the network. Forensics examiners also use honey pots ("We run what we call 'honey pots' and we sniff traffic"). A honeypot is a good example of game theory in the world of computers. In essence, it is like a mousetrap that is used to detect or counteract attempts of cyber attacks or intrusions into information systems. Once the intruder or cyberterrorist enters a honeypot, his or her actions are monitored, enabling the forensics examiner to sniff what kind of danger is coming (Hall, 2004). Overall, the honeypot consists of a computer or an entire network site that seems to be part of a network but which is in fact isolated from everything else. It also seems to contain information or resources that look valuable to cyber attackers. So, a honeypot masquerades as something innocuous. Yet, it is not. The result is that the enemies of computer security experts can fall prey to honeypots.

The next few excerpts concentrate on the different collaborative games that law enforcement agents are able to play with their opponents. Game theory helps demonstrate the potential for collaborative behavior among distrustful players in the game. The first of these excerpts comes from an interview conducted with a computer analyst in a local police department:

> We [computer analysts in local police departments] don't engage in collaborative games with cyberterrorists. On a local level, at the grassroots level, we don't do that. At the federal level, the FBI does that. They collaborate with cyberterrorists in order to get what they want. It's important; you got to communicate with them.

> And, you know, if the cyberterrorists know that the FBI has enough resources to force them to surrender eventually, then the most beneficial strategy for the cyberterrorists is to collaborate.

Here, this excerpt mentions two types of game: the non-collaborative game and the collaborative game. According to our participant, computer analysts in local police departments do not play collaborative games with cyberterrorists. As he expresses it, "on a local level, at the grassroots level, we don't do that." Simply defined, a non-collaborative game is a game where each player pursues his or her own interest independently. The players do not have end goals that are compatible. Yet, it might also be the case here that local police officers are not allowed to do that. The participant was not clear on that issue. However, the participant says that "at the federal level, the FBI does that." They do collaborate with cyberterrorists "in order to get what they want." In a collaborative game, players agree to interact without threats and combine their efforts to reach outcomes (Basar & Olsder, 1999). The Federal Bureau of Investigation has a history of collaborating with cyberterrorists. According to Verton (2001), investigators from the FBI develop close relationships with cyberterrorists through the use of Internet chat rooms. Under such conditions, cyberterrorists ask the investigators to participate in coordinated cyber attacks and, eventually, they offer, in exchange for their participation, to share information that was stolen from other computer networks (Verton, 2001). The result is that the players join forces and do fairly well ("If you participate in our cyber attacks, we will give you what you need"). This collaboration between cyberterrorists and FBI agents is to be viewed as a postmodern two-player game. The excerpt above,

however, does not explain what strategies are used by the players and how FBI agents can use the outcomes of the game to improve the security of their network.

Another important consideration in the excerpt is that the participant emphasizes the importance of communication with the opponents ("It's important; you got to communicate with them"). Communication plays a central role in game theory (Buttyán, Hubaux, & Capkun, 2004). The theory involves the analysis of conflict, cooperation, and the degree of communication necessary to arrive at a desired outcome by each player. Game theory also deals with strategic interaction. A strategic interaction requires that the players make decisions; the outcome of the game depends on the choices made by the players. A strategic interaction intrinsically involves human communication. For instance, the cyberterrorist would need to find a way through communication and trust in order to reach a collaborative outcome with the FBI agent. In fact, in a collaborative game, the ability with which each player communicates, the intensity of communication, and even the organization with which these players communicate will have a great impact on the outcome of the game (Osborne, 2003). If there is no communication between the players, then no collaboration is possible. However, if they can communicate and engage in collaborative behavior, the outcome would be quite different. Consequently, repeated interaction might lead to different outcomes.

A final note regarding this excerpt is that it might be the case that cyberterrorists collaborate with law enforcement agents such as the FBI because they have to. As the participant expresses it, "if the cyberterrorists know that the FBI has enough resources to force them to surrender eventually, then the most beneficial strategy for the cyberterrorists is to collaborate." In fact, Mitnick and Simon (2005) note that former

intruders sometimes cooperate with federal agencies because they have no choice. If they do not cooperate, they go to jail. The collaborative game, in this case, is not altruistic; it is not a function of empathy, but an awareness that one is in need. The next excerpt, selected from an interview conducted with a professor of social networks at a Midwestern university, takes a different angle on the collaborative game between those opponents:

> Law enforcement agents play collaborative games with cyberterrorists, but this is a very important ethical issue. I suppose they have some sort of regulations or rules of the game. They play a game, but where do they stop? They pass themselves as somebody like them [cyberterrorists]. The strategies that they use are meant to reach a specific outcome, to hurt you, to deny some things, to take away some things from you. You don't only want the best solution, but you also want to get the darn enemy. Sometimes, you choose an outcome that is not only unethical, but also the only choice that brings you close to what you want to do.

Based on the participant's comments, it appears that the collaborative game that law enforcement agents play with cyberterrorists is a necessary evil. The means do not matter, only the end. As the participant describes it, "you don't only want the best solution, but you also want to get the darn enemy." This is why the participant thinks that engaging in a collaborative game with the enemy is an ethical issue ("you choose an outcome that is not only unethical, but also the only choice that brings you close to what you want to do"). Let us make an analogy with Hitler's Battle of the Bulge, which took place in the Belgian Ardennes (1944-1945) (Parker, 2004). For Hitler, the Battle of the Bulge was the only solution left for the German military because, eventually, it lost a good number of infantry divisions that could have been moved to the East front.

However, Hitler's idea was that he was operating on the premise that he would push the Allies back into the sea (Dupuy, Bongard, & Anderson, 1994). His goal was related to some type of calculations. He needed to win the war, no matter what. The bottom line is that sometimes we engage in actions that do not take the costs and benefits into account any more. As long as we have the slightest chance, we are engaged and we do it. In the context of cyberterrorism, it seems that law enforcement agents would take the slightest chance to collaborate with the enemy in order to reach their outcomes. The next excerpt was taken from an interview conducted with a visiting faculty at a Midwestern university, where he is also a computer crime specialist with the National White Collar Crime Center:

> First of all, try to avoid making this a "black or white" or "either/or" thing. What we have is a whole bunch of human beings that fall in somewhere along the shade of gray, sometimes people change and go to a different shade of gray, maybe a lighter shade of gray. Some cyberterrorists rationalize what they're doing. You have people who defect to the other side to collaborate with them and you have people who pretend to defect. It's very difficult to categorize people as cyberterrorists or the "good guys." You don't always know who's who.

This excerpt is interesting because, as opposed to all the other excerpts in this section, it highlights the possibility of all the players in the game – that is, both cyberterrorists and their opponents – to fall in the same category. As the participant explains it, it is "a whole bunch of human beings that fall in somewhere along the shade of gray, sometimes people change and go to a different shade of gray, maybe a lighter shade of gray." From this vantage point, it appears that there are no clear opponents or

enemies (there is no "'black or white' or 'either/or' thing"). Unlike battles in actual physical space, the warriors in cyberspace are difficult to identify. This is postmodernism, of which one of the main tenets is a shift away from spatialization as we know it in real life. For this reason, the participant says that "it's very difficult to categorize people as cyberterrorists or the 'good guys.'" As he continues, we cannot always "know who's who."

A good analogy of all this can be made with the fuzzy distinction between "white hats" and "black hats." Just as there is no clear line between opponents in cyberspace, there is no clear difference between "white hats" and "black hats" in the computer security realm. A "white hat" is an intruder who is ethically opposed to compromising computer systems and networks for malicious purposes (Thaddeus, 2000). His or her ultimate goal is to improve computer security by "checking" a computer system. A "black hat" is a generic term for a real hacker, a cyber criminal, and a cyberterrorist (Bischoff, 2001). The term "white hat" comes from American western movies where the hero always wears the white cowboy hat, whereas the villain always wears a black hat. As opposed to clear opponents in western movies, there is no clear line between those who improve security (the white hats) and those who destroy it (the black hats). Indeed, the fact that a white hat generally focuses on securing computer systems and networks while a black hat aims at destroying them is a simplification. For instance, the black hat might wish to secure his or her own computer and the white hat might feel the need to intrude the black hat's computer during an investigation. So, although white hats tend to emphasize that they have altruistic motivations, the difference between white hats and black hats is open to interpretation (Beaver & McClure, 2004). Consequently, the

participant's statement that it is "a whole bunch of human beings that fall in somewhere along the shade of gray" is very consistent with what is found in the scholarly literature on the issue. In fact, the literature talks about "gray hats" (Harris et al., 2004).

What adds to the complication is that the collaborative game between cyberterrorists and law enforcement agents seems blurry as well. As the participant confers to us, "you have people who defect to the other side to collaborate with them and you have people who pretend to defect." In game theory, to defect means to select an action which increases one's own payoffs by switching to the other side (Batson & Ahmad, 2001). The problem is that there are players who *pretend* to defect, which means that they leave and come back. Adopting this tactic can be as confusing as changing one's goals completely. In fact, Carmel and Markovitch (1996a) remark that a single opponent may decide to change objectives. The last excerpt of this section, selected from an interview conducted with the chair of a cyber forensics program in a department of computer and information technology at a Midwestern university, discusses the differences between the end-game of hackers and that of cyberterrorists:

> Hackers and cyberterrorists have a different end-game. The end-game of cyberterrorists will tend to be a massive disruption of technologies. They want to take down entire computer systems and let everybody know about it. The hackers that hack into traffic control systems will hit that point where they go, "Ooh, I have broken into that system; now let's go back." The cyberterrorist will say, "Waw, now let's get down some planes." There's a whole different mindset. There is a fine line here. Most hackers and cyber criminals will stop at a certain point, while cyberterrorists will take steps beyond. I don't think they'll ever stop.

This excerpt clearly makes the point that hackers are less malicious than cyberterrorists. This is illustrated through their end-games. The end-game of hackers is not constantly evolving; rather, they will stop at a certain point. As the participant explains it, "The hackers that hack into traffic control systems will hit that point where they go, 'Ooh, I have broken into that system; now let's go back.'" On the other hand, cyberterrorists will take steps beyond, to such a point that the participant thinks they will never stop ("I don't think they'll ever stop"). Evidently, the postmodern evolutionary game that law enforcement agents (as well cyber forensics experts) are involved in is with cyberterrorists, not innocuous hackers (in which case the game would not be evolutionary; it would stop at a certain point). The sixteen excerpts in this section have showed us important aspects of this postmodern battle; it is evolutionary, there are chess games going on, even collaborative games when needed, and the difference between the good and the bad is sometimes blurry. No matter what, our last participant says that the outcome of cyberterrorists is different from that of hackers. Now, let us move on to the third part of this analysis of **RQ3**: the intersection of social network theory and game theory.

Part III: Intersection of Social Network Theory and Game Theory

Game theory provides a good basis to analyze social networks. In this section, four excerpts serve to illustrate how the cooperation of one node in the network – that is, any Web user; whether the Web user is a cyberterrorist or a law enforcement agent, whether the cooperation is conscious or unconscious, and whether being part of the game is intentional or not – can contribute to the success or failure of social network operations. Hence, social network theory and game theory can be intersected. The first

excerpt was selected from an interview conducted with a forensics examiner in the Southwest:

> What cyberterrorists also do is what we call here "ARP poisoning." Basically, it's when they make it look like you're the router, you're like the link between two law enforcement agents. The goal is to deceive them. There's plenty of commercial applications and free applications out there to do it. And all the traffic is re-routed through you or any private-home PC user, which first of all slows down the traffic and, second of all, you control every piece of traffic that goes down through the network.

The participant mentions ARP poisoning as a way to take advantage of a node ["you or any private-home PC user"] in the network by re-routing information through that node. By definition, ARP poisoning is a technique used against a network whereby a cyberterrorist confuses network devices by sending messages via another computer (Semmelroth, 2006). This excerpt shows that ARP poisoning can be employed in a man-in-the-middle attack (Trabelsi, 2005). A man-in-the-middle attack is an attack where the cyberterrorist can control or change traffic between two law enforcement agents without either of them knowing that the link between them has been compromised (Chirillo, 2002). The link between them, that is, the "man-in-the-middle," can be any private home PC user. The cyberterrorist makes sure that all traffic is forwarded through that private home PC user. "The goal," says the participant, "is to deceive them [law enforcement agents]." Game theory here is plugged into the framework of social network theory in that the operation of the network is based on the unconscious cooperation of the private home PC user who is used as a link (man-in-the-middle) between two law enforcement

agents (who are the enemies of the cyberterrorist). Each node [law enforcement agent] forwards traffic to the other through that man-in-the-middle. Yet, the nodes do not know that they are being deceived by the cyberterrorist. There is a complex game going on here. The following excerpt, taken from an interview conducted with an assistant professor at a Midwestern university, depicts a collaborative strategic game:

> When law enforcement collaborates with cyberterrorists, it's often like this: "If you help us, we're gonna help you too, because we know that you do a part in the game, or you are the game and you can bring in the other cockroaches, before they can crawl away." So, on a personal level, law enforcement agents will use methods to make a cyberterrorist more likely to cooperate with their network.

Game theory can be interpreted here as the aim of persuasion, not just to force cyberterrorists to complete the tasks of law enforcement, but also to take advantage of their knowledge in order to increase the success of the networks consisting of law enforcement agents. For this reason, "law enforcement agents will use methods to make a cyberterrorist more likely to cooperate with their network." In this context, the participation of the user [here, the cyberterrorist who gets caught] can have far-reaching consequences because the operation of the network relies on the collaboration of one node [that cyberterrorist in question] complied to turn in other nodes (as the participant puts it, "you can bring in the other cockroaches, before they can crawl away"). So, game theory provides a good theoretical framework to analyze this issue (Orda, Rom, & Shimkin, 1993). The word "complied" was just used here. Compliance of the user is seen in the following statement: "If you help us, we're gonna help you too." Compliance is more probable if the cyberterrorist believes that, by complying, he or she is ingratiating

him- or herself with individuals who may give the cyberterrorist future benefits. Here, it is, in essence, getting in with the enemy. The following excerpt, taken from an account told by a professor and associate department head in a department of computer and information technology at a Midwestern university, also portrays a collaborative strategic game:

> The fact that law enforcement agents collaborate with cyberterrorists in order to catch other cyberterrorists is a standard law enforcement technique. They want the first person they arrest not to prosecute. They want that person just to get at the people behind this. They're really after the big fish. They'll do a plea bargain with the little fish so that they catch the big fish, the entire network. So, they'll let that first person go.

Here, the tactic of the player is to let one node go away in order to catch the whole network of nodes. In the participant's words, law enforcement agents will "do a plea bargain with the little fish so that they catch the big fish, the entire network." A plea bargain is an agreement between a prosecutor [here, law enforcement] and a defendant [here, the cyberterrorist] in exchange for some agreement from the prosecutor (Rosett, 1976). Given this, the cyberterrorist becomes part of the network of law enforcement agents. Plus, the burden of responsibility is not entirely on the cyberterrorist. This is where the cyberterrorist believes that he or she is not solely responsible for the moves against his or her comrades. In social networks, the selfishness of the users has deeper consequences than in traditional networks because the operation of the network can be based on the cooperation of the nodes against other nodes. So, again, game theory offers a solid theoretical framework to analyze this issue (Orda, Rom, & Shimkin, 1993). The

last excerpt of this analysis of **RQ3** was selected from an interview conducted with the head of a cyber forensics program at a Midwestern university:

> When cyberterrorists get caught by the FBI, sometimes the FBI asks them for supporting their network. That's where they might come back to bite the FBI. If cyberterrorists cooperate, it's not altruistic. They cooperate otherwise they're going to jail. They're compelled to do so. There is no intrinsic motivation for them to cooperate. The cyberterrorists' thought process of what we relate to as unethical or ethical is not necessarily what you and I would consider to be. They have ulterior motives because they have an easy time rationalizing and justifying what they do.

This last excerpt points to the danger of networking with one's enemy. Although law enforcement agents see some benefits to "recruiting" cyberterrorists for supporting their network, they run the risk of being betrayed – what the participant refers to as "bitten back." In other words, even if law enforcement creates a credible situation that makes the cyberterrorist feel that he or she is immersed in the network of the "good" side, their cooperation is "not altruistic." Klarreich (2004) notes that game theory rests on the premise that the players, however cooperative they become, can never be altruistic towards each other because they have ulterior motives. In this excerpt, the participant describes this phenomenon by saying that, in the minds of cyberterrorists, "there is no intrinsic motivation for them to cooperate." Our participant justifies the cyberterrorists' actions by saying that "the cyberterrorists' thought process of what we relate to as unethical or ethical is not necessarily what you and I would consider to be. They have ulterior motives because they have an easy time rationalizing and justifying what they

do." From this vantage point, the way game theory is intersected with social network theory is constructed within a framework of networking with the opposite players (i.e., enemies) without having any intent to establish trust with those players. The last portion of this analysis is the analysis of **RQ4**, which reveals four significant themes that emerged from the participants' accounts.

Chapter VII

Analysis of Research Question 4

RQ4 (What are the themes that emerged across the participants' accounts?) reveals four significant themes that emerged across a vast number of accounts told by the participants. The first of theme, the postmodern state of chaos, revolves around the idea that cyberterrorism has the power to create a state of immense confusion and disorder far different from what our sensory realism, as we know it in actual physical space, has ever experienced. The postmodern state of chaos also implies "cascading failures," that is, ripple effects across a vast network casused by the failure of one important node. The second theme, social engineering, is described as the manipulation by the cyberterrorists of individuals (i.e., Web users) in order to obtain information from them or gain access to a particular location. The main goal of the social engineer is to have control over a network or system. The third theme, called "know thy enemy," is an account of the tactics used by both cyberterrorists and law enforcement to understand the enemy and, by the same token, improve their fight against them. "Know thy enemy" implies the idea of putting oneself in their shoes. The fourth theme, the enemy of my enemy is my friend, is based on the notion that the establishment of a common cause among cyberterrorists is possible through the identification of a common enemy or group of enemies. The same applies to law enforcement; history has recorded that some federal agencies do not get along. However, when they realize they have common enemies, they will fight them together. The data from which these four themes emerged come from many interviews conducted with the participants. No particular question was favored or asked in order to

solicit these themes. All in all, it is the product of all the questions and answers to these questions.

Postmodern State of Chaos

This theme revolves around the idea that cyberterrorism has the potential to generate a postmodern state of chaos. Chaos is a state of extreme confusion and disorder (Gleick, 1987). Although conventional terrorist acts – as the ones usually shown in the media – that are perpetrated against common targets such as mass transit vehicles (i.e., metros, buses, and trains), airplanes, office buildings, and crowded restaurants, create a state of chaos, those conventional terrorist acts have not created a *postmodern* state of chaos, that is, a state of chaos that humans are not able to predict or to which they are not able to respond as they would in actual physical space. Indeed, with respect to conventional terrorist attacks, many emergency reponse initiatives and terrorism preparedness programs have been implemented, particularly after 9/11. What this means is that counter-terrorism agents have strong capabilities to prevent mass-scale terrorist incidents or, at least, fight them, let alone understand them. For instance, they install surveillance cameras (i.e., like those millions of cameras in London), they place scanners at airports, they learn from terrorist tactics, and they send operatives around the world to capture terrorist leaders. These reponses and measures against terrorism are very modernist; they are analog, organized, and disambiguous. They are based on a cause-and-effect sequence. Time and space matter in the modernist perspective. A second reason why conventional terrorist acts have not engendered a postmodern state of chaos lies in the fact that one conventional terrorist act alone cannot jeopardize our critical infrastructure. Although the tragic 9/11 incident caused fear and dismay across the nation,

airports and other major infrastructures were not targeted. As a result, the chaos caused by the nineteen hijackers was very modernist. The weapons that they used (aircrafts) were modernist as well.

However, the thirteen excerpts selected for this theme, all of which come from interviews conducted with seven or eight participants, reveal that cyberterrorist acts have the potential to create a postmodern state of chaos. Although massive cyberterrorist acts have not happened yet, they have the potential to create massive disorder to which we would not be able to respond and of which the effects would be digital, ambiguous, confusing, and non-sequential. These are traits of postmodernism. There is no cause-and-effect sequence as in modernism. Furthermore, cyber attacks are far less predictable, even less understandable or sensical. Nothing happens in a context of spatialization. Postmodernism, just like cyberterrorism, is a shift away from spatialization. Time and space do not matter. In fact, postmodernism challenges both space and the past, the present, and the future. There is no spatial or temporal order possible; everything is discontinous and fragmented. Yet, the effects, as the participants conferred to me during the interviews, could be devastating, far more than what physical attacks could do. The effects of cyberterrorism are such that the state of chaos that humans would endure would be far greater than what they have suffered from modernist terrorist attacks. This is another reason why the state of chaos coming from a massive cyber attack would be postmodern.

The problem is that "when the Internet was designed," said a cyber forensics expert at a Midwestern university, "it was designed to be highly reliable, not highly secure." As it turned out, the Internet designers considered the importance of how to keep

data traffic flowing on the Internet, but not the dangers of failures of routing computers and the disruption of communication links that make up the network. The designers assumed that all computers connected to the Internet belonged to a responsible governmental or commercial enterprise and would never belong to malicious individuals (Dunnigan, 2003). For this theme, the thirteen accounts describe the mechanics of cyberterrorism and its effects in detail. The main focus of their description of what cyberterrorists are capable of doing is on the fact that a cyber attack has the potential to cripple our critical infrastructures, as they rely heavily on computers. Besides, a cyber attack can generate a cascading failure, that is, a cascade caused by the removal of a single node.

The postmodern state of chaos can be explained through chaos theory. One of the main proponents of chaos theory is Edward Lorenz, a meteorologist and mathematician (Gleick, 1987; Stewart, 1989). The main premise of his theory is that it is a theory of nonlinearity. Based on a mathematical approach to nonlinear modeling, chaos is disorderly orderliness (Remer, 2005). It results in sudden and dramatic change at the same time. More importantly, chaos theory deals with plans B to Z, describing unstable states where even small changes can cascade into gigantic long-term effects (Yorke, 2005). This refers directly to what was just mentioned in the last sentence of the previous paragraph; the postmodern state of chaos implies a cascading failure, where the failure of one important node can have a long-term negative impact – like a ripple effect – on the rest of the network. Chaos theory is based on the premise that individuals cannot control their situation. Rather, their situation can change anytime, from moment to moment (Mounier et al., 2005). As such, chaos lacks periodic repetition (Sataloff, 2004). For this

reason, the concept of chaos is postmodern and fits well here. As will also be explained in the second theme ("social engineering"), chaos theory resembles game theory, particularly with respect to having a definite set of rules. Indeed, chaos, in spite of initial perceptions that is it purely random, has actually an inherently ordered and deterministic set of rules (Chamberlain, 1998; Freeman, 1991), just like a chess game. In one of the descriptions of "social engineering," the intersection of game theory and chaos theory is explained in one pararaph.

Although the participants themselves do not use the word "postmodern," from my interpretation of their accounts, the use and consequences of cyberterrorism are very postmodern. The first excerpt, from an interview conducted with an IT Security Analyst II (or assistant IT Security Analyst), working at a Midwestern university, reveals the extreme and deadly damage that cyberterrorism could possibly do to our society:

> If half of a university loses its power, the consequences would be chaotic. All of the things that we rely on, technology-wise, are huge. It regulates the temperature in this room, it regulates lighting, um, communications. Basically, you can't do any type of business any more. We cannot communicate with a person in the next building if we were used to communicating through email or something else. Online courses… It could be harmful. Look at the computers that regulate air traffic control. All computerized; hospitals too. A big thing in the medical field is that a doctor gets called at 2 o'clock in the morning. He doesn't run in anymore to check on a patient. He logs on to his computer; he can even see the patient, interact with them. If that computer system goes down, the life support of that patient could be in jeopardy. Anything that is considered "critical infrastructure"

with the U.S. probably has some type of technology component to it. If technology and computer networks are attacked, if critical infrastructures are attacked, it would have a devastating impact on us.

Based on the words "harmful" in the middle of this excerpt and "devastating" in the last sentence, it is obvious from the participant's account that "if half of a university loses its power," if a cyber attack targets "computers that regulate air traffic control," and if "anything that is considered 'critical infrastructure' with the U.S. probably has some type of technology component to it," the consequences could be, as the participant tells us in the first sentence, "chaotic." What this means is that the impact of a major cyberterrorist incident would not only be chaotic for society; it would also generate a postmodern state of chaos. This resembles the state of disorder that was expected to be set in motion by the predicted Y2K computer crisis, causing widespread social confusion. As all thirteen excerpts will tell us, the potential for cyberterrorism to create mass chaos and insecurity in a society is there.

What this description also indicates is that the postmodern chaos of the electronic world is such that our reliance on critical infrastructures vastly exceeds our ability to protect them. As the participant reveals, hospitals are computerized; if a computer system in a hospital goes down, the life support of a patient could be in jeopardy. We do have reliable technology, but it is not sufficiently secure. For this reason, a postmodern state of chaos implies that, since our infrastructures rely so much on technology, crippling these technologies would cripple an entire nation. Plus, we would not know how to respond. We might not even understand the causes. Computers control things: from hospitals to power plants, from universities to telephones, from critical infrastructures to a million

other crucial elements of life. Disruptions in any one of these can easily cause loss of life or widespread chaos.

In effect, the cyberterrorist will make certain that the population of a nation will not be able to eat, to drink, to move, or to live. Conventional terrorists cannot do that because their weapons of warfare are modernist. Could they cripple the United States by flying two airplanes into buildings? No. Could they harm even a state by blowing up five police departments? No. Even if history records that our emergency responses are slow to massive conventional terrorist attacks, they still operate in a modernist perspective, where there is a time sequence, a cause-and-effect order, and where humans can move and respond in actual physical space. Responders can see what happened and better predict what could happen in the future. However, the possibilities in cyberspace and cyberterrorism are quasi unlimited. As a former FBI agent discussed in an interview, "tactics and weapons in cyberspace are invented, literally, every day." The game between cyberterrorists and their opponents is evolutionary; it's almost surreal. Cyber forensics experts have to learn from cyberterrorists and go from there. The next excerpt, taken from an account told by a cyber forensics expert in the Southwestern part of the United States, corroborates this previous short statement on the capabilities of cyberterrorists:

> Cyberterrorists are amazingly talented people and you'll get to the end of the analysis sometimes when you finally figure out what the premise of some of their routine is or some of their tools. You just sit down and you say, "Oh, my god. This is good." Sometimes, you don't even know what a computer virus has done. You only see the immediate effects on the system, but it can come back next year and wreak havoc. Cyberterrorists do things that are unimaginable, and that

happens on a daily basis. We can't predict the kind of chaos they can do; it's not like conventional warfare.

The problem, the participant says, is that even cyber forensics experts sometimes do not know what a computer virus has done. The postmodern state of chaos could be a step-by-step process where the chaos stops after a few steps (i.e., a situation where a computer virus was launched and we only see "the immediate effects on the system") and then reemerges to propagate terror even more and to shutdown a considerable fraction of a whole infrastructure network ("it can come back next year and wreak havoc"). This, again, is very postmodern. The chaos that results could be gigantic. The cyberterrorist can plant a virus that wreaks havoc for one week, then that stops, and then that manifests itself one year later to wreak havoc on computers again. In essence, a computer virus can be programmed to function at a certain time or only if a certain condition is met. No physical time bomb could do that; once it explodes, it explodes. It will not reemerge some time later. While conventional weapons are analog – that is, used in a linear sequential order – postmodern cyber weapons are digital – that is, they are not based on a continuous analog order. Besides, what is also problematic is that law enforcement agents and those in charge with the protection of a nation do not have warnings as they do with respect to physical terrorist attacks. They will unlikely be able to stop the cyber attacker since he or she is most likely on the other side of the world.

The postmodern aspect of cyberterrorism is also demonstrated in the fact that cyber attackers can win without ever firing a shot. As for the impact of cyberterrorism, Garrison (2003) mentions weapons of mass disruption as means to cause damage to the infrastructure of a society. Cyberterrorism is successful at making the attack as short as

possible, but the impact as long-lasting as possible. Disruption is a vital element of the postmodern state of chaos associated with cyberterrorism. This is well exemplified in the excerpt below, selected from the same participant (the previous cyber forensics expert in the Southwestern part of the United States):

> If you take out the traffic management system in San Antonio, many things would happen: cameras go down, the police have trouble responding, lights go down, accidents, freeway management goes down. It could easily cause mass chaos on the traffic system. There are so many ways imaginable. Those cyberterrorists could theoretically do it. Water control, they can easily open up dam point gates, flood a city and blow it down. Those cyberterrorists out there try to create a new world order and wreak havoc to such a degree that our nation's infrastructure will get dreadfully damaged.

Postmodern terror implies that cyber attacks make chaos more chaotic. Via a computer, "those cyberterrorists could theoretically do it. Water control, they can easily open up dam point gates, flood a city and blow it down." This statement may not be as dramatic as collapsing tall buildings or massive deadly syndromes, but the destructive potential of cyberterrorism is no less catastrophic ("It could easily cause mass chaos on the traffic system"). All in all, it has the capability to lead to unprecedented chaos and destruction with a few clever strokes of a computer keyboard. While modern terrorist attacks are certainly devastating, imagine the panic and overreaction that might ensue if one day our country underwent mass power outages, failures of street lights, and chaos in other crucial facilities. Any service run by an automated computer system is at risk:

systems that control airline traffic, transportation systems, water and oil pipelines, and similar infrastructures.

Another relevant concept in this excerpt is "new world order" ("Those cyberterrorists out there try to create a new world order"). "New world order" became a catchphrase in the late 1980s when the Soviet Union broke up, the Berlin Wall was demolished, the two parts of Germany were reunified, and a variety of other events occurred. "New world order" was widely accepted by the global media as evidence that the world was seeing a new horizon and was made into a new, international order different from and better than the previous one. Yet, "new world order" is also a term that refers to the joining of forces by powerful and secretive individuals or groups to overturn the existing "order," that is, the system of law or government in place. As it was described in the accounts selected in the analysis of **RQ1**, networks of cyberterrorists are both powerful and secretive. Based on diverse cyberterrorists' motives, their networks might be based on a secret agenda to eventually control the world of computers and cause chaos. A "new world order" in this context would happen through postmodern attacks and tactics that would catch everybody off-guard, something that our world has never seen before. This would imply a dramatic overturn in society, like a full-scale apocalypse. The next excerpt was taken from an account told by computer crime analyst in a police department:

> Cyberterrorism is all messed up. It's not like the war on drugs, where we launch a raid on people after we find out where they are. It's always the same. We've been doing it for years. But, I mean, hackers and cyberterrorists, we don't know where to find them. Our fight against them is not consistent. It's fought in the dark. The

> methods they use are new and they're always changing, and because of that, if they hit us with big-time viruses, there would be massive disorder, something we've never seen before.

Here, significant concepts are being used to illustrate the postmodern state of cyberterrorism. Because their "fight against them is not consistent," as opposed to the war on drugs that is "always the same," it implies that there is a lack of continuity or coherent sequence. By the same token, the "methods they use are new and they're always changing." As such, the postmodern theatre of war may be fundamentally changed by the Information Age revolution, at both the strategic and tactical levels (Peters, 2004). Postmodernism implies a reality that is shifting ("always changing") and evolving. The war on cyberterrorism is evolutionary because cyberspace allows this. Cyberspace implies that cyberterrorism is "fought in the dark." What this also means is that modern terrorism is dealt with in a modern way; it is not based on de-structured and de-centered tactics. However, with postmodernism, the idea of disorder and fragmentation is viewed as an acceptable representation of reality. More importantly, according to the participant, "if they hit us with big-time viruses, there would be massive disorder, something we've never seen before." The postmodern state of chaos could be triggered by computer viruses which, on the market, could be launched for free. No single war fought in the modern perspective has ever been fought for free. The next excerpt corroborates some of the statements made earlier with respect to mass chaos:

> Space and time don't matter. The Internet is all over the world. If anything is connected to the Internet, it's vulnerable at some point. Everything is at stake, your water supply, your electricity, your basic necessities of life. If we didn't have

electricity, it would be mass chaos. Look at your critical infrastructure. Vulnerable? Yes, I think everything is vulnerable.

This excerpt has several implications. First, cyberspace is a manifestation of the postmodern condition (Gur-Ze'ev, 2000) because postmodernism rejects all boundaries ("The Internet is all over the world"). Cyberterrorism is global and exceptionally fast and mobile. In highlighting the danger of cyberterrorism, Pillar (2001) points out the ease of movements across international boundaries and the growing potential for cyberterrorists to manoeuvre despite long distances. The space-time compression established by a postmodern communications environment (Lister et al., 2003) enables cyber attacks against the Internet and other computer networks to be carried out far away, making physical barriers irrelevant ("Space and time don't matter"). Cyberspace is the new public sphere because it is all over the world, at any particular time or place (Zarefsky, 1994). Consequently, the postmodern map of cyberspace becomes the totality itself, superseding the world. Cyberterrorism is also a postmodern strategy for spreading terror because it seemingly has no limits; no inside or outside.

Second, without a doubt, cyber attacks can be waged via the Internet, which makes cyber targets extremely vulnerable ("If anything is connected to the Internet, it's vulnerable at some point"). Anything that is connected to the Internet is so vulnerable that "everything is at stake, your water supply, your electricity, your basic necessities of life." As a result, "if we didn't have electricity, it would be mass chaos." It's a unique techno-challenge. Imagine the following: without networks controlled by computers, there would be no water coming out of our taps, there would be no electricity lighting our rooms, there would be no food being carried to our grocery stores, there would be no

monetary funds coming out of our banks, and there would be no emergency systems responding to emergencies. All this would be a postmodern state of chaos. As some participants recounted in previous sections, cyberterrorists' motivations are more than feelings of "what can I do to try to invade someone's space." From the participants' accounts, cyberterrorists motivations are really to cause havoc and chaos.

The following statement is short; it was made by the associate head of an information technology center in the Midwestern part of the United States. For him, "cyberterrorism is real. The real difficult question is how to quantify it." In other words, we can have a rough estimate of Al Qaeda members or even the victims of their terrorist acts. However, because of the anonymous and ubiquitous nature of cyberterrorism, we cannot have a similar type of assessment. If truth be told, it really is impossible to quantify cyberterrorism. As of January 2006, more than one billion people are using the Internet (Internet World Stats, 2006), which means that over one billion humans could launch a computer virus from anywhere and at any time. Are cyber enemies or cyberterrorists countable? No, or, at the very least, "hardly" countable. Even more, although chaos is quantifiable in the modernist realm (i.e., we could count the number of 9/11 victims and the amount of damage inflicted on 9/11), chaos cannot be quantified in the postmodern state of things. If "everything is at stake," is it measurable? No, such chaos could not be measured. Our dams, our electricity, our water supply, our essential infrastructures, basically, our life could be compromised by cyber attacks. Is it quantifiable? No, but it is still very real. For this reason, the state of chaos that could be inflicted by cyberterrorism is very postmodern. The following excerpt comes from an

interview conducted with the chief information security officer at a Midwestern university and its regional campuses:

> Protecting the country against cyberterrorism is the same as protecting the country against terrorism or illegal intruders, with physical borders. The problem is that it's hard for us to tell good zeros from bad zeros. Just because something is good yesterday does not mean it's gonna be good tomorrow. With every new piece of technology comes a new way to try to exploit it. Even if we wanted to take the philosophy of trying to stop all the bad zeros at the "border," it's a never-ending process. We pride of ourselves of creating wonderful technology, but sometimes we feel that we're shooting ourselves at the foot and that we suffer from it.

Numerous implications can be inferred from this excerpt. First, the participant informs us that the "problem is that it's hard for us to tell good zeros from bad zeros." Game theory would apply well in this context. Let us take the example of the fight between the Red Brigades, a Marxist-Leninist terrorist organization active in Italy in the 1970s (Ignazi, 2003; Lloyd, 2002), and their opponents, counter-terrorism agents. The Red Brigaders and their opponents were clear opponents. It was rarely difficult for any player of the game to tell who was who. The rules of the game were easier than those in cyberspace; the Red Brigaders and the counter-terrorism agents were taking actions against each other in a linear dialectical process. This was a battle fought in a modernist realm. Based on game theory, they were learning from each other's strategies as they were taking actions and moving to the right locations. Because they fought in actual space, they were operating within physical borders. As such, it was difficult for any of those players to infiltrate their enemy's "team." However, on the Internet, there is so

much anonymity that it is hard to differentiate good zeros from bad zeros. It is not only difficult to tell what game the cyber attacker is playing; it is also difficult to determine who the other player is or what his or her ulterior goal is. Is the other player a good zero or a bad zero? Is the other player a real danger or is it actually one of our agents acting as a cyber spy? Because of the postmodern nature of the Internet, because of the absence of spatiality, because of the negation of geometry, and because of the shift away from spatialization, the players in this postmodern fight between cyberterrorists and their opponents can move effortlessly across the spatial divide.

Second, as the participant shared with me, "with every new piece of technology comes a new way to try to exploit it." For every wall, there is a ladder. We are vulnerable to the technologies upon which we rely. There are always soft spots. No matter how high we build a wall, it can be reached by helicopter. Postmodernism implies this never-ending process; it is ceaseless, uninterrupted in time, *ad infinitum*, long continuing. Defensive measures in the modernist world, on the other hand, have clear boundaries. Let us take the example of Homeland Security. Its governmental actions made to prevent, detect, and respond to acts of terrorism can, one day, reach a certain scope, to such a point that no terrorist attack will be successful at all. In fact, today it is already much more difficult for terrorists to commit horrendous acts in certain parts of the United States. In addition to the emergency response initiatives put into place, we also have those domestic intelligence activities (largely today within the FBI), protections of critical infrastructures, border security and transportation security measures, biodefense programs, and detection mechanisms for nuclear and radiological materials (Kamien, 2005). The list can go further and further.

Third, related to the same statement, "with every new piece of technology comes a new way to try to exploit it," for every technology, there is a hole and "even if we wanted to take the philosophy of trying to stop all the bad zeros at the 'border,' it's a never-ending process." We can stop the bad zeros today, but new technologies will have new soft spots and new bad zeros will emerge. Likewise, cyberterrorists will try to find these new soft spots. The fight will always be evolving, but it will never end. Both sides will become better at it, but the courses of action against each other will never end. All this can lead to a postmodern state of chaos. Based on game theory, it is really an evolutionary battle that never finds an outcome or end-result. And unconcluded wars or wars without ending are very chaotic. Even if one player thinks they have found an outcome, the outcome might be different tomorrow. To support this last statement, it is worth looking into what the participant said in the indented excerpt selected above: "Just because something is good yesterday does not mean it's gonna be good tomorrow." Law enforcement agents think they got the bad zeros out, but it might be the case that they got the wrong "bad zeros" or that the battle is simply not over.

Fourth, the methods of counter-terrorism that domestic and international agents have perfected over the decades are ineffectual against cyberterrorists. Let us look at it this way: cyberterrorists do not attack us with truckloads of explosives, briefcases of Sarin gas (Sharp, 2006), or dynamite sticks strapped to the bodies of fanatics. Cyberterrorists attack with algorithms (i.e., ones and zeros) at locations where we are most vulnerable and where our lives depend on. And it is so convenient, cheap, and innovative. The multidimensional and slippery facets of postmodernism constitute this innovation; anything goes with anything, like a game without ending. *That* is very

chaotic. Cyberterrorism constitutes a powerful lens through which to view the emergence of postmodern conflict in cyberspace fought within the context of "intellectual technology" (Bell, 1973). Simply put, intellectual technology means that bad zeros [algorithms (problem-solving rules)] are substituted for intuitive tactics (Bell, 1973). Making a comparison between postmodern cyberterrorism and modern warfare, it is the same as saying that mips – that is, millions of computer instructions per second (Gruman, 2005) – are substituted for muscular might.

Lastly, the postmodern state of chaos is representative of our being the slaves of the technologies that we have created. As the participant tells us at the end of the indented excerpt in question, "we pride of ourselves of creating wonderful technology, but sometimes we feel that we're shooting ourselves at the foot and that we suffer from it." This is a throwback to the argument made by Donald Norman (1993) that society has fallen into a machine-centered orientation to life, one that overemphasizes the needs of technology. Our technology is wonderful when it fulfills our needs. As Norman (1993) contends, we create technologies and build machines. What we build makes us smart, even smarter. When designed well, technologies help us do important accomplishments and provide us with affordances for desired behaviors and outcomes. Yet, as the participant recounts, "we feel that we're shooting ourselves at the foot." We devote a lot of time and effort into building machines that can hurt us, to such a point that today we serve our technologies (Norman, 1993). As the participant says, now we "suffer from it." For Heidegger (1977), we have reached the edge of the "supreme danger," that is, of succumbing to the limited vision of technology. Cyberterrorism perfectly exemplifies all this; the notion that our technologies can hurt us when they are targeted. We are proud of

technology, we rely on the Internet and computer systems, but the vision we have of technology can be limited as our blind reliance on technology can be turned against us, to the degree of creating an unprecedented mass chaos. Cyberterrorists know this.

The next excerpt is an addition to the previous one, also dealing with the "never-ending" facet of cyberterrorism and computer technologies. It was taken from an interview conducted with a computer crime analyst in a cyber forensics lab at a Midwestern university:

> Every time we create a new technology, something vulnerable occurs. There are new holes to patch. The Internet reduces naiveté; it reduces a lot of the ethical boundaries. Cyberterrorism is there; we'll always have it. Every time something new is created, we're gonna have another hole.

The statements made by this participant reinforce the statements made by the previous participant. "Every time we create a new technology," the participant says, "something vulnerable occurs." From this vantage point, the possibilities for cyberterrorists to create chaos are tantamount to the vulnerabilities provided by technology. In other words, the probabilities of cyber attacks increase as the vulnerabilities of our technologies increase. With new technologies, "there are new holes to patch." Based on game theory, this evolutionary process is produced by an ongoing conflict of chaos, which will never be totally resolved or put to an end. For this reason, it is never-ending ("Cyberterrorism is there; we'll always have it. Every time something new is created, we're gonna have another hole"). Another problem, our participant continues, is that cyberterrorists have the upper hand because they have no ethical standards (i.e., the Internet is a good means for them because it "reduces a lot of the

ethical boundaries"), which seems that the game law enforcement agents and cyber forensics experts are involved in has to be played by the standards determined by the cyberterrorists. Cyberterrorists, then, are the ones making the rules.

The next excerpt emphasizes the ambiguous and confusing aspects of the Internet. Because of so much anonymity and openness in cyberspace, cyberterrorists turn the Internet to their advantage, as this associate professor and chair of a cyber forensics program in a department of computer and information technology at a Midwestern university conferred to me:

> I believe cyberterrorism is dangerous. The fact is that much of our infrastructure now, the things that we need the most, electricity, water, are run, powered, and managed by computers. Anybody that can attack or take those systems down is a serious threat. And it just takes a few keystrokes. Much of our business, our financial situation, our commerce, is all done on the Internet. Financially, it can be a big problem if those networks were taken down. Not only wouldn't we be able to respond to information warfare attacks but, also, in most cases we wouldn't know where those attacks come from, and we wouldn't know whom to retaliate against. All that stuff is ambiguous and confusing.

The advantages of a cyber attack over a physical attack are evident. A cyber attack can be executed from a remote site and a few keystrokes (i.e., anybody can attack "and it just takes a few keystrokes"); the chance of detection is much smaller than a terrorist setting a time bomb in a shopping mall or in a public bus. Would a cyberterrorist have a crack at gaining entry to the Federal Reserve building or another of those bonanza buildings? It is very unlikely since failure is almost guaranteed. Likewise, a large truck

pulling alongside a building like these is very noticeable. Nevertheless, in the case of a cyberterrorist, the attacker is sitting in his or her room, probably in a remote location, attempting to make a nation's economic system grind to a halt. The chances for such destabilization are more achievable. The cyber attack can be more flexible than a brute force physical attack (again "it just takes a few keystrokes"). The leverage can be much greater than for a physical attack ("Much of our business, our financial situation, our commerce, is all done on the Internet. Financially, it can be a big problem if those networks were taken down"). Such chaos is very postmodern.

What this all means is that the modern, physical world is matter and energy – warm and cold, time and space, all physical matter; bombs and airplanes, all physical matter as well. It is that world in which humans are raised, live, and function. The virtual world is not made of matter and energy; it is postmodern; it is that world in which computer programs function and data move. From a logical standpoint, placing bombs at different locations and at the same time requires at least one operative per location. On the other hand, planting a devastating virus into thousands of connected computers at dispersed sites may take a few keystrokes and only one operative on another continent. This form of terror is very postmodern. So is the chaos thereof. Cyberterrorism, our participant discloses, threatens the global economy (i.e., "Financially, it can be a big problem if those networks were taken down"). This is a throwback to the potential Y2K catastrophe mentioned earlier. A cyberterrorist will disrupt "much of our business, our financial situation, our commerce," all of which is "done on the Internet." The chaos would also be a situation where the citizens of a country lose their confidence in the nation's economic system.

In line with these contentions, the postmodern chaos is demonstrated in the fact that, should a major cyber attack emerge, "not only wouldn't we be able to respond to information warfare attacks but, also, in most cases we wouldn't know where those attacks come from, and we wouldn't know whom to retaliate against." From this, it follows that, since law enforcement and cyber forensics experts might not be able to respond to a major cyber attack, there would be no means of signaling an alert of that cyber attack to the rest of a nation. This is a postmodern challenge that humans have to face. As it turns out, the literature shows that, as a matter of fact, there is a shortage of qualified and trained personnel to detect and respond directly to cyberterrorist attacks (Mecham, 2002). More precisely, even though our country has cyber forensics experts and computer crime analysts working for law enforcement agencies like the FBI or the CIA, there are an insufficient number of Army, Navy, and Air Force personnel able to protect the nation against cyberterrorist attacks. Given these facts, let us picture ourselves in a situation where systems go down simultaneously; electricity shuts down, phone lines fail, 911 emergency services are grinded to a halt, and other incidents.

Such is the chaos that we can all encounter in a postmodern state of affairs, giving us more deconstructions than constructions, more of a fragmented landscape than one of wholeness, and more questions than answers. For this reason, "all that stuff is ambiguous and confusing," says our participant. By "ambiguous" and "confusing," postmodernism is held to the very notion that it has a de-structured, de-centered reality that is also fragmented. So, postmodernism accepts the possibility of ambiguity. Ambiguity implies that reality (i.e., things and events) can have two different meanings simultaneously. A modernist and linear approach is set to avoid or reduce ambiguity as much as possible.

Postmodernism, in contrast, embraces simultaneous views not as conflicting but as being part of the complex patterning of reality (Derrida, 1967). Accordingly, cyberterrorism is to be understood form the standpoint that, for the past several years, part of the paradigm of modernist conflict has shifted to that of postmodern chaos, that is, a state of ambiguity, complexity, de-structuration, deconstruction, discontinuity, and the negation of other modernist aspects of the real.

Of equal relevance is the fact that the postmodern nature of the Internet is such that, according to our participant, "we wouldn't know whom to retaliate against." In fact, postmodernism can dilute the very notion of friend and enemy because, as another participant communicated to me, "on the Internet, nobody knows you're a dog." Hence, this opposite extreme facilitates the replacement of modern order by postmodern chaos. In cyberspace, whom are we dealing with, after all? Who is who? As a computer crime specialist with the National White Collar Crime Center said, "it's very difficult to categorize people as cyberterrorists or the 'good guys.' You don't always know who's who." In today's postmodern terrorism, the human dimension is taken away from the enemy. The postmodern enemy can appear in many guises. Cyberterrorists are held up as the invisible, irrational enemies capable of incalculable damage. They are more mysterious than enemies we have seen before. Postmodern cyberterrorism entails fighting with the mysterious and in mysterious ways. Also mysterious, and certainly problematic is that, as a participant from the South asserted, "the Internet has no center." This means that, because the Internet negates geometry (Mitchell, 1995), cyber attacks come from no center. The postmodern state of chaos represents that very state of de-spatialization and de-structuration mentioned earlier. The next excerpt, selected from the interview with the

same computer crime specialist with the National White Collar Crime Center, is partly a follow-up argument that nobody knows who is who on the Internet:

> Anybody can use a computer to commit a crime. They can do it everywhere throughout the world. A cyberterrorist can create a two-hour outage during which emergency services are impaired or ambulances are not getting a heart-attack victim to a vital destination on time. Every time you interrupt the communication flow, that's a problem because there is a certain amount of communication that takes place on an infrastructure that people's lives depend on. Another thing is what appears as innocuous on the surface and not as something malicious.

From this excerpt, it follows that we do not have to examine the international scene in order to identify potential sources of cyber attacks. The sources are from everywhere ("They can do it everywhere throughout the world") and from every web user ("Anybody can use a computer to commit a crime"). A single individual, working in a private home and taking advantage of commercially available hardware and software, is capable of committing acts that can yield to the economic and social chaos described so far. Besides, if cyberterrorists can launch attacks from anywhere, they can potentially frame other people for their evildoing. Truly, information technology makes time and distance senseless and leads to the disconcerting condition of "everywhere throughout the world." Now, the modernist symbiosis set by time and space is being disassembled. The results are both profound and far-reaching. They lead to vulnerability and volatility.

The participant's other statements not only pertain to the danger of cyber attacks (i.e., "a two-hour outage"), but also to the seemingly harmless aspect of what can be done in cyberspace ("Another thing is what appears as innocuous on the surface and not as

something malicious"). Kevin Mitnick's (2002) book, *The Art of Deception*, is an account of how tactics that look innocuous can actually be very malicious. This book is essentially about earning someone's trust by deceiving them and then abusing that trust for malevolent purposes. The postmodern state of chaos can be amplified by what will be explained later – in the second theme – as "social engineering." The next excerpt, taken from a cyber forensics expert in the Southwestern part of the United States, emphasizes the dangers for computers of having all threads and infrastructures to be connected to the Internet:

> The targets can become primary, secondary or tertiary victims. Targets are going to be the critical infrastructures, which is going to be your telecommunications, your hydroelectric, your oil, your gas, your hospital, your air traffic control, your transportation. All these have connections on the Internet, whether these infrastructures are the primary infrastructures or not. They all have threads, they all have connections.

Without a doubt, the full potential of cyberterrorism is a possibility that should concern us. The participant tells us that "the targets can become primary, secondary or tertiary victims." What is of equal concern is that our interconnectivity ("threads") is what makes us vulnerable (i.e., all these infrastructures "have connections on the Internet, whether these infrastructures are the primary infrastructures or not"). Now we know it: those with a high degree of computer knowledge can use those connections and threads against us. As a result, the threats to critical infrastructures go beyond those of physical attacks. For the past couple of years, each of the infrastructure sectors has gradually more relied on the Internet, information systems, and computer networks for their operations.

The interconnected nature of our infrastructure sectors drastically amplifies the impacts of service disruptions. Major troubles or disorders that start at the local level or in one sector are more likely than ever before to cascade at the regional or national levels. As a result, they would severely impact multiple sectors of the economy.

For this reason, the following accounts pertain to the "cascading failures" caused by the destruction of one node (that is, the knocking down of one actor in the network; be it a critical infrastructure or an important hub in the system) that has been attacked by a cyberterrorist. Such cascading failures, or "ripple effects," or even, simply, "cascades," could contribute tremendously to the postmodern state of chaos associated with cyberterrorism. The first of these accounts, coming from an IT Security Analyst II (or assistant IT Security Analyst), reveals the dangers of computer viruses and the cascading failures that result from those viruses:

> You're familiar with Code Red that came out in 2001? Basically, it was a virus attack against computers running Microsoft's IIS web server, you know, a whole bunch of workstations connected to the Internet. What you had was a cascading failure to a certain degree. Some of the adjacent and connected systems became failures too. I don't think the cyberterrorists brought down what they really wanted. Eventually we recovered from the attack, but it could have been disastrous for the Internet.

What this excerpt is revealing is that the probability of cyberterrorism bringing down the Internet is real and that the technical achievability has been already demonstrated to us, at least partially ("What you had was a cascading failure to a certain degree"). Our participant recounts that what provoked this partial cascade failure was a

virus named Code Red. The literature says that Code Red was a computer virus launched in the summer 2001 that caused an estimated $2.4 billion in damage (Acohido, 2002). The effects of Code Red would have been even more damaging, leading to a postmodern state of chaos ("it could have been disastrous for the Internet"). The word "disastrous" is in the same ballpark as the work "chaotic" stated in previous excerpts. Here, the virus could have been dreadful, affecting the entire Internet and, in the same process, every vulnerable machine connected to the Internet. Berghel (2001) contends that the Code Red virus infected more than 250,000 systems. The virus crawled over the Internet, mixed up important vulnerable systems, and infected other programs connected to those systems. The result was a cascading failure.

From a social network theory perspective, this Code Red incident demonstrates that if one large node (hub) is brought down, other large nodes (hubs) in the network can suffer as well. A cascading failure is a failure in a system of interconnected nodes, where the service provided is contingent upon the operation of a preceding node, and the failure of a preceding node can trigger the failure of successive nodes (Newth & Ash, 2004). An example of cascading failure happened on August 10, 1996 in a western United States power grid. As it turned out, everybody was affected by it (Barabasi, 2002). More precisely, in the summer of 1996 in Oregon, a mixture of hot weather and unusually high demand of electricity made power lines sag into trees, causing a cascade failure of power stations and distribution substations. It also affected infrastructures and power supplies in the neighboring states. Barabasi (2002) calls this destructive step-by-step process a flow of internal failures. If the major part of a network is destroyed, it can induce a cascading

failure in the form of internal chaos in a network. For instance, in a power transmission grid, each node (power station) deals with a load of power. The removal of nodes, either by random breakdown or intentional attacks, alters the balance of flows and provokes a global redistribution of loads all over the network. In turn, this can trigger a flow of internal failures.

For a cascading failure to be successful, the attack that leads to it must be well thought out (Berghel, 2001). The Code Red virus attack exploited a large node, that is, a specific software weakness in one of the tons of servers and workstations connected to the Internet. That weakness was exploited to create the 2001 cascading failure; the Code Red virus provoked a self-replicating failure that induced additional failures (Metz, 2004). In other words, based on the tenets of social network theory, a single point of node failure on a fully loaded network can result in a sudden spike across all nodes of the network. Recall that the attacked node has to be as large as a hub in order to have consequences on the others [i.e., sending a destructive virus against a hub (Barabasi & Albert, 1999)], because small node failures like random node failures are merely drops in the ocean. The network connectivity of the Internet – and hence its functionability – is such that the Internet is robust against random failure of nodes (Albert, Jeong, & Barabasi, 2000) and to some extent is even robust against intentional attacks. However, the Internet, where the load represents the amount of information a node (router) is requested to transmit per unit of time (and overloads correspond to congestion), can collapse, to a certain degree, caused by congestion. Such incidents have been reported since the very inception of the Internet (Barabasi, 2002). Part of the reason is that, as Albert, Jeong, and Barabasi (2000) have contended, there is a very small average distance

between nodes on the Internet, as well as a highly organized distribution of links per node. Rarely will the average distance be affected by the removal of a random number of nodes. Nevertheless, it will increase significantly if the removed nodes are among the most connected ones (Watts 1999a, 1999b).

Fortunately, so far, cascading failures have been limited to only ten thousands of sites (i.e., 250,000 from the Code Red virus). The problem is that, based on what the participant reveals in the excerpt selected previously, the effects of the cyberterrorist actions could be far more disastrous for the Internet. When the cyberterrorists approach the study of Internet weaknesses in a planned and concerted manner, and if their attacks become fully successful, they could create a postmodern state of chaos, like a cyber 9/11. In fact, another participant (a senior analyst engineer in computer forensics) expressed his concern about the possibility of a postmodern state of chaos when he said that "one day, we might have our cyber 9/11." The "cyber 9/11" statement termed by this participant perfectly exemplifies chaos. This adds to other excerpts, selected at the beginning of this theme, that have described the dangers of cyberterrorist attacks against the Internet, power plants, electrical power grids, and other critical infrastructures, all of which can have a deep impact on our lives as they depend on those infrastructures. Here, the main argument is that something needs to be done or the consequences will be a "cyber 9/11" or, as the theme indicates, a postmodern state of chaos. The following excerpt reveals the type of devastation that can be created if there were a successful attack against a few hubs in a scale-free network. This excerpt was selected from an account told by an associate professor specializing in social network theory at a Midwestern university:

> The Internet is a network that's scale-free. If you were to create a map of the Internet, you would come to the conclusion that the Internet is just a large bunch of hubs, you know, like routers and that all that kind of stuff. The Internet is very susceptible to cyber attacks on those hubs, the kind of thing cyberterrorists like to do. It's also heterogeneous, you damage a few of those hubs and the rest falls too.

We saw earlier that the Internet is a scale-free network because it can support most random node failures (Dorogovtsev & Mendes, 2003). In other words, the Internet is not a random network where a small number of random failures can create its collapse. Rather, it is a scale-free network that tolerates random failures up to 80% of its nodes before it gets destroyed. Yet, because the "Internet is just a large bunch of hubs," as the participant tells us, it follows that the "Internet is very susceptible to cyber attacks on those hubs, the kind of thing cyberterrorists like to do." The participant's account is consistent with the scientific proof that scale-free networks are tremendously vulnerable to cyber attacks on their hubs. Indeed, attacks that eliminate even a small amount of important nodes (hubs) in a scale-free network like the Internet can break it apart (Keller, 2005). For this reason, simultaneity of a cyber attack on selected hubs could be extremely chaotic. This is the postmodern nature of cyberwar.

Another important concept stated in this excerpt is the word "heterogeneous." Cascading failures only occur in heterogeneous networks ("It's also heterogeneous, you damage a few of those hubs and the rest falls too"), not in homogeneous networks. The basis for this is the non-homogeneity of the nodes in the network; failures are much more likely to occur on nodes that are quite small (Albert, Jeong, & Barabasi, 2000). Thus, from a social network perspective, cascading failures only occur in heterogeneous

networks, that is, networks where few nodes have the capacity for high-loads (or, simply put, hubs) and where the rest of the nodes only have the capacity for low-loads (that is, small nodes). Another reason the Internet is a heterogeneous network lies in the fact that heterogeneous networks connect computers and other machines with different operating systems and protocols. For instance, LANs (local area networks) that connect Microsoft Windows and Linux-based PCs with Apple Macintosh computers are heterogeneous (Zivkovic et al., 2005). Hence, a homogeneous network does not suffer cascading failures because all its nodes handle an equal load. Unfortunately, most infrastructure networks nowadays – since they rely on information technologies and the Internet – are heterogeneous by design, which makes them very vulnerable or, as the participant informs us, "susceptible" ("The Internet is very susceptible to cyber attacks"). "Susceptible" is the right word here because vulnerability is the susceptibility of a network to fail under a cyber attack. The following excerpt was taken from an interview conducted with the chair of an information technology center at a Midwestern university:

> Cyberterrorism is there. Even the U.S. does not know how to deal with it right now. I see cyberterrorism to be a force multiplier. The first attacks that we will see will be the ones that will be devastating; attacks on critical cyber infrastructures in addition to attacks against traditional physical infrastructures. You blow a dam and you deregulate utilities industries (i.e., gas, water, electricity), you blow a plane and then you target the air traffic control and the other control systems so that you can't even get the emergency responders. You basically increase the force of that attack by magnitudes. It's like a cascading failure.

From this vantage point, the postmodern state of chaos could be a rapid process ("you blow a plane and then you target the air traffic control and the other control systems so that you can't even get the emergency responders"). The cascading failure here is not caused by one hub affecting other hubs, as it was described in the previous accounts. Rather, in this excerpt, it is seen as a "force multiplier" ("You basically increase the force of that attack by magnitudes"). A force multiplier is a term used in the military that refers to a factor that dramatically amplifies – and hence multiplies – the combat effectiveness of a military force (Burkard, 1994). In this context, cyberterrorists can create a force multiplier by using both cyber attacks and conventional attacks ("attacks on critical cyber infrastructures in addition to attacks against traditional physical infrastructures"). A cascading failure will be the result from all the damage caused by the combination of the attacks.

Truly, networks are a vital part of modern society (Strogatz, 2003). The breakdown of one hub can unbalance the flow of the network and, by the same token, cause load redistribution to other hubs or the nodes connected to the hub that was initially damaged (Motter & Lai, 2002). Social network theory treats network ties and nodes as having a random probability of failure. To be more precise, their failure [vulnerability] is the susceptibility to disruptions that can cause reductions in network service or the ability to use a particular network link (Berdica, 2000). In fact, in any network, the hubs are so crucial that when they are destroyed, the network breaks into pieces. More importantly, this dependence and contingence on hubs is a weakness for the Internet and other information networks because an attack against the hubs can be very harmful.

Sadly, these examples do not belong to the realm of science fiction. On the contrary, they are real and can be executed today. As the international community continues to rely increasingly on information technologies, it will become ever more possible for cyberterrorists to cause chaos, on and via the Internet, on a level previously adapted for weapons of mass destruction in actual physical space. The ubiquity of access to harmful cyber weapons and methods brings to mind that a number of cyberterrorists are able to launch the specter of an unanticipated and unprecedented massive-scale attack on critical infrastructures, one that may cripple vital targets like electrical power plants, gas and oil, banking and financial supplies, water supplies, and emergency services. Likewise, imagine the chaos that could result from a cyberterrorist launching malicious programs on military, transportation, and telecommunication networks. Information is disseminated broadly and rapidly ("And it just takes a few keystrokes"). One single-handed cyberterrorist attack could cause the whole infrastructure of a country to crumble. Not only are the information technology means required for mass destruction so different from the WMDs (that we know in the physical world) that they are hardly computable or assessable, but, also, the possibilities of such deadly cyber weapons are very real.

Because the modern world is so interconnected, a cyber attack at one point of the technological infrastructure can generate a disastrous cascading effect. For this reason, the main focus of the last part of this analysis was on cascading failures, that is, cascades caused by the removal of a single hub. The possibility of such chaos is well established. Cascading effects of destruction, even momentarily, of critical infrastructure systems such as power, communication, or emergency care, single-handedly or in conjunction with other attacks, have very much been the concern of governments and law

enforcement agencies. Their goal is to understand and protect our safety in the collective. The postmodern state of chaos could reach a high degree. What makes the possibility of technologies to be turned into weapons of mass disruption and confusion is that (1) cyberterrorist attacks can originate from anywhere, (2) there is a lack of qualified and trained personnel, even in law enforcement agencies, to respond, let alone identify, these attacks, and (3) there are no solid or dependable means to signal a cyber alert to the rest of the country. It is a postmodern challenge that humans have to face. Think of the chaos that could result from a cyber attack coordinated with a conventional strike, such as the bombing of an extremely densed area combined with the compromising of emergency systems (like those that tamper with hospitals and first-responders services for wounded civilians). That is our postmodern fear. It looks like humans have to live with the Y2K panic for the rest of their lives. In a sense, we all do.

Social Engineering

This theme is different from the previous theme of "postmodern state of chaos," but it is equally relevant. We have seen that cyberterrorists attempt to find weak spots or exploit holes in computer systems in order to cause mass chaos. Cascading failures are a good example. Yet, cyberterrorists also use another tactic: social engineering. The theme of "social engineering" emerged in many of the accounts revealed by the participants. Social engineering is as old as humankind. It is defined as the manipulation, by an outsider, of an individual in order to obtain information from that individual or gain access to a particular location (Kopf, 1998). The main goal of the social engineer is to have control over a network or system.

The concept of social engineering was already discussed in the literature over sixty years ago. Karl Popper (1945), for instance, argues vehemently against social engineering, which he equates as manipulation and population control, as exemplified in the social engineering values of Nazism and Communism. For Popper, Nazism bases its social engineering values of control and manipulation on a national level, whereas Communism on an international level. For these reasons, Popper promotes a fundamentally different type of social engineering: "piecemeal social engineering." This essential value of Popper is not to manipulate society, but to advocate changes in an open society and on an individual level (Popper, 1945). Popper is altruistic and wants to improve society. As he explains it, "Whatever his ends, he [man] tries to achieve them by small adjustments and re-adjustments which can be continually improved upon" (Popper, 1961, p. 66).

However, cyberterrorists, as opposed to Popper, are not altruistic and society-oriented. On the contrary, they are selfish, terror-oriented, and manipulative (Matusitz & O'Hair, in press). Social engineering is one of their tactics to reach their ends. In order to be successful, the social engineer will target the weakest link in a network – the human being. As such, the social engineer will exploit human weaknesses such as ignorance, naiveté, and the natural propensity to be liked, helpful, and, above all, gullible and trustworthy (Erlanger, 2004). For the purpose of this analysis, we will limit ourselves to social engineering as described in the context of information technology and the Internet. Based on the accounts from various participants, the outsiders doing social engineering are cyberterrorists and other malicious hackers who use unimaginable tricks on a computer or web user in order to obtain the information they need. Their ultimate goal is

to control a computer or network in order to wreak havoc. One participant, an IT security analyst, expresses his view on social engineering:

> Social engineering is a huge aspect; it can apply to both computers and non-computers. It's basically humanized cyberterrorism. You convince somebody else to give you their password and you've got one piece of the puzzle by being logged into their network. This is what social engineering is. You learn who the player is so that you can actually break into the system more easily in order to control it and eventually destroy it.

This participant clearly reveals that social engineering is an evil practice ("humanized cyberterrorism") of obtaining vital information through the manipulation of Web users. Here, the cyberterrorist tricks people into revealing confidential information ("their password") or getting them to take actions against typical policies (not to let any outsider into their network). Social engineering is the art of persuasion ("you convince somebody else to give you their password"). It is the art of getting humans to comply with one's wishes ("you've got one piece of the puzzle"). As we will see in this section, by using a variety of manipulative techniques that abuse a human being's natural propensity to trust and provide assistance to others, cyberterrorists can learn user names, passwords, ID information, names of key personnel, and other types of data that allow them to penetrate networks and control them – even those secured with highly advanced technology (Erlanger, 2004). Besides, the methods of social engineering use very low cost and low technology means to surmount obstacles posed by information security measures.

Regardless of the method used, the main objective is to convince the person disclosing the information that the social engineer is in fact a person that they can trust with that sensitive information. Because social engineering involves strategies of persuasion, tactics of manipulation, and different moves to capitalize on the victim's ignorance and willingness to blindly trust strangers, social engineering is, in essence, a game. The description below, recounted from a participant who is an expert in cyber forensics, makes it very obvious:

> Social engineering is a game. Social engineering is when an attacker will use tools in addition to, uh, the traditional network to coordinate or launch an attack. They will lure the secretary, to get her provide secret information just as a password or ID. Social engineering is a convenience mechanism. The attacker will take a really good guess at what moves the secretary will make. Kevin Mitnick's book, *The Art of Deception*, has a lot of examples like that.

From this excerpt, it appears that "social engineering is a game." Most of the work of social engineering is in the rules and preparation, rather than the attempt itself. Social engineering is a skill, and like any skill, the more one practices the game, the better one becomes. Practice makes perfect. Game theory can be briefly discussed here. Just like a chess game, social engineering is not a game of chance. It is based entirely on tactics and strategies. Game theory and chaos theory can be intersected here, particularly with respect to having specific rules. Indeed, chaos, in the face of initial perceptions that is it entirely random, has actually an inherently ordered and deterministic set of rules (Chamberlain, 1998; Freeman, 1991), just like a chess game. The success of the game is not influenced by some randomizing device; it is based on tactics, strategies, and, above

all, rules and preparation. In chaos theory, the future is prepared not by conceptualizing some place or time out on the horizon. Rather, the future is based on an individual's next thoughts, words, or actions. It is not solely based on chance (Bright & Pryor, 2005). Likewise, social engineering is the appropriate method whenever the success of an individual depends on another individual. So, in this respect, game theory is an essential component of chaos theory.

As we have just seen, the success of the game is not influenced by some randomizing device. Kevin Mitnick knew this. Kevin Mitnick is a former social engineer who, after being caught, served five years in prison (Shimomura & Markoff, 1996). He was convicted of Internet fraud and of breaking into the computer systems of Fujitsu, Motorola, Nokia, and Sun Microsystems (Littman, 1997). When he was released from jail in 2000, he wrote a seminal book on social engineering called *The Art of Deception*, with his friend William Simon (Mitnick & Simon, 2002). Another reason social engineering is an important theme lies in the fact that social engineering is all about communication. It is the process of using social interactive skills to obtain critical information from a victim. The last four words of the next excerpt, from a cyber forensics expert in the Midwest, clearly demonstrate that social interactions are necessary for social engineering to be successful:

> They also utilize the social engineering skills. They could get in just enough to get the systems administrators information and then you start doing social engineering, contact them and say, "Hey, this is so and so…" "I'm working on your system; I need your password… so…" It seems to me they get a little piece

of the pie and they build on the blocks, those little pieces that they obtain, and one way to do that is social engineering. Social interaction is important.

Indeed, "social interaction is important." Social interaction is the set of behaviors and beliefs between individuals dependent upon the behavior and beliefs of one other and of other individuals. It is a dynamic, evolving sequence of social actions between people who alter their actions and reactions *vis-à-vis* their interactions with others (Mead, 1934). When humans interact in an environment, they do not do it in a vacuum. There are conventions and rules that constrain their social behavior. The same applies to cyberspace. Internet rules and conventions are intended to anticipate certain types of behavior among Web users. For this reason, dictionaries on Internet etiquette ("Netiquette") abound in libraries and bookshops. Cyberterrorists know this. Since communication on the Internet is anonymous, this will be an advantage to them.

Besides, social interactions in cyberspace – as in any other natural environment – are always evolving. This evolution can be lengthy. The main objective of the social engineer is to convince the victim that he or she is an individual that they can trust with vital information that the victim will give them. In order to do so, social engineers will seduce their target through a succession of pleasant exchanges, sometimes over an extended period of time (as the participant demonstrates it in this last excerpt, "they [cyberterrorists] get a little piece of the pie and they build on the blocks"). The easiest way for social engineers to earn trust is to be patient, get that "little piece of the pie," and not ask suspicious questions. Social engineers who request sensitive information too quickly will be less successful than those who do not ask such suspicious questions. Hence, social engineers initiate a series of chats to obtain chunks of information at a time.

They will normally start by asking simple questions that look insignificant to the attacked. Such social interactions not only build trust between the victim and the cyber attacker; they also maintain the appearance of comfortable relationships. It can start with a simple conversation, for instance in a chat room. The chat room is used by cyberterrorists as a hub, a sort of central location in the network (Scott, 2004) where they can develop social interactions with victims-to-be. Essentially, cyberterrorists make cyberspace more user-friendly and receptive to their needs.

The next excerpt makes obvious that the simplest and most popular means of social engineering is still human based. It can involve intense interpersonal communication and deception, using tactics such as pretense, impersonation, or masquerade. As the participant – the same cyber forensics expert from the Midwest mentioned earlier – recounts,

> cyberterrorists engage in social engineering more than we think we know because they are so good at it. They show up at Joe's company and pretend to be network administrators or "repairmen." How do you know if someone is a legitimate person or not? For years, we have trained customer service people to be nice, to be helpful. It's perfect for a cyberterrorist.

Using the tools of the trade such as asserting authority (i.e., pretending to be "network administrators"), they appear as legitimate individuals. As Vijayan (2005) continues the argument, social engineers will sometimes study the structure of a target organization so that they can be able to drop names of important employees in an attempt to gain credibility. Ultimately, it is no surprise that social engineers appear as legitimate persons. What the participant – cyber forensics expert – also reaches out to us is that

social engineering applies to the act of face-to-face manipulation in order to gain physical access to computer systems (i.e., "They show up at Joe's company…"). Even face-to-face communication between individuals can be exploited; all it takes is to be a good liar (Denning, 2000). For the purpose of this analysis, a social engineer is, in essence, a liar, a con artist, a deceiver, and a manipulator. The following excerpt highlights the weakest link in a social network: the human. This short section was lifted from the transcription of an interview conducted with the associate head of a technology lab at a Midwestern university. As the participant recounts,

> because we have passwords, anti-virus programs, and the like, the weakest link may be the operator, the one you give a box of chocolates to. Social engineering means getting around the system through bribery or seduction, the art of being a con man.

Social engineering is a practice that can be used to exploit what has long been considered the weakest link in the security chain of an organization – the human factor. From that participant's account, the weakest link is the human (here, "the operator"). Because of this, social engineering is one of the cyberterrorist's cleverest manipulations of the human tendency to be gullible or reliable. When the cyberterrorist develops trust with a user or befriends them, he or she is going to find it easier to talk them into what they want (Rohan & Donaldson, 2002). The literature even reports that, in some cases, cyberterrorists build trust with naïve users for weeks or even months (Mitnick & Simon, 2002). So, the first objective is to establish trust. How can it be done? As this participant puts it, one gives "a box of chocolates" to the operator. The skilled social engineer is a wolf in sheep's clothing. As an evil manipulator, he or she acquires information very

slowly, doing small favors, and then, in turn, asks the victim for small favors ("through bribery or seduction") or obtains information by means of outwardly innocent conversations.

Kevin Mitnick explains it well. In the corporate world, employers are unlikely to assess a request thoroughly, so they take a mental shortcut (Mitnick & Simon, 2002). The reasoning follows that if a person calls an employee who is willing to help them solve a problem, that employee is on that person's side and means no harm to them. By this method, cyberterrorists take advantage of the natural tendency of a human to trust their words or deeds (i.e., a box of chocolates), rather than solely exploiting computer security holes. Oddly enough, network administrators such as the operator mentioned in this last excerpt do not need to know the password of users. If they are ever asked for their password, it is always a social engineering attack. Yet, from the participants' accounts, even operators fall into a trap. There is a well-recognized rule in social interactions that if someone gives someone else something or promises them something, that "someone else" should return the favor. This tends to be true even if the original gift was not requested or even if what is requested in return is far more valuable than what was originally given. This truth is known as "reciprocation" (Sagarin et al., 2002).

What social engineering reveals is not just blind trust in strangers, but also human ignorance. From the accounts that are being told, social engineering relies on human incapacity to keep up with a culture that relies greatly on information technology. Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. Lack of security awareness and lack of knowledge of information technology on the part of computer users make any computer

user the weakest link in the security chain, threatening the whole network. In other words, based on social network theory, when one node (i.e., secretary) in the network gives valuable information to a cyberterrorist, that node has become a hub because that node has become important to the cyberterrorist. Indeed, that node gave the cyber attacker vital information that they needed: password, ID, security information, and the like. As a result, the node-turned-into-hub can cause the network to be very vulnerable, leading to its destruction.

Figure 7 (on the next page) shows a graph that represents an all-channel network (Leavitt, 1951) where, at the beginning, there are no hubs; there are just nodes. In this typical all-channel network, every actor can be connected to every other actor in the network; there is no central point that is at the hub or core of different connections, otherwise this type of network would be called the "star" or "wheel" network (Bavelas, 1950). Up to the point where the social engineer attacks one of the nodes by manipulating them or convincing them to take certain actions that they would normally not do, there is no "most prominent" individual (i.e., actor, node) standing at the center of the network or having influence on their environment (i.e., in terms of decision-making, etc.). In other words, according to social network theory, no node represents a point that is said to be *locally* central because it has no larger "number of connections in its immediate environment" (Scott, 2004, p. 82). However, when the cyberterrorist/social engineer exploits one node, that is, when the attacker has him or her give them vital information such as password, ID, or security data, the node (Node 4 in the graph) turns into a hub and, hence, becomes a vital actor whose blind and ignorant actions can jeopardize the entire network. The other three nodes are meaningless to the cyberterrorist/social

engineer. They are merely drops in the ocean. The hub, however, is a big ocean in itself. This is the scary part.

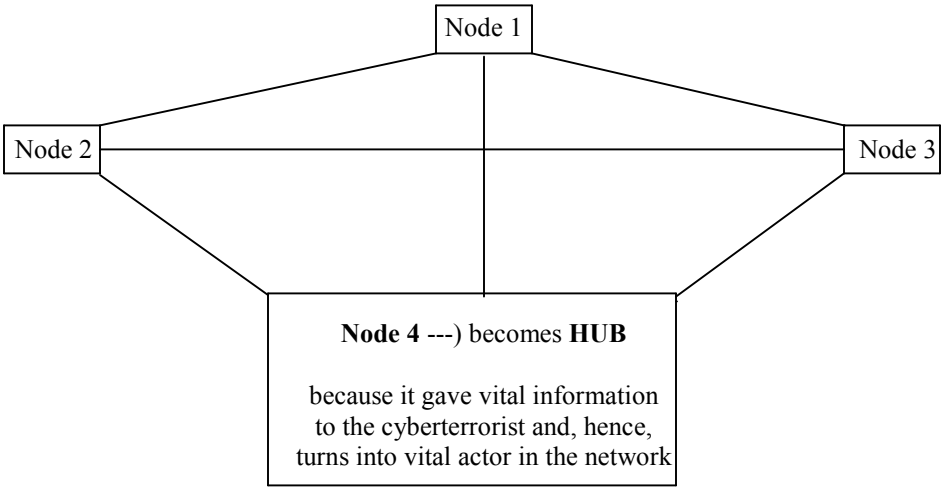

Figure 7 *Example of four nodes composing an all-channel network. One node can turn into a hub (e.g., Node 4) if the information they give is vital to the cyberterrorist.*

Yes, now we have it: the exploitation of a single node by turning it into a hub. Now, the social engineer can take control of a network and, ultimately, wreak havoc. The main conclusion is that social engineering attacks against single nodes are personal. Cyberterrorists are aware that humans are regularly the weakest links in a security system. They are susceptible to fraud and deceit; their reactions can give intruders many opportunities for success. Besides, social engineering can be a great danger because the attacks do not have to be directed against everyone; a single node can provide enough information to the enemy so that it can affect the entire network. It only takes *one* gullible user to make a social engineering attack successful. As a result, it is legitimate to say that

users are the weakest links in a chain of security. The last excerpt, from a former FBI agent who became a professor, is a specific example of social engineering via email:

> I'll give you an example of social engineering. Sometimes, you get an email that is kind of a pleasant surprise: "Look at the file I sent you, it's really cool." It's an executable file that you put on your computer and you find out that it's a virus. That's social engineering.

In this example, cyberterrorists use social engineering strategies to manipulate any Web user who has an email address. The social engineer will load enthralling e-mails (i.e., "Look at the file I sent you, it's really cool") with viruses. In a similar fashion, Mitnick and Simon (2005) report that social engineers send emails with subject lines like "I Love You," which end up in hundreds of thousands of email boxes, destroying email servers and, in some cases, wreaking havoc on information services. Another present-day example of a social engineering attack that uses innocent-looking email attachments as "cyber" weapons is the attack that uses email attachments filled with malicious payloads (i.e., massive quantities of spam). Many users, unfortunately, tend to blindly click on such attachments, thus allowing the attack to work. This really demonstrates to us that social engineering is a combination of gullibility and curiosity. Numerous people tend to want to see what they should not want to see.

Let us focus on a previous example. A few participants mentioned that cyberterrorists use social engineering skills, sometimes for long periods of time, in order to obtain the passwords of their victims. The colossal danger is not only that Web users give their passwords to cyberterrorists, but also the fact that many Web users often repeat the use of one simple password on every account: hotmail.com, yahoo.com, and so on.

As a result, once the cyberterrorist has one password, he or she can probably have access to multiple accounts. In line with these contentions, one way in which social engineers have been known to get hold of passwords is through online forms for web users to fill in. More precisely, social engineers send out some type of sweepstakes information and request the user to write their name, including email address; that way, they might even give their company account password in the process (Mitnick & Simon, 2002).

In another instance, a pop-up window tells the web user that their network connection has been lost and that they need to re-enter their user name and password to reconnect. In doing so, the information is sent to a remote site by a program that the social engineer has installed. Similarly, a cyberterrorist writes a program that asks for usernames and passwords in exchange for a "grand prize" (Flynn, 2003). This is a throwback to the previous comment made by the associate head of a technology lab at a Midwestern university that the weakest link in the computer network system is "the one you give a box of chocolates to." The box of chocolates here is the "grand prize." Those usernames and passwords can be sent to the target by email and be programmed to be sent back to a location to which the cyberterrorist has access. What these three last paragraphs have discussed is a form of nefarious activity using social engineering techniques called "phishing" (Borja, 2006; Sparks, 2005), as commented by the participant in the following excerpt:

> People fall prey to phishing scams all the time, even those who hold a Ph.D. and other brilliant folks. I ask them, "If someone came to your door in person and told you that story, would you believe them?" They would say no. "Then, why did you

believe them when they came to your computer door?" "Well, it was over the Internet and they looked believable."

The term "phishing" stems from the use of increasingly sophisticated manipulations to "fish" for victims' information and passwords (James, 2005). Phishing is characterized by what has been explained so far: efforts to maliciously acquire sensitive information such as passwords, masquerading as a trustworthy person or network administrator, and even building up trust, via chat rooms and the like, in an apparently innocent means of electronic communication (Lininger & Vines, 2005). Phishing is a social engineering technique that is so successful that "even those who hold a Ph.D. and other brillian folks" fall prey to it. The reason is that, on the Internet, it looks more "believable." What this means is that Web users from all layers of society, from the low, uneducated to the high, very educated ones, can be victims of cyberterrorism and social engineering. Phishing also implies a technique known as "reverse social engineering," as commented by an IT analyst in the Southwest:

> Sometimes, you have the problem of reverse social engineering. So, you have a situation where a cyberterrorist is helping you fix a computer security problem that he has himself sabotaged. Basically, he will attack a Web site in some way and then list himself as a person of authority, you know, like an administrator. Then, he'll tell you to contact him to fix your security problem. So, you're gonna do that, you'll give him information he needs, and he's gonna give you far more problems.

From what has been said here, the cyberterrorist sabotages a network, causing a problem arise, then advertises that he or she is the appropriate contact (i.e., "a person of

authority, you know, like an administrator") to fix the problem. When the cyberterrorist proceeds to fix the network problem, he or she asks for additional vital information from the victim and gets what was intended initially. What is really frightening is that the victim never knows the "problem-solver" is a cyberterrorist because, from the outward appearance, the network problem goes away and "everyone is happy." Imagine what happens next, the cyberterrorist is perceived as a hero and has even gained the confidence and trust of the target. Truly, reverse social engineering is even a sneakier method of social engineering because not only does the cyberterrorist get their victims to ask them questions instead of questioning them, but, also, the target feels indebted to the cyberterrorist even before the cyberterrorist resolves the security problem.

To sum it all up, let us compare the main differences between social engineering and reverse social engineering. While in social engineering, the user has to provide information to the cyberterrorists so that he or she can have control over the security network, reverse social engineering implies that the cyberterrorist already has some control over the network, but will obtain even more information from the user by pretending he or she is a person of authority (i.e., network administrator). The ultimate goal is to have even more, if not total, control of the security network. By the same token, while social engineering requires little or "some" preparation for the strategy to be successful, reverse social engineering necessitates significant planning and previous access to a security network. In fact, as Mitnick and Simon (2002) put it, reverse social engineers have to do a lot of planning to make their cyberterrorist acts successful. They must already have some control over the network. Finally, the last difference is that, with

reverse social engineering, victims ask the cyberterrorist questions, rather than vice-versa. In both cases, however, online interaction is needed.

To conclude this section describing the theme of social engineering that emerged in many of the accounts, it appears that all security networks and other information systems across the globe rely on humans who have the vulnerable characteristic of being the weakest link in the chain of security. Social engineering is an ideal situation for the cyberterrorist because humans are generally trusting. Indeed, there is a natural willingness for humans to accept anybody, even an outsider, at their word, possibly leaving many humans vulnerable to harmful attacks. No matter how secure the equipment is from e-invasion, the information extracted from a legitimate user may make a computer network inoperable if used in a "deadly" manner. Let us not forget that social engineers use social skills and human interaction. They instigate a series of conversations to obtain bits of information at a time. They start by asking basic questions that look innocuous to the attacked. This type of communication not only builds trust between the target and the cyber attacker; it also preserves the appearance of a comfortable relationship. It can start with a simple chat, for instance in a chat room.

As we can see, social engineering is a malicious combination of tactics and psychological hoaxes used by cyberterrorists on Web users in order to access computer systems or networks. In addition to the methods discussed so far, usually termed "phishing," cyberterrorists use another method called "reverse social engineering," where they try to learn how to manipulate legitimate users into asking valuable network information so that those users become totally dependent on the social engineer, and not vice versa. The reverse social engineer can even gain further access to the security

network, hence having total control of the network. The consequences could be devastating: for the network involved, for other networks that depend on that network, even for an entire city or county. Accounts could be lost, sensitive information could be compromised, and even reputation could take a toll.

Beyond doubt, social engineering can be a very effective and dangerous method for cyberterrorists to hurt both information and infrastructure. Social engineering is unlike any other threat to the security of a network. It can circumvent the computer technologies put into place to protect and spot malicious acts or attempts. It is a threat that is as old as civilization, that still exists, and that will always exist, because, as we now know it, the weakest link in a network is not the anti-virus software, the thorough patching, the firewall, or the intrusion detection system; the weakest link is the human, the user. It only takes one unaware employee to make a social engineering attack successful, and as a result makes employees the weakest link to a security policy. With the proper training, and policies in place, the risk of social engineering can be effectively mitigated. It only takes *one* gullible user – yes, *one* single node in the network – to make a social engineering attack successful. Consequently, it makes users the weakest links in a chain of security.

Know Thy Enemy

The third theme of this analysis is "know thy enemy." Four interview excerpts were selected to illustrate that "know thy enemy" is a saying that might sound a little obsolete, but, according to the participants, it is a good approach for both cyberterrorists and law enforcement to understand one another and, ultimately, improve their fight against each other. "Know thy enemy" implies "think like the enemy." This rule follows

naturally from the complex nature of computer security. The first excerpt, selected from an account told by a computer forensics examiner and assistant professor at a Midwestern university, shows that information gathering is still widely practiced as a method to know the opponent:

> Networking against others all comes down to intelligence gathering. We know they [cyberterrorists] are trying to gather intelligence on us and they know we are trying to gather intelligence on them. It's just a game back and forth, just like street informants and cops.

From this excerpt, it follows that the theme of "know thy enemy" applies to both law enforcement and cyberterrorist activities ("We know they [cyberterrorists] are trying to gather intelligence on us and they know we are trying to gather intelligence on them"). So, both sides engage in intelligence gathering in order to better understand their opponent and, ultimately, defeat them. Fixmer (2000) notes that law enforcement agents use all kinds of intelligence-gathering tactics used to monitor everything a cyberterrorist suspect types on their computer. Likewise, cyberterrorists from any country and culture know a lot about law enforcement activities, even in cyberspace, which might give them a leg up on how to defeat or fool law enforcement. Part of the reason is that law enforcement officials – voluntarily or involuntarily – share information with cyberterrorists. Cyberterrorists see the new software programs and read professional journals on new technology releases (Neighly, 2000). Some enroll in American universities; this gives them a great idea of what cyber forensics experts do, what decisions will be taken in the future, and even the reasons for making these decisions. All

this boils down to saying that cyberterrorists can base their actions on what they have learned from their enemies.

The next excerpt was selected from an interview conducted with a cyber forensics expert who has spent the last fifteen years tracking cyberterrorists. Holding a doctorate in computer forensics, the participant lives by the idea that in order to understand one's enemy, one has to know them:

> Know thy enemy. It's a simple military strategy. It's the number one condition in the U.S. military handbook. Sun Tzu said the same thing. When you go to war, know whom you are dealing with. In a cyberterrorist situation, how do you know your enemy? You have to know their network, find their weak spots. Pretend you're the tech guy.

As pointed out in this excerpt, Sun Tzu (2003) already said that one cannot defeat one's enemy if one does not know how the enemy operates and why the enemy does so. What this means is that both cyber forensics experts and law enforcement officials have to outwit their enemies and stand in their shoes because ignorance is no bliss when it comes to fighting cyberterrorists. Besides, they must understand more about cyberterrorists' networks to be able to identify their weaknesses. How can it be done? According to the participant, one has to "to know their network, find their weak spots" and to pretend that one is a "tech guy." The following excerpt was selected from the chair of a cyber forensics program, who is also an associate professor in computer and information technology. This participant makes comments on how to know the enemy better:

> Know your enemy: go after the cyberterrorist group, infiltrate the group, pretend that you are a hacker, and that you have all these skills and you go in and join their group. There are those people who are undercover, those agents that do go out and try to penetrate the group, figure out their command and control structure, and try to knock them out that way. Find out where they are. The difficulty is that, because of the Internet, cyberterrorists come from everywhere. They also have different cultures and motives.

A relevant word that emerges in those two excerpts is the word "pretend." To know one's enemy is to "pretend" that one is "one of them." As the participant suggests, one has to go "after the cyberterrorist group," to "infiltrate" it, and pretend that one has those "skills" to "join their group." This understanding of one's enemy was part of the analysis of the accounts based on game theory (see previous chapter). The problem, says the participant, is that it is difficult for law enforcement to "find out where they are" because "cyberterrorists come from everywhere" and "they also have different cultures and motives." An important analogy can be made here. When George Patton fought against Germany, he could make the claim that he knew much about his enemy because the main European enemy in WWII was a Western Nation, being geographically located in Western Europe, sharing a similar cultural heritage, and adopting similar strategies in warfare. However, cyberterrorists come from everywhere; China, Singapore, Brazil, and so on. They can wage attacks, with a simple mouse click, from a laptop computer in the middle of Siberia. Because they come from everywhere, cyberterrorists might come from different cultures and have unknown motives (Jordan, 1999). Behind their cyber attacks lie cultural backgrounds and underlying motives that even George Patton – if he were

alive today – could not decipher. For this reason, law enforcement agents have to find new ways to know their enemies. The next excerpt, taken from an interview with a security analyst in a Midwestern university, is a suggestion on how to better understand the enemy:

> In order to understand and fend against cyberterrorists, our technology has to be at the same level as the technology of the people who are doing it. This goes without saying, but it has been very difficult for law enforcement. It has to become much of an arms' race. They have to keep up with technology every day.

This excerpt focuses more on technology itself rather than tactics and techniques to penetrate cyberterrorist networks. As revealed in the accounts described in previous sections, what law enforcement officials have attempted to do is maintain a team of highly trained specialists who can analyze the history, motives, and actions of every potential cyberterrorist network. Yet, as pointed out in this last excerpt, it is "very difficult" for law enforcement officials "to keep up with technology" on a daily basis and, ultimately, to keep up with their enemies. Only when law enforcement agents have the technology that meets the cyberterrorists' level will those agents better know them. Only then will the fight against malicious hackers be useful. The literature shows that cyberspace is a winner-take-it-all system (Dunnigan, 2003). With knowledge superiority and the latest computer technologies, law enforcement agents expect to shape cyberspace to their advantage – in fact, they want cyberspace to give them that asymmetric edge – but cyberspace levels the playing field rather than tilting it in their favor (MacNulty, 1999).

The concept of cyberspace, with its high-tech battlefield, is truly a conflict between adversaries who are very well matched in terms of computer technology (MacNulty, 1999). Indeed, both opponents always keep their software programs up-to-date. The concept of playing field mentioned previously is postmodern because it may be fundamentally altered by information technologies, both from strategic and tactical standpoints. The increasing breadth and depth of cyberspace has created a playing field to the point at which dominance [in cyber conflict] alone may now generate consistent war-winning advantages to able practitioners. Therefore, collecting information on the enemy (and making sure that they do not collect information about law enforcement) is crucial. Law enforcement must be able to understand how software programs can be used to better understand cyberterrorists' intentions.

The Enemy of My Enemy Is My Friend

Human history abounds with unexpected alliances of previous enemies joining forces to defeat a common enemy, whether they call it imperialists or religious infidels. In Antiquity, for instance, Constantine sought total political unification of the Roman Empire. In order to achieve his goal, he proceeded to unify the various religious, ethnic, and linguistic groups that lived under Roman rule, but that had long been fighting with each other. Constantine accomplished his objective by inculcating in Roman citizens a common sense of brotherhood, namely by identifying common enemies of the Roman state (Leadbetter, 2002). Likewise, in 19th-century America, many Indian tribes that had long been waging war with each other joined forces in order to stop the slaughter of the "invaders" and regain the land all over the Plains. Those tribes came together to fight a common enemy. The Kiowa, Comanche, Arapaho, and Cheyenne were among the tribes

that participated in combined raids in an attempt to put an end to the invasion to the land (Malinowski, 1998). These two historical cases exemplify that "the enemy of my enemy is my friend."

Even in cyberspace "the enemy of my enemy" can be "my friend." The formation of a common cause among cyberterrorists is sometimes strengthened by the identification of a common enemy or group of enemies. Among these enemies are anything and anyone perceived as prohibiting access (including secret source codes) as well as mechanisms that promote dependence. Major corporations and federal agencies are identified as common enemies (Lehmann, 2004). Likewise, there is increasing evidence that individual Islamic cyberterrorist groups that have been traditionally fighting are now banding together and becoming interlinked through a shared pro-Islamic agenda (Hosenball, 2002). Each networked group wages cyber attacks under a common banner, that is, to fight against Israel and the United States. In another example, for the past few years, the Zapatistas have had an interconnected network of Web sites where groups have been progressively learning to network as they have realized they have common enemies (Elison, 2000; Martinez-Torres, 2001).

These facts illustrate that, even with regard to the Internet and cyberterrorism, the phenomenon of the "enemy of my enemy is my friend" is very real. This theme is analyzed and interpreted based on selected excerpts from interviews conducted with experts in cyber forensics. The first excerpt of this theme was selected from an interview conducted with a supervisor in a computer forensics unit who used to work for a state branch of the FBI as a cyber investigator. For the past four or five years, he has been involved in computer crime and computer forensics. His account is enlightening:

> Maybe cyberterrorists groups aren't all tight-knit groups or like each other, but there sometimes is this alliance that has the same cause to deface others' web sites or even to cause more havoc. And there are cyberterrorists on the Web with specific mission statements. It may be that they don't even know each other and they don't even know their real name, but they've met on the Internet. They both have a common enemy, so to speak.

This excerpt is analyzed thoroughly. The first important element of this excerpt is that, according to our participant, cyberterrorist groups that are not "tight-knit" can still form an "alliance that has the same cause." The phenomenon of "the enemy of my enemy is my friend" is applied here in the context of common-goal networks. Unlike a network of trust that is based on blood, kinship ties, or bonding, a common-goal network is composed of groups that do not necessarily have the same structure, culture, philosophy, or core purpose, but that form as communities of practice because of a common goal, usually based on a same enemy or target (Brown & Duguid, 2000). Drawing from elements of social network theory, the nodes in the network are not tight-knit. Instead, these nodes are loosely affiliated actors who display emergent properties as they join forces, execute a task, and then disband. This notion of loose affiliated groups is not to be taken for granted. Some major acts of cyberterrorism are perpetrated by those common-goal groups that network for a certain period of time before departing from one another. In this context, they collaborate because, as the participant says, they "have a common enemy, so to speak." They have nothing in common, apart from their common enemy. In the information age, this has become part of what Arquilla and Ronfeldt (1996; 2001) call "netwar design." Network design is a pattern of communication and synchronization

among totally distinct organizations that join forces on behalf of their common goal (Arquilla & Ronfeldt, 1996; 2001). This pattern fits within the standard model of social network theory; nodes converge gradually into a "relationship" circle, then disband, but survive on their own by self-organizing in their respective environment.

Second, this type of synergistic cyberterrorism based on a common enemy is developed by not only independent or ad-hoc groups, but also by networks of ill-defined and constantly shifting groups (Fulghum, 2005). They come together to plan and carry out a single mission before completely disbanding. Not only do these groups not necessarily fight for the same cause, but, also, they might be unbeknownst to each other (as the participant says, "it may be that they don't even know each other"). The literature reveals that the Internet can be used in such a way that the structure of cyberterrorist networks allows some groups to communicate with each other while they do not even know one another (McClure & Scambray, 1999). They just join forces when they find it necessary or when they have a common enemy. They act like sleeper cells that are located in various locations, maybe Colorado or the Philippines, and that communicate "in the dark" (Arquilla & Ronfeldt, 2001). They operate in a harmonized fashion without their members meeting face to face (Kerbs, 2001). However, some of these groups are enemies towards each other. They have been for years (Verton, 2002a). They sometimes come to realize, though, that they have a common enemy. For this reason, through the Internet, these groups will act conjointly across great distances.

Third, our participant says that not all cyberterrorist groups "like each other," but they can also have a common enemy. So, they will create an alliance "to deface others' web sites or even to cause more havoc." When enemies have a common enemy, it is

enough to sustain an alliance. Two concise real-life examples illustrate this phenomenon. At the end of the 1980s, a cyberterrorist named Lex Luthor, his online name, founded Legion of Doom, a cyberterrorist group. Two members of this group got into a feud. Phiber Optik, one of these two members, left and created a rival cyberterrorist group named Masters of Deception (Verton, 2002a). Later, it was found that the two cyberterrorist groups reconciled after they discovered that they had a common enemy: U.S. agencies of various kinds (Verton, 2002a). In a similar fashion, a couple of years ago, a cyber war broke out between web users responsible for launching different computer worms. The creators of these malicious programs started to send each other viruses. As it turned out, the fight between the different virus writing groups escalated (www.news.bbc.co.uk). Cyber forensics experts said that the groups behind the viruses appeared to have had different motives. In all cases, the intent was on enrolling infected computers into a network of remotely controllable PCs so that they could be used to forward viruses or act as a launch pad for other viruses. More importantly, it has been found that, recently, those former enemies joined forces against anti-virus companies in order to cripple them; they had resolved their long-time conflict by targeting a common enemy (www.news.bbc.co.uk).

So, as we can see, it is sometimes the case that cyberterrorists resolve their quarrels by creating a team that fights against a common enemy. Cyberterrorism truly makes strange bedfellows, that is, individuals who find themselves together against a common enemy, but who would not normally work together or even communicate with each other (Levy, 2001). The following excerpt, from the same participant, emphasizes

the easiness of joining forces against enemies thanks to the anonymity allowed by the Internet:

> It's this cooperative play, this chess, this partnering, this "enemy of my enemy is my friend." On the Internet, thanks to anonymity, there are more opportunities for interactions and development of cyber programs against common enemies. Anonymity also allows you to reduce the threat of your mission to be compromised.

The Internet, our participant says, facilitates "this cooperative play, this chess, this partnering." In other words, it is a forum for binding people together in allegiance against a common enemy ("interactions and development of cyber programs against common enemies") and who may never meet each other (what our participant calls "anonymity"). As mentioned earlier, cyberterrorism has a distinctive structure that enables networks of independent individuals to operate in complete anonymity. Anonymity, as it turns out, "also allows you to reduce the threat of your mission to be compromised." By the same token, this method of action means that it is very difficult for law enforcement agents or cyber forensics experts to penetrate these networks as they are anonymous (Donath, 1999). So, because of all those "opportunities for interactions and development of cyber programs against common enemies," common enemies, then, make for common friends. The next excerpt, selected by an IT Analyst II (or assistant analyst in computer forensics), highlights other concepts that, in the social sciences, would be referred to as legitimation, "alliance vs. amity," and "in-group vs. out-group."

> Sometimes cyberterrorists see that they're really rather alike, compared to other folks that are not into the hacking thing. Some of them don't respect each other,

usually because of jealously and distrust. But what they will agree on is to agree on a common enemy that they can blame for all kinds of stuff. They will legitimate their cyber attacks based on that.

This is an interesting excerpt in the sense that it is obvious that one must not confuse amity with alliance. Based on the statement, "Some of them don't respect each other, usually because of jealously and distrust," it can be inferred that there is certainly not always amity among cyberterrorists. Instead, if they "agree on a common enemy," it is more of an alliance. While they may gain some satisfaction for being alike ("cyberterrorists see that they're really rather alike"), while others are different ("compared to other folks that are not into the hacking thing"), nothing makes their communal heart stronger than being united against a common enemy and blame them "for all kinds of stuff." What the concept of blame also means here is that when they have no enemies, they can create them. Indeed, their alliance involves the creation of easy targets because "they can blame" them "for all kinds of stuff."

In philosophy and international law, common enemies are sometimes referred as *hostes humani generis*, or enemies of humankind (Alfert, Jr., 1992). If a network of cyberterrorists feels burdened with *hostes humani generis* (that is, the "rest of the world," cyber forensics experts, their opponents, and all the ones to be blamed "for all kinds of stuff"), they will legitimize their cyber attacks. In other words, they will feel they have an obligation to use all reasonable resources to target their enemies (Bialke, 2004). This legitimation is explained in terms of the cyber weapons that they use, the rules of their game, their vision of the common good, and, above all, the formation of a common

enemy (Eisenstadt, 1996). For this reason, says the participant, "they will legitimate their cyber attacks."

Lehmann (2004) claims that, in the early days of computing, such collective identity was already underpinned by shared practices. Our participant expresses the same view when he says that "cyberterrorists see that they're really rather alike." This might account for how they form socially in certain circumstances, one of which is the recognition of a common enemy (more precisely, "a common enemy that they can blame for all kinds of stuff"). The term "social formation" here refers to the types of social connections between Web users (Wellman, 2005) and exists only when people are united by a common cause (Strauss, 1978). This alliance makes obvious that cyberterrorists sometimes like to have a collective self-image, based on that common enemy. That self-image, in turn, forms the boundary line, separating "us" from "them." This boundary is sustained by a set of practices, that is, what the in-group members [cyberterrorists] do and what the outsiders do not do (i.e., the "other folks that are not into the hacking thing") (Lehmann, 2004).

In line with these contentions, in order for cyberterrorists to feel themselves to be members of a group, there must be nonmembers who, in the eyes of cyberterrorists, represent the dark side (i.e., those who can be blamed "for all kinds of stuff"). In this sense, cyberterrorists' self-representation exemplifies some of the tenets of social identity theory (SIT). SIT is based on the comparisons that people make between in-groups (groups to which a person feels he or she belongs) and out-groups (groups to which a person feels he or she does not belong) (West & Turner, 2000). Tajfel (1978) created SIT to emphasize that individuals express a desire to compare themselves with others, find a

new meaning about their own identities, and, to some extent, think highly of themselves. It is sometimes the case that one plays up the qualities of his or her own group and denigrates the attributes of others to make the common enemy look darker and the common goal more definite (Monteith & Winters, 2002). From this vantage point, the perception of cyberterrorists that they belong to a particular world (i.e., that of cyberspace, systems invasion, network destruction, etc.) and that others belong to other groups (i.e., the "rest of the world," cyber forensics experts, their opponents, and so on) is sufficient to create common enemies. This bias is based on their [cyberterrorists'] need for collective definition, mission statement, and fundamental purposes. It is their human recognition of a common plight, as described in Marxist theory (Edwords, 2005). All in all, as social identity theory shows that people will legitimate or rationalize their collective effort for the "common good" (Strauss, 1982), cyberterrorists get tied together by a common enemy, be it a hundred thousand computers on the West Coast or Microsoft.

The next two excerpts fall very much under this theme, but, this time, it is the role of law enforcement in their social formation of friends and enemies that is analyzed. The excerpt below was taken from an interview conducted with a former FBI agent and specialist in computer forensics:

> Between law enforcement agencies, historically, there has been jealousy and fighting. So collaboration has not always been good. But when it comes to fighting a common enemy, those agencies collaborate. With the case of hacking and cyberterrorism, collaboration has even been done at the international level.

From this excerpt, two important inferences can be drawn here. First, historically, between law enforcement agencies there have been feuds ("jealousy and fighting"). Second, "when it comes to fighting a common enemy, those agencies collaborate." And it is applicable to the case of fighting against hackers and cyberterrorists. The literature shows that there have been many feuds among agencies. At the local level, Smith (1997) remarks that there are feuds between police departments and district attorneys' offices in several states. Likewise, law enforcement officials in New York City claim there was a public fight between the NYPD and Port Authority Police Department over policies regarding major airports (Rashbaum, 2001). At the national level, two of the most important federal agencies, the CIA and the FBI, of which some of the members participated in this study, have been fist-fighting for more than six decades, to the point of stealing one another's missions or revealing cover-ups (Riebling, 2002). The FBI has been accused of exploiting the political weakness of the CIA. This feud goes back to 1947, when President Hoover opposed the creation of the CIA. In the 1940s, when the CIA was created to organize the U.S. response to the new threat of global communism, it was excluded from operating inside the United States. Instead, it received exclusive responsibility for intelligence and counter-intelligence overseas. This meant that the FBI had to withdraw many of their agents from posts abroad, which infuriated President Hoover. While the CIA was mostly a cosmopolitan and intellectual elite, the FBI considered itself as equally elite but was composed of commoner personnel (Posner, 2003).

Today, even without those obvious differences, the FBI and the CIA still oppose each other on different mission goals. The CIA is committed to espionage – as well as

cyber espionage – working overseas and outside the limits of U.S. law. Its goal is to collect information and weaken the enemy by any means. The FBI needs the CIA, and vice versa, when it comes to accomplishing certain tasks (Riebling, 2002). This has great implications on this study because not only does the literature tell us that an agency like the FBI needs serious monitoring with regard to computer capabilities (Posner, 2003), but, also, several participants revealed that the FBI is insufficiently trained to understand and, consequently, fight cyberterrorism. For instance, the head of a computer and information technology department at a Midwestern university claims that "the FBI doesn't have the manpower to do computer forensics or computer crime investigation." What this all means is that the FBI needs to collaborate with other agencies in this fight against cyberterrorists. As the previous excerpt tells us, "when it comes to fighting a common enemy, those agencies collaborate. With the case of hacking and cyberterrorism, collaboration has even been done at the international level."

The last excerpt in the analysis of this theme was selected from an enforcer of the law working for a federal agency in the Midwestern part of the United States:

> By collaborative security, I mean all those agencies joining forces to defeat a common stealthy enemy. I mean, agencies privately or publicly work together with each respective security system, so that they can share information about a new cyber attack that is experienced precisely at the moment of attack. The goal is to protect the citizens we serve from the dangers of cyberterrorism.

Based on these statements, when there are common enemies, it is best to fight them together. The emphasis here is not on how agencies, historically, have been fighting with each other, but on how they join forces in order "to defeat a common stealthy

enemy." This excerpt explains how networking defines itself as much as what it opposes (i.e., a "common stealthy enemy" and "cyber attacks") as what it defends ("the citizens we serve from the dangers of cyberterrorism"). It is mobilized as much through opposition to common enemies as by common solidarities and interests ("collaborative security"). Hence, when there is a new cyber attack, all other parties are informed right away so that corrective actions and defensive positions can be taken properly. The state of cyber security is too unsafe to avoid opportunities to build coalitions. For this reason, "agencies privately or publicly work together with each respective security system." That head of an information technology center said in one of the interviews that his "cyber forensics experts are involved in various national and international societies that are looking at various aspects of cyber crime." And they "get calls for help from all over the world." This very much acknowledges the importance of various countries to work together against a common enemy: cyberterrorists.

So, to conclude these last thoughts, it appears, from selected interviews, that, despite some disagreement between key government agencies about how operations should be conducted (Perlmutter, 2000), both the FBI and CIA (as well as other agencies) should keep in mind that they have a common ultimate goal; not only is the goal to defeat the common enemy (as discussed in great lengths), but, also, it is to secure Web users and citizens from the dangers of cyberterrorism. Close coordination among law enforcement agencies can minimize hurdles concerning the handling of cyberterrorism. They share the same enemy; they share the same purpose; and they share the same goal: to protect the world – and the *cyber* world – from the menace of computer attacks.

Chapter VIII

Conclusions, Implications, and Limitations

The first ten pages or so of this chapter are devoted to the conclusion of this study, that is, the analysis of the four research questions. The following pages deal with the implications of this study. The last few pages discuss the limitations of this study.

Conclusions of the Study

The qualitative data produced from the interviews have laid the groundwork for the premises put forth in this study. With respect to the analysis of **RQ1** (What do computer security experts' and law enforcement officials' accounts reveal about networks of cyberterrorists?), the participants' accounts reveal the dangers of cyberterrorism and the similarities and differences it has with other types of intrusion, particularly hacking. While both hacking and cyberterrorism are forms of intrusion, cyberterrorism has the distinguishing characteristic of being deliberate in wreaking havoc or causing harm. A few examples were given to demonstrate the potential threat of cyberterrorism; it could flood a town, harm a power plant, cripple an entire infrastructure, or compromise computer systems. Although hacking could be a good means for threatening computers or make them more vulnerable, attacks through the Internet or against networks or systems need to have a terrorist component in order to be labeled "cyberterrorism." For this reason, the motives of cyberterrorists are the same as those of conventional terrorists. Whereas cyberterrorist motives tend to be political, social, ethnic, religious, or ideological, financial motives for cyberterrorists do not seem to be as prominent as the other motives. More importantly, just like terrorism is primarily a process of communication between terrorists and target audiences (Tuman, 2003), an important goal

of cyberterrorists is to send a powerful signal, whose meaning is intended to frighten and coerce. Cyberterrorism is a semiotic act; it is a message, a symbol, and a new media image. Our society is wrapped up with images, signs, and symbols. Given this, there is a powerful semiotic dimension to cyberterrorism. Without a doubt, it can involve sending images of fear.

The analysis of **RQ1** also consists of analyzing their social networks. Overall, it was found that cyberterrorists tend not to work alone. Rather, they team up with others. Cyberterrorists are nodes in a network of rapidly expanding networks; they can be male or female with an average age of twenty-eight years old. Cyberterrorist networks are so flexible, nimble, and rapid that they can have sub-networks or hybrids. They are also characterized by a decentralized structure that is composed of cells. Given this, cyberterrorists do not communicate or collaborate among each other in traditional hierarchies (as opposed to armies and traditional terrorist organizations). Because of the absence of leadership and the postmodern nature of the Internet, collaboration and communication tend to be horizontal, in an all-channel manner, and anonymous. Part of the analysis of their network is the role of their hubs. Hubs are important nodes in the network of cyberterrorists that have so much potential that they can connect a great number of other nodes [cyberterrorists]. The end-result of the analysis is that any type of network is much stronger when its hubs are active. Three types of hubs are identified in this study: (1) hubs as humans with high degrees of centrality, (2) hubs as go-betweens, and (3) hubs as central locations (the central location being the Internet chat room or IRC).

Of equal relevance in the participants' accounts is that networks of cyberterrorists were found to be communities of practice. As such, a cyberterrorist network constitutes a culture in itself because it has its own distinctive "community of practice" that enables cyberterrorists to create and maintain their networks. It was also found that part of their communities of practice involves a way of life that uses "leet" speak, a jargonized lingo used by cyberterrorists in order to reinforce their culture and avoid detection by law enforcement. Likewise, it was assumed that cyberterrorists tend to be emotional communicators via online media (i.e., the Internet). One participant mentioned the importance of cyberterrorists' knowledge. For him, their knowledge is tacit and embedded knowledge; it is not explicit, but implicit. Along the same lines, cyberterrorists build networks of trust through a method called chaining. From a social network theory perspective, chaining implies following connections from one node to the next (i.e., introducing a friend of a friend). For this reason, it was found that cyberterrorist communities resemble the conspiratorial communities like the Carbonari in Italy and the Freemasons in that they are broken into small cells, which would be nodes in the cyberterrorist world. Finally, the analysis of cyberterrorist networks can be articulated upon the individualism-collectivism dimension as well. Two strong quotes reveal that cyberterrorists tend to be individualistic, even if they are part of a cyberterrorist network and even if they come from collectivistic cultures. Cyberterrorists are also individualistic because they try to protect their private space (for them, privacy is important).

In regard to the analysis of **RQ2** (What do computer security experts' and law enforcement officials' accounts reveal about their own networks?), the participants' accounts begin by demonstrating that it takes networks to fight networks. As such, it was

found that it is necessary to combine efforts, through networking, in order to fight, let alone understand, cyberterrorist networks. In the same way that cyberterrorists collaborate worldwide thanks to the rapid evolution of global electronic networks and anonymity on the Internet, law enforcement agencies also collaborate at the global level. Because cyberterrorism incidents can go past regional, state, and even international jurisdictional boundaries, to the point where traditional jurisdictions and boundaries are no longer valid, American federal agencies feel the need to network with foreign agencies that would be willing to track the identified cyberterrorists and prosecute them. Overall, cyberterrorists' and the law enforcement's networks are largely similar, but they also have a few differences. For instance, while some law enforcement agencies model a social network design where interagency connections are done in an all-channel manner (just like cyberterrorist networks), other law enforcement agencies model a design where there is a jurisdictional hierarchy between them.

In line with these contentions, it was also found, based on the participants' accounts, that it is necessary for law enforcement, in their fight against cyberterrorists, to consult with cyber forensics labs in order to maximize the outcomes of their investigations. Cyber forensics specialists have outstanding computer expertise and superior technical skills. Cyber forensics labs improve investigation into an ever-growing era of crimes that uses computers, computer-aided terrorism, cyberterrorism, and espionage. One of the participants found that "no man is an island," meaning that people cannot be isolated from one another, but they should be interconnected. As such, positive outcomes in the fight against cyberterrorists can only be achieved not by working alone, but by being involved in a social network that relies on a feedback mechanism. Feedback

mechanisms are necessary to maintain stable conditions and achieve a dynamic equilibrium in a network. When there is a continuous feedback mechanism, there is an ongoing flow of communication between humans. As the network seeks to increase its performance, feedback helps the network make essential adjustments.

This analysis of **RQ2** also reveals that participants stress the importance of networks of trust among law enforcement agents. In order to be part of their network, one should have earned their trust beforehand. Just as it is the case for cyberterrorist networks, this practice of using someone whom we know to gain more people in the network is called chaining. In addition, because the cyber forensics community "is still a virtual community," trust is done through "a transitive trust model." The transitive trust model portrays trust as being a two-relationship model between three nodes. So, trust is transitive, that is, transmitted through another party. Based on the main tenets of social network theory, node A validates and trusts node B; node B validates and trusts node C; node A trusts but does not need to validate node C. However, some of the participants' accounts also reveal that there are downsides to networking with others. Although federal agencies have developed networks among each other for the past couple of years, it appears that not all networks can be trustworthy or dependable for keeping information secret. Plus, it is not always possible to know every node. The level of trust decreases under those circumstances. Every time humans network with others, they expose themselves to risks and to others with power over them.

This analysis of **RQ2** also discusses the theory of the strength of weak ties in informal networks of law enforcement agencies. The main benefit is the extreme facility of information flow, that is, the ample diffusion of information among actors in the

network. By having an informal network, by having a grasp on who knows whom and who knows what, law enforcement agents can easily manage their networks because it is assumed that they provide or feed relationships that they see fit. Formal networks are not good for using informants. However, having ties with informants in informal networks can be beneficial for law enforcement agents in that they can flexibly communicate and cooperate with them, as they might possess specialized knowledge and capabilities. Of equal importance is the role of structural holes in those informal networks. For Burt (1992), individuals with whom a person has weak ties are less likely to be connected to one another. In other words, the person is embedded in a structural hole. The structural hole is a knot in the social network that gives access to missing knowledge. Therefore, an individual who is the only one linking a group to another is at a significant advantage. As such, the individual can gain from having access to a different set of information unavailable elsewhere. The participants' accounts also point to the importance of key players in networks of law enforcement agents. From a social network standpoint, hubs are humans with high degrees of centrality in their networks. Just as it is for a cyberterrorist network, any type of network between law enforcement agencies is much stronger when its hubs are active. Therefore, the role of hubs considerably influences how the network operates.

With respect to the analysis of **RQ3** (How can the conflict and interaction between cyberterrorists and computer security experts [and law enforcement officials] be explained through the use of social network theory and game theory?), the participants' accounts reveal that law enforcement agents do not always engage in battle with cyberterrorists. They sometimes try to interact with them in order to obtain more

information about their networks (and vice versa). The more interactive the network, the more open the network, and the more open the network, the more chances to obtain new information and ideas about the enemy than closed networks that have no interaction whatsoever. However, it was also found that the danger of interacting with the enemy is exposing one's network to the enemy. For this reason, law enforcement agents and cyberterrorists do fight with each other as well. Just as cyberterrorists try to target the hubs of their enemies' networks, so do law enforcement agents; they attempt to cripple the big actors in cyberterrorists' networks. Who are these big actors? They are the go-betweens. A chat room is considered a hub by law enforcement agents as they try to target it. The procedure seems to be the same: to approach the enemy (and, by the same token, to know them), to get them, and to destabilize their network.

The second part of the analysis of **RQ3** illustrates the importance of game theory in the understanding of the complexity of the interaction and conflict between cyberterrorists and cyber forensics experts (and law enforcement officials). One excerpt portrays a very good example of a zero-sum game ("Cyberterrorists' victory is based on law enforcement's defeat"). A zero-sum game is a game where, no matter what the outcome of the game is, the victory of one player is exactly balanced by the defeat of the other player. In this conflict between cyberterrorists and law enforcement agents, the cyberterrorist will win only at the expenses of the law enforcement agent, but the benefits and losses to both players amount to the same value. For this reason, it is a zero-sum game. No matter what, the battle is a chess game, where each player does not know what moves the opponent will take. Therefore, each of the players finds a strategy to examine the possible actions of each other in the situation. The ultimate goal is to determine the

best course of action for him- or herself. This chess game played by cyberterrorists and law enforcement agents is a strategies-versus-counterstrategies game where the players who prevail are those who possess the structural advantage. One might think that to disrupt is structurally less difficult than to protect, but an agent can create a situation where the cyberterrorist's defeat equals that of a scorpion killing itself with its sting.

Another example of the conflict between law enforcement agents and cyberterrorists depicts a Nash equilibrium. One of the tenets of the Nash equilibrium is that each player takes his or her opponent's current strategies as given. As such, a player has nothing to gain by changing only his or her own strategy. If a player has selected a tactic and if he or she cannot benefit by changing that tactic, while the other player keeps his or hers unchanged as well, then the current set of tactics and the payoffs that result from the outcome of the game constitute a Nash equilibrium. What gives the Nash equilibrium all its legitimacy is that law enforcement agents use counter-strategies and use the same strategies over and over again. The end-result, or the outcome, is an equilibrium of strategies between the two players. In other words, it is a Nash equilibrium. Both cyberterrorists and law enforcement agents can maximize their outcomes that way. There is no reason to change their strategies in that type of situation.

In line with these arguments, it was also found that the conflict between cyberterrorists and their opponents is an evolutionary game because new methods are constantly invented. The goal of the cyberterrorists is to create tactics and weapons that continually change in an effort to defeat their opponents' networks and systems. If the cyberterrorists lose today, they will not disappear. Rather, they will learn what did not work and use it against their enemies tomorrow. The reason is that there are always

continuous patches and changes in technology. On the part of the cyber forensics experts and law enforcement agents, they will choose the option for the highest expected payoff by having the latest technological measures to protect their networks. It is an evolutionary game because it is based on situations where the players know their own strengths, but they can only estimate their opponents' power (as well as their resources and capabilities) based on the level of their moves (that is, their actions, tactics, and attacks or defensive measures). For this reason, participants see it as a "continuous struggle." If cyber security is a game, then cyberterrorists are the ones who make the rules. Indeed, the game law enforcement agents and cyber forensics experts are involved in has to be played by the standards determined by the cyberterrorists. Cyberterrorists, then, are the ones making the rules. Protective measures like anti-virus software programs and firewalls are measures taken by cyber forensics experts and law enforcement as a reaction to cyberterrorist attacks. When the latter ones launch a new computer virus, the target side has to adapt to it. When the cyberterrorists manage to find a hole in the new adapted technology that has just been used against the virus, the target side has to adapt again. This evolutionary game seems to be an endless match where the target has to play by the cyberterrorists' rules. Moreover, their very rules may change during the game, based on new cyber weapons, new tactics, new tools, all of which can be acquired a few mouse clicks away.

The third part of this analysis of **RQ3** is the intersection of social network theory and game theory. Overall, game theory helps demonstrate the potential for collaborative behavior among distrustful players in the game. It was found that law enforcement agents have a history of collaborating with cyberterrorists, but the collaborative game that those agents play with cyberterrorists is a necessary evil. The collaborative game, in this case,

is not altruistic. It is not a function of empathy, but an awareness that one is in need. In the context of cyberterrorism, it seems that law enforcement agents would take the slightest chance to collaborate with the enemy in order to reach their outcomes. One of the tactics used by law enforcement is to let one node go away in order to catch the whole network of nodes. For instance, law enforcement agents will do a plea bargain with the little fish [a cyberterrorist who got caught] so that they catch the big fish [the entire network]. Given this, the cyberterrorist becomes part of the network of law enforcement agents. Plus, the burden of responsibility is not entirely on the cyberterrorist. This is where the cyberterrorist believes that he or she is not solely responsible for the moves against his or her comrades. In social networks, the selfishness of the users has deeper consequences than in traditional networks because the operation of the network can be based on the cooperation of the nodes against other nodes. Game theory rests on the premise that the players, however cooperative they become, can never be altruistic towards each other because they have ulterior motives. So, there is no intrinsic motivation for them to cooperate. From this vantage point, the way game theory is intersected with social network theory is constructed within a framework of networking with the opposite players (i.e., enemies) without having any intent to establish trust with those players.

Finally, with respect to the analysis of **RQ4** (What are the themes that emerged across the participants' accounts?), four themes were found across the participants' accounts. The "postmodern state of chaos" was the first of these themes. It was about the idea that cyberterrorism has the potential to create a state of immense confusion and disorder far different from what our sensory realism, as we know it in actual physical

space, has ever experienced. “Social engineering” was the second theme. A social engineer is a manipulator of naïve individuals (i.e., Web users). The goal is to gain information from them or gain access to a particular location. The ultimate motive of the social engineer is to have control over a network or system. “Know thy enemy” was the third theme. This theme gives an account of the tactics used by both cyberterrorists and law enforcement to understand the enemy and, by the same token, improve their fight against them. “Know thy enemy” implies the idea of putting oneself in the shoes of one’s opponents. The fourth theme, “the enemy of my enemy is my friend,” rests on the principle that the establishment of a common cause among cyberterrorists is likely if they identify a common enemy or group of enemies. The same applies to law enforcement; history has shows that some federal agencies do not get along. Yet, when they become conscious that they have common enemies, they will join forces and fight them.

Implications of the Study

The implications of this study are considerable. A first implication is that, now, readers have a better understanding of the meaning and impact of cyberterrorism. Based on the analysis of all the four research questions and the findings in this study, we can conclude that cyberterrorists challenge principles and laws that are at the heart of American concepts of liberty, private space, personal rights, and possession. The face of terrorism is evolving. While the motives remain the same, we are increasingly confronting new and unknown weapons. The intelligence systems, counter-attacks, and security procedures that were once created to protect individuals, systems, and countries, are powerless against this postmodern, devastating weapon. Cyberterrorism is postmodern terrorism because it is disorderly. Cyberterrorists use grand strategies

envisaging disorganization of the respective enemy. Against opponents who fight in a postmodern fashion, conventional strategies lead nowhere. The motives for cyberterrorists are that our lives depend immensely on technology. The danger of cyberterrorism is that it has been inadequately considered by many people and leads insufficiently to our shared anxieties.

A second implication of this study is that it is the first to explore – thoroughly, rigorously, and methodologically – the fight between cyberterrorists and law enforcement agents (and cyber forensics experts). One of the supreme goals is to provide a new approach as what law enforcement agents can do to counter cyberterrorism. The fight between cyberterrorists and their enemies seems to be offensive on the cyberterrorist side and preemptive on the law enforcement side. Yet, what will give law enforcement the asymmetric advantage? One answer to such question, for instance, is the "know thy enemy" concept, that is, knowledge superiority. Based on this study, we can say that Sun Tzu was right. Part of what knowledge superiority encompasses is not only being acculturated in the cyberterrorists' world, but also being "bilingual" in their "language." We saw earlier that cyberterrorists' lingo is leet speak. As such, it is not only important to examine and understand their language and dialects (as well as their mode of communication); it is also essential for cyber forensics experts and law enforcement officials to interpret messages such as, "The big event is coming soon" or "The blade will hit again." Recall that cyberterrorists are emotional communicators. So, it is important to be in their shoes.

No matter what, this study has revealed that all the measures taken by various local, federal, and even international agencies indicate an unprecedented commitment

from the anti-cyberterrorism community to galvanize a united front against postmodern reapers of terror. The fight against cyberterrorism is well underway. Participants have emphasized the importance for various agencies to cooperate and share intelligence in ways they have never had before. As such, social networks are necessary. If agencies do not create these networks, who knows what can happen tomorrow if a massive-scale cyberterrorist attack goes through? If social networks of law enforcement agents and cyber forensics experts fail to protect their citizens where the virtual and physical realms converge, then all that will ensue is terror – like one participant expressed it, terror "in ones and zeros." Therefore, the main implication of this dissertation is that this study concerns everybody who lives in a country where infrastructures and networks rely heavily on computers and the Internet. Many quotes from the participants have revealed that the full-blown power of cyberterrorism – whose goal is to wreak greatest havoc around the world – is a possibility that should concern us. We are interconnected. This means that we are vulnerable. Malicious hackers can use it against us. In this respect, the future of terror may come from anybody and from any part of the world.

A third important implication is theoretical and broadens the horizons of research prospects for social network theorists. This study has shown that social network theory can overcome the limitation of both individual-based and structural-based theories. Indeed, social network theory appreciates the interconnections that influence an individual's actions because this individual is part of a social network, whether it is a social network of cyberterrorists or law enforcement agents. Decisions made in a social network do not take place in a vacuum, even in cyberspace. Rather, decisions are made within a context (Musalia, 2005). Thus, as Lin (2001) would argue, the resources

embedded in social networks, especially through the strength of weak ties (Granovetter, 1973), orchestrate both the flow of information and influence on the actors who are linked to those networks. This study has also demonstrated that the social networks of both cyberterrorists and law enforcement agents are very similar; for instance, hubs are as crucial to the interconnectedness of cyberterrorist networks as they are for networks of law enforcement agents (and cyber forensics experts). Yet, their networks also differ on several aspects. For example, some networks of law enforcement agents have some type of hierarchical structure, especially when it comes to making decisions related to a particular case of cyberterrorism. No matter what, it would not be surprising if the Internet, a communication medium with so much power to unite people worldwide, regressed to its origins in the Cold War and became an international battlefield.

A fourth implication is also theoretical and concerns game theorists. This study has brought to light that, despite the fact that law enforcement agents have come to realize that they must possess and ultimately master sophisticated computer technology in order to understand cyberterrorist networks, they should not believe that their fight against cyberterrorists will be fought on their terms. Rather, as participants have described it, the game of cyberterrorism is not fought by the law enforcement agents' rules; the game is evolving and law enforcement agents have to learn from their enemies' weapons and strategies. Law enforcement agents must learn new rules as they fight their opponents; they must create new technologies to protect our systems; and they must learn how to play with new, postmodern players. These findings are very consistent with the contention made by MacNulty (1999) that law enforcement agents must not assume that they automatically understand their enemy's logic or motivations. For this reason, game

theory was applied to this study on cyberterrorism. In part, it emphasized the role of postmodern actors and their evolutionary strategies. As a qualitative tool for the researcher, the strength of game theory is the methodology it offers for structuring and analyzing issues related to strategic moves in cyberspace. This game-theoric approach will, hopefully, enable scholars to further explore these phenomena in a rigorous and consistent manner.

A fifth implication of this study is that it is the first to intersect social network theory and game theory. Game theory can overlap with social network theory because the Internet is a wide-scale network that cannot be managed by one central hub, but by various nodes or hubs that interact with each other and that use all kinds of strategies. Some of these nodes or hubs are cyberterrorists themselves and they are also part of the game. So, game theory provides a sound basis for analyzing social networks. As we have seen, the cooperation of one node in the network can contribute to the success or failure of the operations of that social network. Hence, social network theory and game theory can be intersected. For instance, the operation of a social network can be based on the unconscious cooperation of a private home PC user who is used as a link (man-in-the-middle) between two law enforcement agents. The culprit behind all this is, of course, another node: the cyberterrorist. Law enforcement agents are not aware of the fact that they are being tricked by the cyberterrorist. All this boils down to saying that there is a complex game going on in the network. Likewise, game theory can be intersected with social network theory when there is a situation where opponents collaborate without having any intent to establish trust with those players. There is a game that is being played here.

Limitations of the Study

My work represents an original foray into the world of cyberterrorist networks and the networks of their opponents, a largely uncharted field. Given the exploratory nature of this extensive study, there are some limitations that should be discussed. The first limitation is that the researcher has never been like any of the participants in this study. In other words, the researcher has never been a cyber forensics expert or a law enforcement agent. Had the researcher had experience in a network of law enforcement officials and cyber forensics experts, the conclusions of the study might have been different. By the same token, the accounts told about networks of cyberterrorists are told from a law enforcement and cyber forensics perspective, not a cyberterrorist point of view. Had the participants been cyberterrorists themselves, the results of this study might have been different as well.

A second limitation pertains to the method used in this study: face-to-face interviewing. The twenty-seven interviews might not have extracted typical accounts of what cyberterrorism is and how to fight it. Mishler (1995) observes that "the teller of the tale is also engaged in a retelling. The version we hear or read is shaped both by the context of its telling and the history of earlier retellings" (p. 118). In other words, it is possible that participants alter their accounts for unknown reasons. There is also the risk of distorted interpretations being made by the researcher. Of equal relevance is that the number of participants (n=27) is, at this point in the research, insufficient to fully examine the nature of this study.

A third limitation pertains to the transitive trust model mentioned in the analysis of research question two (**RQ_2**). As such, in cyberspace, the transitive trust model can be

dangerous. Risks including conspiracy and wrong recommendations can be serious threats for those involved in the social network. The notion of "A trusts B; B trusts C; therefore, A can trust that C will be a reliable member of the social network" is too simplistic for network in cyberspace. These connectivity relationships are oftentimes not transitive in real-life situations. In real life, it is regularly the case that "A trusts B; B trusts C; yet, it does not imply that A trusts C." One of the real problems with the postmodern nature of the Internet is that it is so ambiguous.

Chapter IX

Future Directions

This is the last chapter of this dissertation. Future directions are important because they can give scholars valuable suggestions based on the conclusions of this study. This chapter is divided into four subsections. It gives future directions from (1) an organizational communication perspective, (2) an intercultural communication perspective, (3) an international communication perspective, and (4) a law enforcement perspective.

An Organizational Communication Perspective

This study has thoroughly described what social networks of cyberterrorists are and how their opponents create social networks themselves in order to fight those networks. It might be interesting for organizational communication scholars to further explore the structures of social networks that can present more than one design. As such, since the postmodern nature of cyberspace is so ambiguous, could a network be a line (or chain) network and an all-channel network at the same time? It would also prove useful to further examine to what degree a network can blend a multitude of webs of relationships. In order to cope with cyberterrorism from a social network perspective, scholars must first learn what kinds of networks cyberterrorists are involved in and draw upon the best methods for analysis. Besides, how deep are the communication patterns among cyberterrorists in their networks? The same issue could be analyzed in networks of law enforcement agents and cyber forensics experts. Given this, a new comparative study between the two opposing networks is worthwhile. Cyberterrorists know they had better conceal their interrelationships, let alone their presence of their networks

(Dunnigan, 2003). Therefore, it might be helpful for organizational communication scholars to investigate whether or not cyberterrorists create social networks in order to create diversions or to hide their real intentions. The literature says that it takes a while for law enforcement agents to dismantle, let alone to identify a network in an efficient way (Arquilla & Ronfeldt, 2001). Do cyberterrorists intentionally send confusing or deceptive information through their networks in order to strike targets on their own?

More importantly, technology is only one way law enforcement can look at cyberterrorism in order to cripple cyberterrorist networks. There are multiple factors to take into consideration, like the "social policy" of the network and other soft dynamics. As such, an area of future research is to investigate the ways in which cyberterrorists handle and control their social networks as well as the strengths and weaknesses of the communication paradigms that are possible when they use the Internet. In a similar fashion, the significance of social network theory is partially contingent upon the precise connection between nodes in a social network. Therefore, it might be useful for organizational communication scholars to investigate how small changes in those connections may produce large changes in the properties of social networks of cyberterrorists. It is clear, however, that, unless the researcher infiltrates their networks, becomes a member of their communities, and "thinks" like them, any study of cyberterrorist networks will miss some data about how many nodes there are in those networks, how deep the communication patterns are, and so on. In other words, had the participants been cyberterrorists themselves, the results of this study might have been different.

For this reason, it might prove useful if future researchers take an emic approach whereby the information that the researchers gather is a direct account of cyberterrorism by cyberterrorists themselves, that is, a description of their behavior and actions in terms that are meaningful to them. In this case, the researchers would not be the outsiders, but the insiders. Hence, the analysis of the data would reflect the viewpoint of the native informants. At the same time, it would also be very innovative and ground-breaking.

An Intercultural Communication Perspective

A second area for future research is in intercultural communication. Understanding the culture of cyberterrorist networks should be at the forefront of counter-cyberterrorism concerns, whether law enforcement agencies and cyber forensics experts are dealing with small networks or massive-scale networks. The cyberterrorists' culture may consider disruptions of computer networks and denial-of-service attacks as acceptable actions, but the targeted victims usually look at these matters differently. So do law enforcement agents and cyber forensics experts (MacNulty, 1999). The disagreement on what is acceptable on the Internet and what is not can result in long-lasting intercultural miscommunication. Therefore, further research on improving intercultural communication in that respect should be conducted. We know that, offline, efforts at intercultural dialogue are increasing worldwide (Conhaim, 2005). Yet, does intercultural dialogue ever exist in the fight between cyberterrorists and their opponents online? If so, how does it occur? These are vital questions that can only be answered through profound digging into the realm of cyber warfare. If we do not understand the culture of cyberterrorists, then our ability to gather information quickly as well as our ability to make decisions and carry them out much faster than cyberterrorists becomes

even more critical. For these reasons, it is important that we get inside the cyberterrorists' decision loop.

In line with these contentions, is it easier to share an enemy than a friend? In cyberspace, does the "enemy of my enemy is my friend" phenomenon hold water because it is easier to share an enemy than a friend? The answers to these questions would help us understand the nature of the cyberterrorists' culture and the possible motives that may cause them to launch their attacks. This implies that linguistic and interactive skills become as important as technical skills. It is also essential to understand how law enforcement agents may deal with them appropriately as both potential allies and enemies. They should know the "Other" and what they value. Cyberterrorist values, like any other value, are largely shaped by cultural norms (Johari, 2005). Ideologies do not die easily. If all computers in a foreign country are taken down, it will not erase the ideology. Cyberterrorists will find a different way of communicating their acts of terror. Therefore, it would be useful to look at the fundamental root causes that lead cyberterrorists to engage in malicious activities against our information systems and networks. By the same token, law enforcement should strive to understand more about their own culture so that they can recognize their own strengths and weaknesses as well.

Likewise, it might prove interesting to further explore how culture affects the way cyberterrorists use the computer and the interfaces they might choose. For some Web users, the Internet is another facet of new media that highlights their inability to "speak" at all. As such, it would be important to know whether or not cyberterrorists commit cyber attacks because of their inabilities to "speak." It is evident that cyberterrorists understand technology; their culture leads them to look for different applications and

utilizations of what is available in cyberspace (Slay et al., 2003). Therefore, more insight may be gained by finding out if collectivistic cyberterrorists use different cyber weapons than individualistic cyberterrorists do. And is there a difference between the way collectivistic cyberterrorists encounter – or conflict with – law enforcement agents and the way individualistic cyberterrorists do?

Of equal importance is to study cultural customs such as taboos within the cyberterrorist's culture, and how they might affect their culture's decision-making or interacting processes. Murdock (1965) already studied taboos from an anthropological perspective, but no research has ever been conducted on cyberterrorists' taboos, or even their sacred values. What are the implications of these taboos or values for scholars interested in intercultural communication? In what ways can intercultural communication theory help us understand these taboos or values? How is the conventional study of intercultural communication, bound as it is to the face-to-face or interpersonal context, relevant to the new issues arising with cyberterrorism?

It is also necessary to understand new cultural constructions in the emerging communicative spaces established by cyberterrorists. Intercultural communication in cyberspace is affected by cultures that members of cyberterrorist networks bring to each exchange (Kluver, 2004). Scholars should examine the developing processes and tools that cyberterrorists bring into play and exploit to negotiate or embody group identity and collective construction of meaning in their virtual chat rooms. Regarding the issue of online privacy, as the Internet and computer technologies open doors for an increasing number of cyberterrorists, one fundamental area of future research is to determine whether or not maintaining the advantages of free communication on the Internet should

be appropriate. The debate is complicated by the intercultural dimensions of communication today; what is regarded as freedom in some cultures is perceived as sinful or profligate in other cultures (Triandis, 1995). If the law enforcement's goal is to chase cyberterrorists, should it be to the detriment of online freedom? Our big intercultural challenge, and inherently the global challenge, is to determine how free we want ourselves to be.

Similarly, our vulnerabilities need to be identified, whether they are cultural, psychological, or social, and work to minimize them. The Internet is certainly bringing a major part of life to a few mouse clicks away, but to what extent do all those whom it brings together really understand one another? What if opponents do not understand one another? Do law enforcement agents understand the culture of whom they are dealing with? Do cyberterrorists really belong to another culture or do they share the same culture as their opponents? Truly, research on intercultural communication in these areas is no longer an option, but a necessity. Intercultural communication as an approach for understanding cyberterrorism must be part of a coherent scholarly effort. We must not assume that we automatically know our enemy's logic or motivation.

Finally, cyberterrorism exemplifies the notion that, at the cultural level, the Information Age has made – in part – a negative impact on worldwide culture. For example, American movies such as *Firewall* (starring Harrison Ford), that glorify cyberterrorism, are distributed in other parts of the world and do not necessarily convey a positive image of the United States (Matusitz, 2005b). As the old saying goes, "your cultural image is your country's image." Hence, an important task of our representatives – whether they are tourists or diplomats – is to appease the rising bitterness from allies

and others based on the cyberterrorist culture exported by the United States to their nation states. Changes need to be brought in that respect. For instance, more movies and cartoons should be released that stress the counter-cyberterrorism culture more and give accounts for how the fight against the dark side of the Information Age can be won (Matusitz, 2005b). This cultural package could be used by intercultural communication scholars as a stepping stone to create conceptual models that rationalize how the future of the digital age may turn out to be positive if the war on cyberterrorism is fought the proper way.

An International Communication Perspective

Since this study deals with conflict in cyberspace and the Information Age, it has multiple effects on international communication as well. Therefore, providing directions for future research seems more than appropriate in this context. Let us start by defining what international communication is. International communication is the study of global information, its development, and its pervasion in the political and international realms (Thussu, 2001). Through international communication, nations like the United States are better positioned than other countries to interact with other cultures through sophisticated and less sophisticated means. The less sophisticated means are common means such as talk. The sophisticated means are means such as communication technologies. Yet, because the Information Age has revolutionized how the United States communicates with other countries and because this colossal openness of interchange is available to everyone, cyberterrorists – as this study has revealed – have taken the chance of finding soft spots in those communication technologies and launch various cyber attacks. This is

bad news not only for the United States but also for the international arena (Matusitz, 2005b).

One of the top issues in international communication is the vulnerability to these new global security threats (Thussu, 2001). Our enemies are not only nation states, but also increasingly powerful and determined non-state actors who rely on information technologies and other technological innovations to strike their targets. A postmodern type of terrorist has emerged: the cyberterrorist. The globalization of information through computers and networks is partially directing the world into the dark side of the Information Age (Matusitz, 2005b). Not only are our enemies increasingly non-state actors, but they are also cyberterrorists who try to cripple entire infrastructures a few mouse clicks away. This is a chief international issue because cyberterrorism exemplifies our vulnerability to new security threats. Therefore, the changing nature of global relations and how we improve them are basic factors defining international communication (Harvey & Griffith, 1999). Now the question remains as to how international communication scholars can better explain the phenomenon of cyberterrorism. What future research can be done for improving international communication in that respect?

It is a maxim that international communication always improves through an understanding of how national interests can be developed in the best way possible (Bloom, 1993). Some questions that scholars might explore are the following: "How can nations determine how serious the threat of cyberterrorism is to global communication?" "Can global communication affect national interests because of cyberterrorism?" "Are there any communication means to fight cyberterrorism, or does the fight against cyber

warriors have to be fought mainly through firewalls (and the like) or collaboration with cyberterrorists who got caught?" "Will a global communication network, comprising of not only law enforcement agents and cyber forensics experts, but also diplomats and officials, help reduce cyberterrorist threats?" "And can we improve the understanding of cyberterrorism through international education?" To be able to answer these questions, which are just a sample of all the questions that are necessary to ask in order to improve the situation, it will take years of research for international communication scholars. Therefore, it is important to look at those issues now.

In line with these contentions, given the powerful trends of the globalization of information and based on the main tenets of international relations and American foreign policy, it might prove interesting to further investigate how international policy-making is increasingly involved in global policy processes (Matusitz, 2005b). As such, it would be useful to answer the following questions: "In this fight against cyberterrorism, what are the outcomes for international policy-making processes?" and "As the awareness of cyberterrorism is different in some countries than in others, how can advanced countries like the United States persuade foreign audiences that cyberterrorism is a matter of a high international priority?"

A Law Enforcement Perspective

A final area of research is that of law enforcement. As such, scholars of relevant disciplines should explore how law enforcement agents can implement security and cyberterrorism prevention measures that are concomitant with technology and computer-based development. Law enforcement agents might have progressively learned to better counter cyber attacks with new technologies, but the ability of the local law enforcement

community to fight cyberterrorism would be much improved if they could figure out how to communicate and exchange information in a seamless fashion. As such, it is the responsibility of scholars to develop theoretical models that rationalize, or at least facilitate, this communication and exchange of data in the law enforcement community. Besides, it might prove useful if scholars could offer a conceptual knowledge framework of the systems and structures that enable cyberterrorists to commit their crimes in the digital age. After all, did cyberterrorism emerge simultaneously with computer technology or not?

Another suggestion for future research is to examine how the United States and other countries that use computer technologies a great deal can develop treaties that impose the same, unique Internet regulations on their citizens. This would make the task of counter-cyberterrorism agents much easier. Constraining Web users to subscribe to a state-run Internet service provider would remove objectionable web sites (Denning, 2001). The major benefit of having strict Internet rules is that it would facilitate the identification of where digital attacks originate. By the same token, because existing laws on Internet regulations are unique in each country, it would be important to investigate how legal liability and jurisdiction become serious issues for the judicial and legal systems. The major task of law enforcement agencies is to solve issues of jurisdiction that are ambiguous and those matters of concern that fall across multinational borders.

Truly, no matter what area of research scholars investigate in order to understand the complex phenomenon of cyberterrorism, there needs to be "continued progress towards a just and humane world order" (Swazo, 2004, p. 15). The time to act is now. Hopefully, the lengthy review of the literature, the analysis of the accounts told by the

participants, the conclusions of this study, its implications, and its suggestions for future research will make readers fully aware of the growing phenomenon of cyberterrorism.

References

Acohido, B. (2002, February 13). Research group finds holes in Net security. *USA Today, 1*, p. A4.

Adams, J. (1998). *The next world war*. London: Hutchinson.

Adler, P. S., & Kwon, S. W. (2002). Social capital: Prospects for a new concept. *Academy of Management Review, 27*(1), 17-40.

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

Alavi, M., & Leidner, D. E. (1999). Knowledge management systems: Issues, challenges, and benefits. *Communications of the AIS, 1*, Article 7.

Albert, R., & Barabasi, A. L. (2000). Topology of evolving networks: Local events and universality. *Physical Review Letters, 85*(24), 5234-5237.

Albert, R., Jeong, H., & Barabasi, A. L. (2000). Error and attack tolerance of complex networks. *Nature, 406*(27), 378-382.

Alfert, Jr., R. (1992). Hostes humani generis: An expanded notion of U.S. counterterrorist legislation. *Emory International Law Review, 6*, p. 171.

Alston, R. (1995). *Soldier and society in Roman Egypt*. New York: Routledge.

Alston, R. (1998). The revolt of the Boukoloi: Geography, history, and myth. In K. Hopwood (Ed.), *Organised crime in Antiquity* (pp. 129-153). London: Duckworth.

Alter, C., & Hage, J. (1993). *Organizations working together*. Beverly Hills: Sage Publications.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues, 33*(3), 66-84.

Altheide, D. L., & Johnson, J. M. (1994). Criteria for assessing interpretive validity in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 485-499). Thousand Oaks, CA: Sage Publications.

Andelman, D. A. (1994). The drug cartel's weak link. *Foreign Affairs, 1*, p. 94.

Anderson, S., & Sloan, S. (2002a). *Historical dictionary of terrorism*. Metuchen, NJ: Scarecrow Press.

Anderson, S., & Sloan, S. (2002b). *Terrorism: Assassins to Zealots*. Metuchen, NJ: Scarecrow Press.

Archick, K. (2003). Cybercrime: The council of Europe convention. In J. V. Blane (Ed.), *Cybercrime and cyberterrorism* (pp. 1-6). Hauppauge, NY: Novinka Books.

Arquilla, J., & Ronfeldt, D. (1996). *The advent of netwar*. Santa Monica: RAND.

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

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

Atkinson, B., Heath, A., & Chenail, R. (1991). Qualitative research and the legitimization of knowledge. *Journal of Marital & Family Therapy, 17*(2), 161-166.

Aumann, R., & Hart, S. (Eds.) (1992). *Handbook of game theory with economic applications*. Amsterdam: Elsevier Science Publishers.

Bailey, K. D. (1997). The autopoiesis of social systems: Assessing Luhmann's theory of self-reference. *Systems Research and Behavioral Science, 14*(2), 83-100.

Baker, G. (2005). Beware of the botnets. *New Zealand Management, 52*(3), p. 20.

Ball, P. (2000). The missing links. *Nature, 85*(27), 20-27.

Ballard, J., Hornik, J, & McKenzie, D. (2002). Technological facilitation of terrorism: Definitional, legal, and policy issues. *American Behavioral Scientist, 45*(6), 989-1016.

Banathy, B. H. (1996). Systems inquiry and its application in education. In D. H. Jonassen (Ed.), *Handbook of research for educational communications and technology* (pp. 74-92). New York: Macmillan.

Bandura, A. (1977). *Social learning theory*. Upper Saddle River, NJ: Prentice Hall.

Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. *Information Polity: The International Journal of Government & Democracy in the Information Age, 10*(1), 65-78.

Barabasi, A. L. (2002). *Linked: The new science of networks*. Cambridge, MA: Perseus.

Barabasi, A. L. (2003). *Linked: How everything is connected to everything else and what it means for business, science, and everyday life*. New York: Penguin Group.

Barabasi, A. L., & Albert, R. (1999). Emergence of scaling in random networks. *Science, 286*, 509-512.

Barabasi, A. L., & Bonabeau, E. (2003). Scale-free networks. *Scientific American, 288*, 60-69.

Barber, B. (1995). *Jihad vs. McWorld: How globalism and tribalism are reshaping the world*. New York: Random House.

Baring, A., & Cashford, J. (1991). *The myth of the goddess*. London: Viking.

Bar-Yam, Y. (1988). *Dynamics of complex systems*. Reading, MA: Addison-Wesley.

Basar, T., & Olsder, G. J. (1999). *Dynamic noncooperative game theory* (2nd Ed.). Philadelphia, PA: SIAM.

Batson, C. D., & Ahmad, N. (2001). Empathy-induced altruism in a prisoner's dilemma II: What if the target of empathy has defected? *European Journal of Social Psychology, 31*(1), 25-36.

Baudrillard, J. (1990). *Seduction*. London: Macmillan.

Baudrillard, J. (2003). *Simulacra and simulation*. Ann Arbor, MI: The University of Michigan Press.

Bavelas, A. (1950). Communication patterns in task-oriented groups. *Journal of the Acoustical Society of America, 22*, 725-730.

Beaver, K., & McClure, S. (2004). *Hacking for dummies*. Hoboken, NJ: John Wiley & Sons.

Becker, E. (1999, October 8). Pentagon sets up new center for waging cyberwarfare. *New York Times*, p. A16.

Bednarz, J. (1988). Autopoiesis: The organizational closure of social systems. *Systems Research, 5*(1), 57-64.

Beiser, F. C. (1993). *The Cambridge companion to Hegel*. Cambridge, MA: Cambridge University Press.

Bell, D. (1973). *The coming of post-industrial society: A venture in social forecasting*. New York: Basic Books.

Benford, G. (1998). A scientist's notebook. *Fantasy & Science Fiction, 95*, 117-128.

Benseler, F. Hejl, P., & Kock, W. (Eds.) (1980). *Autopoiesis, communication, and society: The theory of autopoietic systems in the social sciences*. Frankfurt, Germany: Campus Verlag.

Ben-Yehuda, N. (1998). Where Masada's defenders fell. *Biblical Archaeology Review 24*(6), 32-39.

Berdan, F. F. (1998). Crime and control in Aztec society. In K. Hopwood (Ed.), *Organised crime in Antiquity* (pp. 255-269). London: Duckworth.

Berdica, K. (2000). *Analyzing vulnerability in the road transportation system*. Licentiate Thesis, Department of Infrastructure and Planning, Royal Institute of Technology, Stockholm, Sweden.

Berger, A. (1989). *Signs in contemporary culture*. Salem, WI: Sheffield

Berger, A. (1998). *Organizational innovation and redesign in the information age: The drug war, netwar, and other low-end conflict*. Master's thesis. Monterey, CA: Naval Postgraduate School.

Berghel, H. (2001). The Code Red worm. *Communications of the ACM, 44*(12), 15-19.

Berkman, R. I., & Shumway, C. A. (2003). *Digital dilemmas: Ethical issues for online media professionals*. Ames, IA: Iowa State Press.

Berlinski, D. (1976). *On systems analysis*. Cambridge, MA: Massachusetts Institute of Technology Press.

Bertalanffy, L., von (1962). General systems theory: A critical review. *General Systems, 7*, 1-20.

Bertalanffy, L., von (1968). *General systems theory*. New York: Braziller.

Best, S., & Kellner, D. (1991). *Postmodern theory: Critical interrogations*. New York: The Guilford Press.

Beucke, D. & Grow, B. (2005). One man's phishing expedition. *Business Week, 3938*, p. 16.

Bhaskar, R. (2006). State and local law enforcement is not ready for a cyber Katrina. *Communications of the ACM, 49*(2), 81-83.

Bialke, J. P. (2004). Al-Qaeda & Taliban unlawful combatant detainees, unlawful belligerency, and the international laws of armed conflict. *Air Force Law Review, 4*, 10-24.

Bilbao, J., Fernandez, J., Jimenez, N., & Lopez, J. (2002). Voting power in the European Union enlargement. *European Journal of Operational Research, 143*, 181-196.

Bilde, P. (1988). *Flavius Josephus between Jerusalem and Rome: His life, his works, and their importance*. Sheffield: Sheffield Academic Press.

Bischoff, G. (2001). Fear of a black hat. *Telephony, 241*(10), 24-28.

Block, A. (1974). *The Mafia of a Sicilian village 1860-1960: A study of violent peasant entrepreneurs*. New York: Harper & Row.

Block, A. (1979). *East-side-west-side: Organizing crime in New York 1939-1959*. Swansea, UK: Christopher Davis.

Bloom, J. (2002). *The Roman-Judaeo war of 66-74 AD: A military analysis*. Rochester, NY: Sage Publications.

Bloom, W. (1993). *Personal identity, national identity and international relations*. Cambridge, England: Cambridge University Press.

Bogdan, R. C., & Biklen, S. K. (1992). *Qualitative research for education*. *An introduction to theory and methods* (2nd Ed.). Boston: Allyn and Bacon.

Bonachich, P. (2001). The evolution of exchange networks: A simulation study. *Journal of Social Structure, 2*(5), 10-24.

Borja, R. R. (2006). Cyber-security concerns mount as student hacking hits schools. *Education Week, 25*(19), 1-13.

Boyle, M. (2005). The latest hit: CSI in your hard drive. *Fortune, 152*(10), p. 39.

Brenner, M., Brown, J., & Canter, D. (Eds.). (1985). *The research interview: Uses and approaches*. New York: Academic Press.

Brewer, J., & Hunter, A. (1989). *Multimethod research: A synthesis of styles*. Newbury Park, CA: Sage Publications.

Bright, J. E. H., & Pryor, R. G. L. (2005). The chaos theory of careers: A user's guide. *Career Development Quarterly, 53*(4), 291-305.

Brink, E. C. M., van den (1987). A geo-archeological survey in the North-Eastern Nile Delta, Egypt: The first two reasons, a preliminary report. *MDAIK, 43*, 7-24.

Brink, E. C. M., van den (1988). *The archeology of the Nile Delta: Problems and priorities*. Amsterdam: Netherlands Foundation for Archaeological Research in Egypt.

Britain warns of Trojan horse computer attacks (2005). *Information Management Journal, 39*(5), p. 20.

Britt, P. (2005). Ethical hackers: Testing the security waters. *Information Today, 22*(8), 1-28.

Britz, M. (2004). *Computer forensics and cyber crime*. Upper Saddle River, NJ: Prentice Hall.

Brown, J. S., & Duguid, P. (2000). *The social life of information*. Boston: Harvard Business School Press.

Brynjolfsson, E., & Mendelson, H. (1993). Information systems and the organization of modern enterprise. *Journal of Organizational Computing, 3*, p. 4.

Bubitt, S. (2002). Digital filming and special effects. In D. Harries (Ed.), *The new media book* (pp. 17-29). London: BFI Publishing.

Buchanan, M. (2002). *Nexus: Small worlds and the groundbreaking science of networks*. New York: Norton Press.

Bucher, H. J. (2002). The power of the audience: Interculturality, interactivity and trust in internet-communication: Theory, research design, and empirical results. In F. Sudweeks & C. Ess (Eds.). *Proceedings, cultural attitudes towards technology and communication* (pp. 3-14). Murdoch, Australia: Murdoch University Press.

Burkard, D. J. (1994). *Push-pull mobilization: A force multiplier*. Randolph Field, TX: Office of History and Research, Headquarters AETC.

Burkert, W. (1983). *Homo necans: Anthropology of ancient Greek sacrificial ritual and myth*. Berkeley: University of California Press.

Burt, R. S. (1992). *Structural holes: The social structure of competition*. Cambridge, MA: Harvard University Press.

Burt, R. S. (1993). The social structure of competition. In R. Swedberg (Ed.), *Explorations in economic sociology* (pp. 65-103). New York: Sage Publications.

Burton, J. (1972). *World society*. Cambridge, MA: Cambridge University Press.

Buttyán, L., Hubaux, J. P., & Capkun, S. (2004). A formal model of rational exchange and its application to the analysis of Syverson's protocol. *Journal of Computer Security, 12*(3), p. 551.

Cahill, R. T., & Klinger, C. M. (2000). Self-referential noise as a fundamental aspect of reality. *AIP Conference Proceedings, 511*(1), 43-48.

Cairncross, F. (1997). *The death of distance*. Boston: Harvard Business School Press.

Cangemi, D. (2004). Procedural law provisions of the council of Europe convention on cybercrime. *International Review of Law Computers & Technology, 18*(2), 165-171.

Capurro, R. (2005). Privacy: An intercultural perspective. *Ethics and Information Technology, 7*(1), 37-47.

Carlson, C., & Fisher, D. (2004). Feds pressured on phishing. *eWeek, 21*(39), p. 14.

Carlson, S. (2004). Courses in cyber forensics gain popularity on campuses. *Chronicle of Higher Education, 50*(30), p. A37.

Carmel, D., & Markovitch, S. (1996). Learning and using opponent models in adversary search, *Technical Report, CIS9606*.

Carooso, J. (2004). Are you 133t? One-time hacker slang now ridiculed by all except those who use it. *Network World, 1*, p. 76.

Carter, D., & Katz, A. (1996). Computer crime. *FBI Law Enforcement Bulletin, 4*, 1-8.

Casey, E. (2004). *Digital evidence and computer crime*. New York: Academic Press.

Castells, M. (1996). *The rise of the network society*. *The information age: Economy, society, and culture*. Oxford: Blackwell.

Castells, M. (2000). The network society. In D. Held & A. McGrew (Eds.), *The global transformations reader: An introduction to the global debate* (pp. 76-81). Cambridge, MA: Polity Press.

Castilla, E., et al. (2000). Social networks in Silicon Valley. In C. M. Lee, W. F. Miller, M. G. Hancock, & H. S. Rowen (Eds.), *The silicon valley edge* (pp. 218-247). Stanford, CA: Stanford University Press.

Center for Strategic and International Studies, The (1998). *Cybercrime, cyberterrorism, and cyberwarfare: Averting an electronic Waterloo*. Washington D.C.

Cha, A. E. (2001, November 4). For Clarke, a career of expecting the worst: Newly appointed cyberspace security czar aims to prevent "Digital Pearl Harbor." *Washington Post*, p. A5.

Chamberlain, L. (1998). An introduction to chaos and nonlinear dynamics. In L. L. Chamberlain, & M. R. Butz (Eds.), *Clinical chaos: A therapeutic guide to nonlinear dynamics and therapeutic change* (pp. 3-14). Philadelphia: Brunner/Mazel.

Champagne, J. (2002). Gaia's Brain: Integrating humanity and the biosphere. *Synearth, 6*, 10-18.

Charalabidis, A. (1999). *The book of IRC: The ultimate guide to Internet Relay Chat*. San Francisco: No Starch Press.

Chirillo, J. (2002). *Hack attacks testing: How to conduct your own security audit*. New York: Wiley.

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

Cohen, S. J. D. (1982). Masada: Literary tradition, archaeological remains and the credibility of Josephus. *Journal of Jewish Studies, 33*, 385-405.

Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly, 35*, 128-152.

Coleman, J. S. (1988). Social capital in the creation of human capital. *American Journal of Sociology, 94*, 95-120.

Coleman, R. (2002). Hackers beware: Student lab ranks among the world's best computer security teams. *UNT News*, p. A1.

Collin, B. (1996). *The future of cyberterrorism*. Proceedings of 11th Annual International Symposium on Criminal Justice Issues: The University of Illinois at Chicago.

Collins, P. D. (2002). *The hidden face of terrorism: The dark side of social engineering from Antiquity to September 11*. Bloomington, IN: AuthorHouse.

Collins, R., Hanneman, R., & Mordt, G. (1995). Discovering theory dynamics by simulation. *Sociological Methodology, 25*, 1-46.

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

Cortes, F., Przeworski, A., & Sprague, J. (1974). *Systems analysis for social scientists*. New York: Wiley.

Cronbach, L. J. (1971). Test validation. In R. L. Thorndike (Ed.), *Educational measurement* (pp. 442-507). Washington, D.C.: American Council of Education.

Cronbach, L. J. (1975). Beyond the two disciplines of scientific psychology. *American Psychologist, 30*(2), 116-127.

Crotty, M. (1998). *The foundation of social research: Meaning and perspective in the research process*. Thousand Oaks, CA: Sage Publications.

Crystal, D. (2001). *Language and the Internet*. Cambridge, MA: Cambridge University Press.

Cyber Forensics at Purdue University (2005). www.cyberforensics.purdue.edu.

Davidson, J. (1997). *Courtesans and fishcakes: The consuming passions of classical Athens*. London: Fontana Press.

Davis, J. M., & Preiss, B. (2006). *Conspiracy and the Freemasons: How the secret society and their enemies shaped the modern world*. New York: St. Martin's Griffin.

Davis, M. (1997). *Gangland: Cultural elites and the new generationalism*. Allen & Unwin, St Leonards.

Debrix, F. (2001). Cyberterror and media-induced fears: The production of emergency culture. *Strategies: Journal of Theory, Culture & Politics, 14*(1), 149-168.

Degenne, A., & Forse, M. (1999). *Introducing social networks*. London: Sage Publications.

Deibert, R. J. (1997). *Parchment, printing, and hypermedia: Communication in world order transformation*. New York: Columbia University Press.

Dekker, S. (2002). *The field guide to human error investigations*. London: Ashgate Publishing.

Delio, M. (2005). Enterprises share phishing tales. *InfoWorld, 27*(4), p. 35.

Demaio, H. B. (2001). *B2B and beyond: New business models built on trust*. Hoboken, NJ: John Wiley & Sons.

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

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

Denning. D. E. (2000). *Information warfare and security*. Boston: Addison-Wesley.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism. The internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars* (pp. 239-288). Santa Monica, CA: RAND.

Denzin, N. K., & Lincoln, Y. S. (1998). Introduction: Entering the field of qualitative research. In N. K. Denzin, & Y. S. Lincoln (Eds.), *The landscape of qualitative research: Theories and issues* (pp. 1-34). Thousand Oaks, CA: Sage publications.

Der Derian, J. (2005). Imaging terror: Logos, pathos, and ethos. *Third World Quarterly, 26*(1), 23-37.

Der Derian, J., & Douglas, I. R. (2005). *VirtualY2K*. Providence, RI: Watson Institute for International Studies.

Derrida, J. (1967). *Writing and difference*. Chicago: University of Chicago Press.

Derrida, J. (1973). *Speech and phenomena*. Evanston, IL: Northwestern University Press.

Dewett, T., & Jones, G. R. (2001). The role of information technology in the organization: A review, model, and assessment. *Journal of Management, 27*(3), 313-346.

Diamond, J., Moniz, D., Slavin, B., Hall, M., & Despeignes, P. (2003, September 11). 6 fronts of the war on terrorism. *USA Today*, p. A4.

Diani, M., & McAdam, D. (2003). *Social movements and networks: Relational approaches to collective action*. Oxford: Oxford University Press.

Digital Evidence (2005). http://ncfs.ucf.edu/digital_evd.html.

DiNardo, K. (2004, June 25). Be careful out there. *USA Today*, p. A4.

Diones, B. (2006). Firewall. *New Yorker, 82*(2), p. 19.

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

Donath, J. S. (1999). Identity and deception in the virtual community. In M. A. Smith, & P. Kollock (Eds.), *Communities in cyberspace* (pp. 29-59). New York: Routledge.

Dorogovtsev, S. N., & Mendes, J. F. F. (2003). *Evolution of networks: From biological networks to the Internet and WWW*. Oxford: Oxford University Press.

Dunn, A. (1999, April 3). Crisis in Yugoslavia: Battle spilling over onto the Internet. *Los Angeles Times*, p. A3.

Dunnigan, J. F. (2003). *The next war zone: Confronting the global threat of cyberterrorism*. New York: Citadel Press.

Dupuy, T. N., Bongard, D. L., & Anderson, R. C. (1994). *Hitler's last gamble: The Battle of the Bulge, December 1944-January 1945*. New York: HarperCollins.

Dussauge, P., Garrette, B., & Mitchell, W. (2000). Learning from competing partners: Outcomes and durations of scale and link alliances in Europe, North America, and Asia. *Strategic Management Journal, 21*, 99-126.

Eco, U. (1986). Towards a semiological guerrilla warfare. In U. Eco (Ed.), *Travels in hyperreality* (pp. 135-144). San Diego: Harcourt.

Edwords, F. (2005). Humanism and communism. *Humanist, 65*(2), 40-41.

Eichenwald, K. (2001). *The informant: A true story*. New York: Broadway.

Eisenstadt, S. N. (1996). Barbarism and modernity. *Society, 33*(4), 31-39.

Ekman, P. (2003). *Emotions revealed: Recognizing faces and feelings to improve communication and emotional life*. New York: Times Books.

Elison, W. (2000). Netwar: Studying rebels on the Internet. *Social Studies, 91*(3), 127-131.

E-mail users caught in virus feud (2004). www.news.bbc.co.uk.

Erlanger, L. (2004). The weakest link. *PC Magazine, 23*(5), 58-59.

Evan, W. M. (1972). An organization-set model of interorganizational relations. In M. Tuite, R. Chisholm, & M. Radnor (Eds.), *Interorganizational decision-making* (pp. 181-200). Chicago: Aldine.

Fadia, A. (2005). *The unofficial guide to ethical hacking*. Washington: Course Technology PTR.

Faloutsos, M., Faloutsos, P., & Faloutsos, C. (1999). On power-law relationships of the internet topology. *The ACM Computer Communication Review, 29*, 251-262.

Farah, D. (1997, August 31). Antigua Internet bank vanishes into cyberspace. *The Washington Post*, p. A30.

Farmer, W. R. (1956). *Maccabees, Zealots, and Josephus*. New York: Columbia University Press.

Feldman, L. H., & Hata, G. (1987). *Josephus, Judaism, and Christianity*. Detroit: Wayne State University Press.

Fent, T., Feichtinger, G., & Tragler, G. (2002). A dynamic game of offending and law enforcement. *International Game Theory Review, 4*(1), 71-89.

Fernandez, R. M., & Gould, R. V. (1994). A dilemma of state power: Brokerage and influence in the national health policy domain. *American Journal of Sociology, 99*(6), 1455-1491.

Financial crimes and money laundering (1997). *U.S. Department of State*. International Narcotics Control Strategy Report.

Fisher, D., Nobel, C., & Taft, D. (2003). The high-tech war. *eWeek, 20*(13), p. 1.

Fisher, N. (1992). *Hybris: A study in the values of honour and shame in ancient Greece*. Warminster: Aris & Phillips.

Fisher, N. (1998). Workshops of villains: Was there much organised crime in classical Athens? In K. Hopwood (Ed.), *Organised crime in Antiquity* (pp. 53-96). London: Duckworth.

Fiske, J. (1982). *Introduction to communication studies*. New York: Methuen.

Fixmer, R. (2000). More than Intel inside. *Interactive Week, 7*(50), p.8.

Flanagin, A. J. (2002). The elusive benefits of the technological support of knowledge management. *Management Communication Quarterly, 16*(2), 242-248.

Floyd, S., & Fall, K. (1999). Promoting the use of end-to-end congestion control. *IEEE/ACM Transactions on Networking, 7*(4), 458-472.

Flynn, M. K. (2003). It takes a hacker. *PC Magazine, 21*(18), p. 26.

Franklin, G., Powell, J. D., & Emami-Naeini, A. (2005). *Feedback control of dynamic systems*. Upper Saddle River, NJ: Prentice Hall.

Frederick, R. (2005). Tapping into students' cultural identity. *Educational Leadership, 63*(4), 69-70.

Freeman, L. C. (1981). Social networks: A beginner's bookshelf. *Social Networks, 4*(2), 6-10.

Freeman, W. (1991). The physiology of perception. *Scientific American, 264*, 78-85.

Frost, T. (2005). *The secret society of the Carbonari*. Kila, MT: Kessinger Publishing.

Fudenberg, D., & Tirole, J. (1991). *Game theory*. Cambridge, MA: MIT Press.

Fukuyama, F. (1996). *Trust: The social virtues and the creation of prosperity*. New York: Free Press.

Fulghum, D. A. (2005). Wireless war. *Aviation Week & Space Technology, 163*(16), 48-50.

Gabrys, E. (2002). The international dimensions of cyber-crime. *Information Systems Security, 11*(4), 21-32.

Garrison, A. H. (2003). Terrorism: The nature of its history. *Criminal Justice Studies, 16*(1), 39-52.

Gebser, J. (1985). *The ever-present origin*. Athens, OH: Ohio University Press.

Geertz, C. (1973). *The interpretation of cultures: Selected essays*. New York: Basic Books.

General Accounting Office (1991). *Computer security: Hackers penetrate DOD computer systems*. Washington, DC: GAO/T-IMTEC.

Gibson, W. (1984). *Neuromancer*. New York: Ace Books.

Gill, K. S. (Ed.). (1996). *Information society: New media, ethics, and postmodernism*. New York: Springer.

Girard, R. (1977). *Violence and the sacred*. Baltimore: The Johns Hopkins University Press.

Gleick, J. (1987). *Chaos: Making a new science*. New York: Viking.

Goldsborough, R. (2006). Mastering computers. *Tech Directions, 65*(6), p. 9.

Goodman, M. (2001). Making computer crime count. *FBI Law Enforcement Bulletin, 70*(8), 10-17.

Goodman, M. (2002). Current scholarship on the first revolt. In A. Berlin & J. A. Overman (Eds.), *The first Jewish Revolt* (pp. 15-24). London: Routledge.

Goodman, N. (1978). *Ways of worldmaking*. Indianapolis, IN: Hackett.

Graham-Rowe, D. (2003). Red alert on the e-war front. *New Scientist, 179*(2402), 38-43.

Granovetter, M. (1973). The strength of weak ties. *American Journal of Sociology, 78*, 1360-1380.

Granovetter, M. (1982). The strength of weak ties: A network theory revisited. In R. Collins (Ed.), *Sociological theory* (pp. 105-130). San Francisco: Jossey-Bass.

Granovetter, M. (1983). The strength of weak ties: A network theory revisited. *Sociological Theory, 1*, 201-233.

Gray, R. (1993). *Prophetic figures in late second temple Jewish Palestine: The evidence from Josephus*. Oxford: Oxford University Press.

Greenie, K. (2005). Untangling a web. *Science News, 168*(15), p. 230.

Greif, A. (1994). Cultural beliefs and the organization of society: A historical and theoretical reflection on collectivist and individualist societies. *Journal of Political Economy, 102*(5), 912-950.

Greif, A. (1997). On the interrelations and economic implications of economic, social, political, and normative factors: Reflection from two late medieval societies. In J. N. Drobak, & J. V. C. Nye (Eds.), *The frontiers of the new institutional economics* (pp. 57-94). San Diego: Academic Press.

Groom, A. J. R., & Taylor, P. (Eds.). (1977). *International organizations: A conceptual approach*. London: Frances Pinter.

Gruman, G. (2005). Is it time to scarp big iron? *InfoWorld, 27*(47), 33-39.

Guba, E., & Lincoln, Y. (1989). *Fourth generation evaluation*. Beverly Hills: Sage Publications.

Gur-Ze'ev, I. (2000). Critical education in cyberspace. *Educational Philosophy and Theory, 32*(2), 209-231.

Habeeb, M. (2004). Venturing into computer forensics. *Community College Week, 17*(7), p. 12.

Habermas, J. (1980). *Moral consciousness and communicative action*. Cambridge, MA: MIT Press.

Hafner, K., & Markoff, J. (1991). *Cyberpunk: Outlaws and hackers on the computer frontier*. New York: Simon & Schuster.

Hall, M. (2004). Sticky security. *Computerworld, 38*(3), p. 48.

Hamel, G. (1991). Competition for competence and inter-partner learning within international strategic alliances. *Strategic Management Journal, 12*, 83-103.

Hamilton, D. (1998). Traditions, preferences, and postures in applied qualitative research. In N. K. Denzin, & Y. S. Lincoln (Eds.), *The landscape of qualitative research: Theories and issues* (pp. 111-129). Thousand Oaks, CA: Sage Publications.

Harris, S., Harper, A., Eagle, C., Ness, J., & Lester, M. (2004). *Gray hat hacking: The ethical hacker's handbook*. Boston: McGraw-Hill.

Harvey, F. P., & Griffith, A. L. (1999). *Foreign and security policy in the Information Age*. Dalhousie University: Centre for Foreign Policy Studies.

Haythornthwaite, C. (2000). Online personal networks. *New Media and Society, 2*(2), 195-226.

Hecht, M. L., Warren, J. R., Jung, E., & Krieger, J. L. (2005). The communication theory of identity: Development, theoretical perspective, and future directions. In W. B. Gudykunst (Ed.), *Theorizing about intercultural communication* (pp. 257-278). Thousand Oaks, CA: Sage Publications.

Heidegger, M. (1977). The question concerning technology. In D. Krell, *Martin Heidegger: Basic writings* (pp. 55-93). New York: Harper & Row.

Hejl, P. (1984). Towards a theory of social systems: Self-organization and self-maintenance, self-reference and syn-reference. In H. Ulrich, & G. J. B. Probst (Eds.), *Self-organization and management of social systems: Insights, promises, doubts, and questions* (pp. 60-78). Berlin, Germany: Springer-Verlag.

Hermann, P., Issarny, V., & Shiu, S. (2005). *Trust management: Third international conference, iTrust 2005, Paris, France, May 23-26, 2005, proceedings*. London: Springer-Verlag.

Heydebrand, W. V. (1989). New organizational forms. *Work and Occupations, 16*(3), 323-357.

Heylighen, F. (2003). The science of self-organization and adaptivity. *The encyclopedia of life support systems*. EOLSS Publishers Co. Ltd.

Hildreth, P. M., & Kimble, C. (2002). The duality of knowledge. *Information Research, 8*(1), p.142.

Hildreth, P. M., & Kimble, C. (2004). *Knowledge networks: Innovation through communities of practice*. London: Idea Group Inc.

Hodapp, C. (2005). *Freemasons for dummies*. Indianapolis: Wiley Publishing Inc.

Hoffmann, G. (1999, October 24). US opens the door to cyberwar technology: The Kosovo conflict saw the first electronic attacks on enemy computer and communications systems. *Orange Reg*., p. A35.

Hofstede, G. H. (1991). *Cultures and organizations: Software of the mind*. New York: McGraw-Hill.

Holden, C. (2005). Economics Nobel gets in the game. *Science Now, 5*, 2-3.

Holman, V. (2004). *Rescuing Patty Hearst: Growing up sane in a decade gone mad*. New York: Simon & Schuster.

Holsapple, M. (2005, October 26). Purdue engages law enforcement with computer forensics triage training. *Purdue University News,* p. A1.

Hopwood, K. (1998). Bandits between grandees and the state: The structure of order in Roman Rough Cilicia. In K. Hopwood (Ed.), *Organised crime in Antiquity* (pp. 177-206). London: Duckworth.

Horsley, R. A. (1986). The Zealots: Their origin, relationships, and importance in the Jewish revolt. *Novum Testamentum, 28*, 159-192.

Hosenball, M. (2002). Islamic cyberterror. *Newsweek, 139*(20), p. 10.

Hosmer, C., Gordon, G., Hyde, C., & Grant, T. (2000). *Cyber forensics 2000*. Washington D.C.: Proceedings, 1st Annual Study of the State-of-the-Art in Cyber Forensics.

Hsu, F., Anantharaman, S., Campbell, M. S., & Nowatzyk, A. (1990). Deep thought. In T. A. Marsland & J. Schaeffer (Eds.), *Computer, chess, and cognition* (pp. 55-78). New York: Springer Verlag.

Hunter-Carsch, M., & Cooper, P. (2006). *The handbook of social, emotional and behavioural difficulties: Educational engagement and communication*. London: Continuum International Publishing Group.

Hutton, D. B., & Mydlarz, A. (2003). *Guide to homeland security careers*. New York: Barrons Educational Series.

Ignazi, P. (2003). Italy. *European Journal of Political Research, 42*(7), 990-995.

Internet World Stats (2006). Internet usage statistics: The big picture. www.internetworldstats.com/stats.htm.

James, L. (2005). *Phishing exposed*. Rockland, MA: Syngress Publishing.

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

Janesick, V. (2000). The choreography of qualitative research design: Minuets, improvisations, and crystallization. In N. K. Denzin & Y. S. Lincoln (Eds.), *The handbook of qualitative research* (pp. 379-400). Thousand Oaks, CA: Sage Publications.

Jehle, G. A., & Reny, P. J. (2001). *Advanced microeconomic theory* (2nd Ed.). Boston: Addison-Wesley Longman.

Johari, A. (2005). Intercultural Internet-based learning: Know your audience and what it values. *Educational Technology Research & Development, 53*(2), 117-127.

Johnson, B. R. (1997). Examining the validity structure of qualitative research. *Education, 118*(3), 282-292.

Johnson, G. (2000, December 26). First cells, then species, now the web. *New York Times*, p. M1.

Johnson, P. (1990). The seven deadly sins of terrorism. In H. H. Hahn (Ed.), *Terrorism and politicial violence: Limits and possibilities of legal control* (pp. 189-190). New York: Oceana Publications.

Johnson, P., & Levin, G. (2002). It's not just Koppel vs. Letterman. *USA Today*, p. A4.

Jones, A. H. M. (1964). *The later Roman Empire 284-602: A social, economic, and administrative survey*. Oxford: Oxford University Press.

Jordan, T. (1999). *Cyberculture: The culture and politics of cyberspace and the Internet*. London: Routledge.

Josephus (1982). *The Jewish war*. Israel: Steimatzky.

Jøsang, A., Gray, E., & Kinateder, M. (2003). *Analyzing topologies of transitive trust*. In the proceedings of the Workshop of Formal Aspects of Security and Trust (FAST), Pisa, Italy, 2003.

Kagitcibasi, C. (1994). A critical appraisal of individualism and collectivism: Toward a new formulation. In U. Kim, H. C. Triandis, C. Kagitcibasi, S. C. Choi, & G. Yoon (Eds.), *Individualism and collectivism: Theory, method, and applications* (pp. 52-65). Thousand Oaks, CA: Sage Publications.

Kalathil, S., & Boas, T. C. (2003). *Open networks, closed regimes: The impact of the*

Internet on authoritarian rule. Washington D.C.: Carnegie Endowment for International Peace.

Kamien, D. (2005). *The McGraw-Hill Homeland Security handbook*. Boston: McGraw-Hill.

Kandell, M. J. (1995). Public housing: The ostrich strategy. *American Planning Association, 61*(6), 10-13.

Kee, E. (2005). Understanding elite speak. *Computimes, 3*, p. 50.

Keller, E. F. (2005). Revisiting "scale-free" networks. *BioEssays, 27*(10), 1060-1068.

Kellner, D. (1989). *Jean Baudrillard: From Marxism to postmodernism and beyond*. Palo Alto, CA: Stanford University Press.

Kerbs, V. E. (2001). Mapping networks of terrorist cells. *Connections, 24*(3), 43-52.

Kettinger, W., & Grover, V. (1997). The use of computer mediated communication in an interorganizational context. *Decision Sciences, 28*(3), 513-555.

Kincheloe, J. L., & McLaren, P. (2000). Rethinking critical theory and qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *The handbook of qualitative research* (pp. 279-314). Thousand Oaks, CA: Sage Publications.

Kirk J., & Miller M. (1986). *Reliability and validity in qualitative research*. London: Sage Publications.

Klarreich, E. (2004). Generous players. *Science News, 166*(4), 58-60.

Klein, H., & Myers, M. (1999): A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*(1), 67-93.

Kling, R., & Carmel, E. (1997). American hegemony in packaged software trade and the "culture of software." *Information Society, 13*(1), 125-142.

Kluver, R. (2004). Political culture and information technology in the 2001 Singapore general election. *Political Communication, 21*, 435-458.

Knapp, E. M. (1998). Knowledge management. *Business and Economic Review, 44*(4), 3-6.

Knight, W. (2005). Police deactivate network of 100,000 "zombie" PCs. www.newscientist.com/article.ns?id=dn8145

Kojève, A. (1969). *Introduction to the reading of Hegel*. New York: Basic Books.

Kopf, D. (1998). Dealing with the devil. *America's Network, 102*(4), 19-25.

Kouri, J. (2005, November 18). FBI strategy plan predicts large scale computer attacks. *American Chronicle*, p. A2.

Kozeriok, C. (2005). *The TCP/IP guide: A comprehensive, illustrated internet protocols reference*. San Francisco: No Starch Press.

Kramer, E. M. (1997). *Modern/postmodern: Off the beaten path of antimodernism*. Westport, CT: Praeger.

Krapp, P. (2005). Terror and play, or what was hacktivism? *Grey Room, 1*(21), 70-93.

Kshetri, N. (2005). Hacking the odds. *Foreign Policy, 148*, p. 93.

Kumar, K. (1997). The post-modern condition. In A. H. Halsey, H. Lauder, P. Brown, & A. S. Wells (Eds.), *Education: Culture, economy, and society* (pp. 86-112). Oxford: Oxford University Press.

Kuzel, A. J., & Like, R. C. (1991). Standards of trustworthiness for qualitative studies in primary care. In P. G. Norton, M. Stewart, F. Tudiver, M. J. Bass, & E. V. Dunn

(Eds.), *Primary care research: Traditional and innovative approaches* (pp. 138-158). Newbury Park, CA: Sage Publications.

Kvale, S. (1995). The social construction of validity. *Qualitative Inquiry, 1*(1), 19-40.

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

Labov, W., & Waletsky, J. (1967). Narrative analysis: Oral versions of personal experience. In J. Helm (Ed.), *Essays on the verbal and visual arts* (pp. 12-34). Seattle: University of Washington Press.

Landa, J. T. (1994). *Trust, ethnicity, and identity*. Ann Arbor, MI: University of Michigan Press.

Lapan, H. E., & Sandler, T. (1988). To bargain or not to bargain: That is the question. *American Economic Review, 78*(2), 16-20.

Lapan, H. E., & Sandler, T. (1993). Terrorism and signalling. *European Journal of Political Economy, 9*(3), 383-397.

Laqueur, W. (1999a). *Terrorism and history*. Oxford: Oxford University Press.

Laqueur, W. (1999b). *The new terrorism: Fanaticism and the arms of mass destruction*. Oxford: Oxford University Press.

Larson, A. (1992). Network dyads in entrepreneurial settings: A study of governance of exchange relationships. *Administrative Science Quarterly, 37*, 76-104.

Lather, P. (1993). Fertile obsession: Validity after poststructuralism. *Sociological Quarterly, 34*(4), 673-693.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22-42.

Leadbetter, B. (2002). Constantine and the bishop: The Roman Church in the early fourth century. *Journal of Religious History, 26*(1), 1-14.

Leavitt, H. J. (1951). Some effects of certain communication patterns on group performance. *Journal of Abnormal and Social Psychology, 46*, 38-50.

Lee, A. S. (2001). Challenges to qualitative researchers in information systems. In E. M. Trauth (Ed.), *Qualitative research in IS: Issues and trends* (pp. 240-270). USA: Idea Group Publishing.

Lee, D. R. (1988). Free riding and paid riding in the fight against terrorism. *American Economic Review, 78*(2), 22-26.

Lehmann, F. (2004). FLOSS developers as a social formation. *First Monday, 9*(11), 10-24.

Lendon, J. E. (1997). *Empire of honour: The art of government in the Roman world*. Oxford: Oxford University Press.

Lenzner, R., & Vardi, N. (2004). The next threat. *Forbes, 174*(5), 70-81.

Leonard, D., & Sensiper, S. (1998). The role of tacit knowledge in group innovation. *California Management Review, 40*(3), 112-132.

Leonard-Barton, D. (1995). *Wellsprings of knowledge: Building and sustaining the sources of innovation*. Boston: Harvard Business School Press.

Lévi-Strauss, C. (1966). *The savage mind* (2nd Ed.). Chicago: University of Chicago Press.

Levy, P. (2000). *Kyberkultura*. Prague: Karolinum.

Levy, S. (2001). *Hackers: Heroes of the computer revolution*. London: Penguin.

Lewis, B. (1969). The Ishmaelites and the Assassins. In M. W. Baldwin (Ed.), *The first hundred years* (pp. 99-132). Madison, WI: University of Wisconsin Press.

Lewis, B. (1987). *The Assassins: A radical sect in Islam*. Oxford: Oxford University Press.

Liell, S. (2003). *Tom Paine, common sense, and the turning point to American independence*. Philadelphia: Running Press.

Lilienfeld, R. (1978). *The rise of systems theory*. New York: John Wiley & Sons.

Lin, N. (2001). Building a network theory of social capital. In N. Lin, K. Cook, & R. S. Burt (Eds.), *Social capital: Theory and research* (pp. 3-30). New York: Aldine de Gruyter.

Lincoln, Y. S., & Denzin, N. K. (1998). The fifth moment. In N. K. Denzin, & Y. S. Lincoln (Eds.), *The landscape of qualitative research: Theories and issues* (pp. 407-429). Thousand Oaks, CA: Sage publications.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Beverly Hills, CA: Sage Publications.

Lincoln, Y. S., & Guba, E. G. (2000). Paradigmatic controversies, contradictions, and emerging confluences. In N. K. Denzin & Y. S. Lincoln (Eds.), *The handbook of qualitative research* (pp. 163-188). Thousand Oaks, CA: Sage Publications.

Lininger, R., & Vines, R. D. (2005). *Phishing: Cutting the identity theft line*. Indianapolis: Wiley Publishing, Inc.

Lipnack, J., & Stamps, J. (1986). *The networking book: People connecting with people*. New York: Routledge and Kegan Paul.

Lister, M., Dovey, J., Giddings, S., Grant, I., & Kelly, K. (2003). *New media: A critical introduction*. New York: Routledge.

Littlejohn, S. W. (1992). *Theories of human communication*. Belmont, CA: Wadsworth Publishing Company.

Littman, J. (1997). *The fugitive game: Online with Kevin Mitnick*. New York: Little, Brown, and Company.

Littman, M. L. (1994). Markov games as a framework for multi-agent reinforcement learning. *Proceedings of the Eleventh International Conference on Machine Learning*, 157-163.

Lloyd, J. (2002). Paving the way for the Red Brigades. *New Statesman, 131*(4601), p. 16.

Lofland, J., & Lofland, L. H. (1995). *Analyzing social settings: A guide to qualitative observation and analysis*. Belmont, CA: Wadsworth Publishing.

Longueuil, D. J. (2002). *Wireless messaging demystified: SMS, EMS, MMS, IM, and others*. Boston: McGraw-Hill.

Lorrain, F. (1975). *Reseaux sociaux et classifications sociales*. Paris: Hermann.

Lott, S., & Taylor, A. (2005). Hub networks hurt by handling capacity. *Aviation Week & Space Technology, 163*(18), p. 56.

Love Bug Revenge Theory (May 10, 2000). *BBC News*.

Luhmann, N. (1982). The world society as a social system. *International Journal of General Systems, 8*, 131-138.

Luhmann, N. (1995). *Social systems*. Stanford, CA: Stanford University Press.

Lukács, G. (1975). *The young Hegel*. London: Merlin Press.

Luskin, B. J. (1996). Toward an understanding of media psychology. *T H E Journal, 23*, 82-85.

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

Lyotard, J. F. (1984). *The postmodern condition*. Minneapolis, MN: University of Minnesota Press.

Mackey, A. G. (1996). *The history of freemasonry*. New York: Gramercy Books.

MacNulty, A. A. R. (1999). *Socio-political change and asymmetry in information warfare and intelligence*. InfoWarCon99, Washington, September 1999.

Maddox, R. L. (1985). Contemporary hermeneutic philosophy and theological studies. *Religious Studies, 21*, 517-529.

Madorsky Elman, N., & Kennedy-Moore, E. (2003). *The unwritten rules of friendship: Simple strategies to help your child make friends*. New York: Little, Brown, and Company.

Maier, P. (1993). *Flavius Josephus: The essential writings*. Grand Rapids, MI: Kregel Publications.

Mair, L. (1962). *Primitive government*. Harmondsworth, England: Penguin Books.

Malinowski, S. (1998). *Gale encyclopedia of Native American tribes*. Farmington Hills, MI: Thomson Gale.

Mansfield, R. (2000). *Hacker attack*. San Francisco: Sybex.

Markus, L. M., Bikson, S., El-Shinnawy, M., & Soe, L. L. (1992). Fragments of your communication: Email, email and fax. *The Information Society, 8*, 207-226.

Martinez-Torres, M. E. (2001). Civil society, the Internet, and the Zapatistas. *Peace Review, 13*(3), 347-355.

Marwick, A. D. (2001). Knowledge management technology. *IBM Systems Journal, 40*(4), 10-18.

Matlis, J. (2002). Scale-free networks. *Computerworld, 1*, 10-17.

Matthews, J. (2005). *Computer networks: Internet protocols in action*. Hoboken, NJ: John Wiley & Sons.

Matusitz, J. (2005a). The current condition of visual communication in colleges and universities of the United States. *Journal of Visual Literacy, 25*(1), 97-112.

Matusitz, J. (2005b). Cyberterrorism: How can American foreign policy be strengthened in the information age? *American Foreign Policy Interests, 27*(2), 137-147.

Matusitz, J. (2005c). Deception in the virtual world: A semiotic analysis of identity. *Journal of New Media and Culture, 3*(1), 54-63.

Matusitz, J., & O'Hair, D. (in press). Cyber-terrorism. In D. O'Hair, R. Heath, K. Ayotte, & G. R. Ledlow (Eds.), *Terrorism: Communication and rhetorical perspectives*. Cresskill, NJ: Hampton Press.

McClure, S., & Scambray, J. (1999). Tricks of the trade obscure hacker tracks and make anonymity easily attainable. *InfoWorld, 21*(3), p. 61.

McCracken, H. (2004). Is this any way to fix security holes? *PC World, 22*(11), p. 17.

McCullough, J. (2004). *185 wireless secrets: Unleash the power of pdas, cell phones, and wireless networks*. Hoboken, NJ: John Wiley & Sons.

McDermott, C. (1992). *Essential design*. London: Bloomsbury.

McDonnell, M. (2004). Cyber terrorism and espionage is real and growing. *Bulletin, 58*(4), 2-15.

McFarland, D. (1971). *Feedback mechanisms as animal behaviour*. London: Academic Press.

McGinn, D., Raymond, J., & Joseph, N. (2002). Brave new job hunt. *Newsweek, 140*(13), 54-57.

McKenzie, W. (2004). *Hacker manifesto*. Cambridge: Harvard University Press.

McNamara, J. (2003). *Secrets of computer espionage: tactics and countermeasures*. Indianapolis: Wiley Publishing, Inc.

McQuade, S. C. (2005). *Understanding and managing cybercrime*. Boston: Allyn & Bacon.

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

Mead, G. H. (1934). *Mind, self, and society*. Chicago: University of Chicago Press.

Mecham, M. (2002). Cyber uncoordinated. *Aviation Week & Space Technology, 157*(5), p. 17.

Medd, R. (1997). International terrorism on the eve of the new millennium. *Studies in Conflict and Terrorism, 20*(3), 208-282.

Mehlmann, A. (2000). *The game's afoot! Game theory in myth and paradox*. Providence, RI: American Mathematical Society.

Mercer, L. D. (2004). Computer forensics characteristics and preservation of digital evidence. *FBI Law Enforcement Bulletin, 73*(3), 28-32.

Merriam, S. B. (1988). *Case study research in education: A qualitative approach*. San Francisco: Jossey-Bass Publishers.

Messmer, E. (2005). DoD targets child porn on military PCs. *Network World*, p. A1.

Metcalfe, R. (1993). Computer/network interface design: Lessons from Arpanet and Ethernet. *IEEE Journal on Selected Areas in Communications, 11*(2), 173-180.

Metz, C. (2004). The IM security threat? *PC Magazine, 23*(14), p. 20.

Meyer, J. W., & Rowan, B. (1977). Institutional organizations: Formal structures as myth and ceremony. *American Journal of Sociology, 80*, 340-363.

McFadden, R. D. (1997, March 11). Limits on cash transactions cut drug-money laundering. *New York Times,* p. 1.

Midgley, G. (Ed.) (2003). *Systems thinking*. London: Sage Publications.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35-57.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: A sourcebook of new methods*. Beverly Hills: Sage Publications.

Miller, C., Matusitz, J., O'Hair, D., & Eckstein, J. (in press). The complexity of terrorism: Groups, semiotics, and the media. In D. O'Hair, R. Heath, K. Ayotte, & G. R. Ledlow (Eds.), *Terrorism: Communication and rhetorical perspectives*. Cresskill, NJ: Hampton Press.

Miller, J. (1978). *Living systems*. New York: McGraw Hill.

Milner, J. (1995). A Nobel Prize for John Nash. *Mathamatical Intelligencer, 17*(3), 7-17.

Milone, M. (2003). Hacktivism: Securing the national infrastructure. *Knowledge, Technology, & Policy, 16*(1), 75-103.

Mingers, J. (1994). *Self-producing systems: Implications and applications of autopoiesis*. New York: Plenum Publishing.

Mishler, E. G. (1986). *Research interviewing: Context and narrative*. Cambridge, MA: Harvard University Press.

Mishler, E. G. (1995). Models of narrative analysis: A typology. *Journal of Narrative and Life History, 5*(2), 87-123.

Misztal, B. A. (1996). *Trust in modern societies*. Cambridge, UK: Polity Press.

Mitchell, S. (1998). Native rebellion in the Pisidian Taurus. In K. Hopwood (Ed.), *Organised crime in Antiquity* (pp. 155-175). London: Duckworth.

Mitchell, W. J. (1995). *City of bits*. Cambridge, MA: MIT Press.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis: Wiley Publishing, Inc.

Mitnick, K. D., & Simon, W. L. (2005). *The art of intrusion: The real stories behind the exploits of hackers, intruders and deceivers*. Indianapolis: Wiley Publishing, Inc.

McNamara, J. (2003). *Secrets of computer espionage: tactics and countermeasures*. Indianapolis, IN: Wiley Publishing, Inc.

Mokhiber, R. (2000). White collar crime spree. *Multinational Monitor, 21*(7), p. 38.

Monge, P. R. (1987). The network level of analysis. In C. R. Berger & S. H. Chaffee (Eds.), *Handbook of communication science* (pp. 239-270). Newbury Park, CA: Sage Publications.

Monge, P. R., & Contractor, N. S. (2001). Emergence of communication networks. In F. M. Jablin & L. L. Putman (Eds.). *The new handbook of organizational*

communication: Advances in theory, research, and methods (pp. 440-502). Thousand Oaks, CA: Sage Publications.

Monge, P. R., & Contractor, N. S. (2003). *Theories of communication networks*. New York: Oxford University Press.

Monge, P. R., & Fulk, J. (1999). Communication technology for global network organizations. In G. Desanctis & J. Fulk (Eds.), *Shaping organizational form: Communication, connection, and community* (pp. 70-101). Thousand Oaks, CA: Sage Publications.

Monteith, M., & Winters, J. (2002). Why we hate. *Psychology Today, 35*(3), 44-65.

Moore, C. (2005). Cyber sleuths. *Career World, 34*(1), 6-9.

Moore, D., & Hebeler, J. (2001). *Peer-to-peer: Building Secure, scalable, and manageable networks*. Boston: McGraw-Hill.

Moreno, J. L. (1934). *Who shall survive? Foundations of sociometry, group psychotherapy, and sociodrama*. Washington, DC: Nervous and Mental Disease Publishing Company.

Mory, E. (2003). Feedback research revisited. In D. H. Jonassen (Ed.), *Handbook of research for educational communications and technology* (pp. 919-956). New York: Simon & Schuster Macmillan.

Motter, A., & Lai, Y. C. (2002). Cascade-based attacks on complex network. *Physical Review, 66*, 65-68.

Mounier, J., Peckel, E., Rose, M., Lopez, S., Leisy, M., & Arnold, G. (2005). Spam. *Skiing, 57*(5), 16-20.

Murdock, G. P. (1965). *Culture and society*. Pittsburgh, PA: University of Pittsburgh Press.

Musalia, J. (2005). Gender, social networks, and contraceptive use in Kenya. *Sex Roles: A Journal of Research, 12*(4), 10-24.

Mutton, P. (2004). *IRC hacks*. Cambridge, MA: O'Reilly Media.

Nakada, M., & Tamura, T. (2005). Japanese conceptions of privacy: An intercultural perspective. *Ethics and Information Technology, 7*(1), 27-36.

Nakamura, M., Shaver, J. M., & Yeung, B. (1996). An empirical investigation of joint venture dynamics: Evidence from U.S.-Japan joint ventures. *International Journal of Industrial Organization, 14*, 521-541.

Nash, J. (1950). Equilibrium points in n-person games. *Proceedings of the National Academy of the USA, 36*(1), 48-49.

Neel, J. J. (2005). Game theory can be used to analyze cognitive radio. *Electronic Engineering Times, 1386*, 69-72.

Neumann, J. von, & Morgenstern, O. (1944). *Theory of games and economic behavior*. Princeton: Princeton University Press.

Newth, D., & Ash, J. (2004). *Evolving cascading failure resilience in complex networks*. Proceedings of the Eighth Asia Pacific Symposium on Intelligent and Evolutionary Systems. Cairns, Australia.

Nissenbaum, H. (2001). Securing trust online: Wisdom or oxymoron? *Boston University Law Review, 81*, 101-130.

Nohria, N., & Eccles, R. G. (Eds.) (1992). *Networks and organizations: Structure, form, and action*. Boston, MA: Harvard Business School Press.

Nonaka, I., & Takeuchi, H. (1994). A dynamic theory of organizational knowledge creation. *Organizational Science, 5*(1), 14-37.

Nordlinger, E. A. (1995). *Isolationism reconfigured*. Princeton, NJ: Princeton University Press.

Norman, D. (1993). *Things that make us smart: Defending human attributes in the age of the machine*. New York: Addision-Wesley.

Nöth, W. (1995). *Handbook of semiotics*. Bloomington, IN: Indiana University Press.

Nutt, J. (1999). *John Donne: The poems*. Basingstoke, England: Palgrave Macmillan.

Oberle, K. (2002). Ethics in qualitative health research. *Annals RCPSC, 35*(8), 563-566.

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

Ohbuchi, K. I., Fukushima, O., & Tedeschi, J. T. (1999). Cultural values in conflict management: Goal orientation, goal attainment, and tactical decision. *Journal of Cross-Cultural Psychology, 30*, 51-71.

Oklahoma Digital Forensics Lab (2005). https://odfl.ou.edu.

Olesen, V. L. (2000). Feminisms and qualitative research at and into the millennium. In N. K. Denzin & Y. S. Lincoln (Eds.), *The handbook of qualitative research* (pp. 215-256). Thousand Oaks, CA: Sage Publications.

Oliver, C. (1991). Strategic responses to institutional processes. *Academy of Management Review, 16*, 145-179.

Oram, A. (2001). *Peer-to-peer: Harnessing the power of disruptive technologies*. New York: O'Reilly Media.

Orda, A., Rom, R., & Shimkin, N. (1993). Competitive routing in multi-user communication networks. *IEEE/ACM Transactions on Networking, 1*(5), 510-521

Osborne, M. J. (2003). *An introduction to game theory*. Oxford: Oxford University Press.

Overgaard, P. B. (1994). Terrorist attacks as a signal of resources. *Journal of Conflict Resolution, 38*(3), 452-478.

Palmer, C. C. (2001). Ethical hacking. *IBM Systems Journal, 40*(3), 769-780.

Park, S. Y., & Yun, G. W. (2004). The impact of internet-based communication systems on supply chain management: An application of transaction cost analysis. *JCMC, 10*(1), Article 12.

Parker, D. S. (2004). *The Battle of the Bulge: Hitler's Ardennes offensive, 1944-1945*. Cambridge, UK: Da Capo Press.

Pastor-Satorras, R., & Vespignani, A. (2001). Epidemic spreading in scale-free networks. *Physical Review Letters, 86*(14), 3200-3203.

Pearson, G., & Hobbs, D. (2004). "E" is for enterprise: Middle level drug markets in ecstasy and stimulants. *Addiction Research & Theory, 12*(6), 565-576.

Perlmutter, D. D. (2000). *Policing the media: Street cops and public perceptions of law enforcement*. Thousand Oaks, CA: Sage Publications.

Pervin, L.A. (1984). *Personality*. New York: Wiley.

Peters, M. A. (2004). Postmodern terror in a globalized world. *Globalization, 3*, 1-14.

Peterson, M. M. (2002). Agencies, companies urged to set guidelines for fighting cyberterrorism. *National Journal's Technology Daily*, p. A4.

Phillips, A., Nelson, B., Enfinger, F., & Steuart, C. (2005). *Guide to computer forensics and investigations*. Boston: Course Technology.

Philipsen, G. (1992). *Speaking culturally: Explorations in social communication*. New York: State University of New York Press.

Pike, K. L. (1967). *Language in relation to a unified theory of structure of human behavior*. The Hague: Mouton.

Pillar, P. R. (2001). *Terrorism and U.S. foreign policy*. Washington D.C.: Brookings Institution Press.

Polanyi, M. (1966). *The tacit dimension*. Garden City, NY: Doubleday.

Polanyi, M. (1975). Personal knowledge. In M. Polnayi & H. Prosch (Eds.), *Meaning* (pp. 22-45). Chicago: University of Chicago Press.

Popper, K. R. (1945). *The open society and its enemies*. Routledge: London.

Popper, K. R. (1961). *The poverty of historicism*. Routledge: London.

Poppo, L., & Zenger, T. R. (1998). Testing alternative theories of the firm: Transaction cost, knowledge-based, and measurement explanations for make-or-buy decisions in information services. *Strategic Management Journal, 19*, 853-877.

Posner, G. L. (2003). *Why America slept: The failure to prevent 9/11*. New York: Simon & Schuster.

Poster, M. (1997). Cyberdemocracy: The Internet and the public sphere. In D. Porter (Ed.), *Internet culture* (pp. 201-218). New York: Routledge.

Poster, M. (2001). *What's the matter with the Internet?* Minneapolis: University of Minnesota Press.

Potter, G. W. (1994). *Criminal organizations*. Prospect Heights, IL: Waveland Press.

Poundstone, W. (1992). *Prisoner's dilemma: John von Neumann, game theory, and the puzzle of the bomb*. New York: Doubleday.

Prigogine, I. (1969). *Structure, dissipation, and life: Theoretical physics and biology*. Amsterdam: North-Holland Publishing Company.

Prosise, C., & Mandia, K. (2001). *Incident response: Investigating computer crime*. New York: McGraw-Hill.

Provan, K., & Milward, H. B. (1995). A preliminary theory of interorganizational network effectiveness: A comparative study of four community mental health system. *Administrative Science Quarterly, 40*, 1-33.

Radcliff, D. (2002). The security sentinels. *Computerworld, 36*(15), 34-35.

Radcliffe-Brown, A. R. (1940). On social structure. *Journal of the Royal Anthropological Institute, 70*, 1-12.

Raider, H. J. (1998). Market structure and innovation. *Social Science Research, 27*, 1-21.

Rajak, T. (1984). *Josephus: The historian and his society*. Philadelphia, PA: Fortress Press.

Ranstorp, M. (1994). Hizbollah's command leadership: Its structure, decision-making and relationship with Iranian clergy and institutions. *Terrorism and Political Violence, 6*(3), 300-318.

Rapoport, A. (Ed.). (1974). *Game theory as a theory of conflict resolution*. Boston: D. Reidel Publishing Company.

Rashbaum, W. K. (2001, January 6). Police ponder fallout in feud over airports. *New York Times*, p. B3.

Rawlings, L. (1998). Condottieri and clansmen: Early Italian raiding, warfare, and the state. In K. Hopwood (Ed.), *Organised crime in Antiquity* (pp. 97-127). London: Duckworth.

Regan, T. (1999). Balkans war reaches our corner of the Web. *Christian Science Monitor, 91*(97), p. 15.

Remer, R. (2005). An introduction to chaos theory for psychodramatists. *Journal of Group Psychotherapy, Psychodrama, & Sociometry, 5*8(3), 130-150.

Renzulli, L. A., & Aldrich, H. (2005). Who can you turn to? Tie activation within core business discussion networks. *Social Forces, 84*(1), 323-341.

Report of the Defense Science Board Task Force on Information Warfare Defense (1996, November). *Department of Defense*, Washington, p. A3.

Report on Love Bug Virus Submitted (2000, June 13). *New York Times*, p. A1.

Rheingold, H. (1998). *The virtual community*. New York, NY: Simon & Schuster.

Riebling, M. (2002). *Wedge: The secret war between the FBI and the CIA*. New York: Simon & Schuster.

Riessman, C. K. (1993). *Narrative analysis*. Thousand Oaks, CA: Sage Publications.

Rist, O., & Chee, B. (2004). EnCase keeps tabs on compliance. *InfoWorld, 26*(41), 31-32.

Robb, J. (2004). Scale-free networks and terrorism. www.globalguerrillas.typepad.com.

Roberts, P. F. (2005). School studies net attacks. *eWeek, 22*(19), p. 18.

Roberts, S. (1979). *Order and dispute: An introduction to legal anthropology*. Harmondsworth, England: Penguin Books.

Rohan, R., & Donaldson, S. A. (2002). Social engineering. *Black Enterprise, 33*(2), 53-55.

Ronfeldt, D. (2000). Social science at 190 MPH on NASCAR's biggest superspeedways. *First Monday, 5*(2), 10-19.

Rosett, A. I. (1976). *Justice by consent: Plea bargains in the American courthouse*. New York: Lippincott Williams & Wilkins.

Roson, R. (2001). Assessing the option value of a publicly provided service: The case of local transport. *Urban Studies, 38*(8), 1319-1327.

Ross, A. (1988). *Universal abandon? The politics of postmodernism.* Minneapolis, MN: University of Minnesota Press.

Roth, C. (1959). The Zealots in the war of 66-73. *Journal of Semitic Studies, 4*, 332-355.

Rowley, T. J. (1997). Moving beyond dyadic ties: A network theory of stakeholder influences. *Academy of Management Review, 22*, 887-910.

Rubin, H., & Rubin, I. (1995). *Qualitative interviewing: The art of hearing data*. Thousand Oaks, CA: Sage Publications.

Rutten, R. (2004). Inter-firm knowledge creation: A re-appreciation of embeddedness from a relational perspective. *European Planning Studies, 12*(5), 659-673.

Sadler, R. L. (2005). *Electronic media law*. Thousand Oaks, CA: Sage Publications.

Sagarin, B. J., Cialdini, R. B., Rice, W. E., & Serna, S. B. (2002). Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion. *The Journal of Personality & Social Psychology, 83*(3), 526-541.

Saint-Onge, H., & Wallace, D. (2003). *Leveraging communities of practice*. Burlington, MA: Butterworth Heinemann.

Saksena, N. S. (1985). *Terrorism: A weapon in international politics*. India: Abhinav Publications.

Salem, D. A., Anne Bogat, D., & Reid, C. (1997). Mutual help goes on-line. *Journal of Community Psychology, 25*(2), 189-207.

Sandler, T. & Hartley, K. (1995). *The economics of defense*. Cambridge: Cambridge University Press.

Sandler, T., & Lapan, H. E. (1988). The calculus of dissent: An analysis of terrorists' choice of targets. *Synthèse, 76*(2), 245-261.

Sandler, T., Tschirhart, J. T., & Cauley, J. (1983). A theoretical analysis of transnational terrorism. *American Political Science Review, 77*(4), 36-54.

Sassen, F. (2002) *Global networks: Linked cities*. New York: Routledge.

Sataloff, R. T. (2004). Chaos. *ENT: Ear, Nose & Throat Journal, 83*(2), p. 80.

Scheurich, J. J. (1992). *The paradigmatic transgressions of validity*. Unpublished manuscript.

Schiano, D. J. (1999). Lessons from LambdaMOO: A social, text-based virtual environment. *Presence: Teleoperators & Virtual Environments, 8*(2), 127-170.

Schmid, A. P. (1984). *Political terrorism: A research guide to concepts, theories, data bases, and literature*. Amsterdam: Transaction Books.

Schmid, A. P. (1996). The links between transnational organized crime and terrorist crimes. *Transnational Organized Crime, 2*(4), 40-82.

Schneier, B. (1996). *Applied cryptography*. New York: Wiley.

Schneier, B. (2005). Titan Rain. www.schneier.com/blog/archives/2005/12/titan_rain_1.html.

Schwandt, T. A. (2001). *Dictionary of qualitative inquiry*. Thousand Oaks, CA: Sage Publications.

Schwartau, W. (1996). *Cyberterrorism: Protecting your personal security in the electronic age*. New York: Thunder Mouth Press.

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

Scott, J. (1991). *Social network analysis*: *A handbook*. Thousand Oaks, CA: Sage Publications.

Scott, J. (2000). *Social network analysis*: *An introduction*. New York: Sage Publications.

Scott, J. (2004). *Social network analysis: A handbook*. Thousand Oaks, CA: Sage Publications.

Scott, J. L. (1991). Reputation building in hostage incidents. *Defence Economics, 2*(2), 209-218.

Seale, C. (1999). Quality in qualitative research. *Qualitative Inquiry, 5*(4), 465-478.

Sebeok, T. A. (1994). *Signs: An introduction to semiotics*. Toronto: University of Toronto Press.

Seffers, G. I. (1999, March 15). Stealthy new software enhances hacker arsenal. *Defense News*, p. 3.

Selten, R. (1988). A simple game model of kidnappings. In R. Selten (Ed.), *Models of strategic rationality* (pp. 77-93). Boston: Kluwer Academic Press.

Semmelroth, J. (2006). Keep your small network sailing safely in dangerous waters. *Computers in Libraries, 26*(1), 6-48.

Shafritz, J. M., & Ott, J. S. (1996). *Classics of organization theory*. New York: Harcourt Brace.

Sharp, D. (2006). Long-term effects of sarin. *Lancet, 367*(9505), 95-97.

Shaw, B. (1984). Bandits in the Roman Empire. *Past and Present, 105*, 3-51.

Shaw, B. (1990). Bandit highlands and lowland peace: The mountains of Isauria-Cilicia. *Journal of the Economic and Social History of the Orient, 33*, 199-233.

Sherwell, P., Nikolic, S., & Strauss, J. (1999, April 7). Clinton orders "cyber-sabotage" to oust Serb leader. *Daily Telegraph*, p. A1.

Shimomura, T., & Markoff, J. (1996). *Takedown: The pursuit and capture of Kevin Mitnick, America's most wanted computer outlaw – By the man who did it*. New York: Hyperion Books.

Shukla-Mehta, S., & Albin, R. W. (2003). Twelve practical strategies to prevent behavioral escalation in classroom settings. *Clearing House, 77*(2), 50-56.

Silverman, D. (1993). *Interpreting qualitative data: Methods for analyzing talk, text, and interaction*. Thousand Oaks, CA: Sage Publications.

Silverman, S. (1977). Patronage as myth. In E. Gellner & J. Waterbury (Eds.), *Patrons and clients in Mediterranean societies* (pp. 7-19). London: Duckworth.

Simmel, G. (1950). *The sociology of George Simmel*. New York: The Free Press.

Simpson, L. (1995). *Technology, time, and the conversations of modernity*. New York: Routledge.

Simpson, M. (2005). *Hands-on ethical hacking and network defense*. Washington: Course Technology.

Sinha, D. (1997). A cultural perspective on organizational behavior in India. In P. C. Earley & M. Erez (Eds.), *New perspectives on international industrial/ organizational psychology* (pp. 53-74). San Francisco: Lexington.

Sinha, D., & Tripathi, R. C. (1994). Individualism in a collectivist culture: A case of coexistence of opposites. In U. Kim, H. C. Triandis, C. Kagitcibasi, S. C. Choi, & G. Yoon (Eds.), *Individualism and collectivism: Theory, method, and applications* (pp. 123-136). Thousand Oaks, CA: Sage Publications.

Slay, J., Darzanos, K., Quirchmayr, G., & Koronios, A. (2003). *Towards a mature understanding of "culture" in information systems security research*. IFIP Joint WG 8.2 + 9.4 Conference, Athens University of Economics and Business, Greece, June 2003.

Sloan, S. (1995). Terrorism: How vulnerable is the United States. In S. Pelletiere (Ed.), *Terrorism: National security policy and the home front* (pp. 1-40). Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College.

Sloan, S., & Kearney, R. (1978). Non-territorial terrorism: An empirical approach to policy formation. *Conflict: An International Journal for Conflict and Policy Studies, 1*(1), 10-23.

Smith, C. (1997). *Death of a little princess: The tragic story of the murder of JonBenet Ramsey*. Bayton, TX: St. Martin's Paperbacks.

Smith, H. J. (2001). Information privacy and marketing: What the U.S. should (and shouldn't) learn from Europe. *California Management Review, 43*(2), 8-33.

Smith, M. (1971). Zealots and Sicarii: Their origins and relation. *Harvard Theological Review, 64*, 1-19.

Smith, P. B., & Bond, M. H. (1993). *Social psychology across cultures*. Cambridge, UK: Cambridge University Press.

Smith, S. (2000). College starts cyber forensics program. *Community College Week, 12*(13), p. 20.

Sobchack, V. (1992). *The address of the eye: A phenomenology of film experience.* Princeton, NJ: Princeton University Press.

Sparks, J. (2005). Who's got my keys? *Newsweek, 146*(25), p. E2.

Stallings, W. (1998). *Cryptography and network security: Principles and practice*. Upper Saddle River, NJ: Prentice Hall.

Stengers, I., & Prigogine, I. (1997). *The end of certainty: Time, chaos, and the new laws of nature*. New York: Free Press.

Stewart, L. (1989). *Does God play dice: Mathematics of chaos*. Oxford: Blackwell.

Stewart, T. A. (1996). The great conundrum: You vs. the team. *Fortune, 134*, 165-166.

Stohl, C. (1989). *The cuckoo's egg*. New York: Simon & Schuster.

Stohl, C. (1995). *Organizational communication: Connectedness in action*. Thousand Oaks, CA: Sage Publications.

Stone, A. (2001, January 11). USA's dependence on satellites places nation at risk: Militarization of space controversial, perhaps inevitable. *USA Today*, p. A1.

Strauss, A. (1978). A social world perspective. *Studies in Symbolic Interaction, 1*, 119-128.

Strauss, A. (1982). Social worlds and legitimation processes. *Studies in Symbolic Interaction, 4*, 171-190.

Strogatz, S. H. (2003). *SYNC: The emerging science of spontaneous order*. New York: Theia.

Sun Tzu (2003). *The art of war*. London: Penguin Books.

Swartz, J. (2003). Tech pros get to know their enemy. *USA Today*, p. A3.

Swartz, J. (2004). Cyberterror impact, defense under scrutiny. *USA Today*, p. A2.

Swazo, N. K. (2004). Primacy or world order? The new Pax Americana. *International Journal on World Peace, 21*(1), 15-37.

Tajfel, H. (1978). *Differentiation between social groups*. London: Academic Press.

Tanaka, J. (2001). Don't get burned. *Newsweek, 138*(8), 52-53.

Telushkin, J. (1991). *Jewish literacy*. New York: William Morrow and Co.

Tesauro, G. (1994). TD-Gammon, a self-teaching backgammon program achieves master-level play. *Neural Computation, 6*, 215-219.

Thackeray, J. (1968). *Josephus: The man and the historian*. New York: Ktav Publishing House.

Thaddeus, J. (2000). The confessions of a white hat hacker. *Computerworld, 34*(49), p. 72.

Thibodeau, P. (2002). White House pushes voluntary data sharing. *Computerworld, 36*(31), p. 10.

Thilmany, J. (2004). Rifling for evidence. *Mechanical Engineering, 126*(10), 18-20.

Thornburgh, N., Forney, M., Bennett, B., Burger, T. J., & Shannon, E. (2005). The invasion of the Chinese cyberspies (and the man who tried to stop them). *Time, 166*(10), 34-39.

Thussu, D. K. (2001). *International communication: Continuity and change*. Oxford: Oxford University Press.

Todorov, T. (1977). *The poetics of prose*. Ithaca, NY: Cornell University Press.

Trabelsi, Z. (2005). Switched network sniffers detection technique based on IP packet routing. *Information Systems Security, 14*(4), 51-60.

Tran, L. (1996). The concept of privacy in intercultural communication. In A. Barthel (Ed.), *Intercultural interaction and development: Converging perspectives* (pp. 210-217). Sydney, Australia: University of Technology-Sydney.

Trauth, E. M. (Ed.). (2001). *Qualitative research in IS: Issues and trends*. USA: Idea Group Publishing.

Triandis, H. C. (1995). *Individualism and collectivism*. Boulder, CO: Westview.

Trigg, R. (1993). *Understanding social science*. Oxford, England: Blackwell.

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

Turkle, S. (1992). *Psychoanalytic politics: Freud's French revolution*. London: Free Association Books.

Turkle, S. (1995). *Life on the screen: Identity in the age of the Internet*. New York, NY: Simon and Schuster.

Turner, P. E. (2005). Cheating viruses and game theory. *American Scientist, 93*(5), 428-435.

Uzzi, B. (1996). The sources and consequences of embeddedness for the economic performance of organizations: the network effect. *American Sociological Review, 61*, 674-698.

Vankin, J., & Walen, J. (2004). *The 80 greatest conspiracies of all time*. New York: Citadel Press.

Vegh, S. (2002). Hacktivists or cyberterrorists? The changing media discourse on hacking. *First Monday, 7*(10), 12-25.

Verhoeven, L. (2000). Components in early second language reading and spelling. *Scientific Studies of Reading, 4*(4), 313-330.

Verton, D. (1999, May 3). New cyberterror threatens AF. *Federal Computer Week*, p. A1.

Verton, D. (2001a). Black hat highlights real danger of script kiddies. *Computerworld, 35*(30), p. 17.

Verton, D. (2001b). FBI operation penetrates hacker underground. *Computerword*, p. A1.

Verton, D. (2002a). *The hacker diaries: Confessions of teenage hackers*. Portland: Osborne/McGraw-Hill.

Verton, D. (2002b). Web sites seen as terrorist aids. *Computerword*, p. A1.

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

Verton, D. (2003b). Private sector key to cybercrime fight. *Computerworld, 37*(46), p. 12.

Vidanage, H. R. (2006). Apparition of the predator. *The Lanka Academic, 6*(281), p. 3.

Vijayan, J. (2005). Targeted attacks pose new security challenge. *Computerworld, 39*(26), 1-16.

Virilio, P. (2000). *From modernism to hypermodernism and beyond*. London: Sage Publications.

Voronov, M., & Singer, J. A. (2002). The myth of individualism-collectivism: A critical review. *The Journal of Social Psychology, 142*(4), 461-480.

Wakabayashi, M. (2002). Urban space and cyberspace: Urban environment in the age of media and information technology. *International Journal of Japanese Sociology, 11*(1), 6-18.

Wall, D. (2001). *Crime and the Internet*. London: Routledge.

Walsham, G. (1993). *Interpreting information systems in organizations*. Wiley, UK: Chichester.

Wasserman, S., & Faust, K. (1994). *Social network analysis*. Cambridge, MA: Cambridge University Press.

Watts, D. J. (1999a). Networks, dynamics, and the small-world phenomenon. *American Journal of Sociology, 13*(2), 493-527.

Watts, D. J. (1999b). *Small worlds: The dynamics of networks between order and randomness*. Princeton, NJ: Princeton University Press.

Wayner, P. (1996). *Disappearing cryptography: Setting up networks with hidden communications*. Boston: AP Professional.

Webb, C. L. (2001, August 17). CACI profit surged 58% in quarter: Government work lifts tech firm. *Washington Post*, p. A3.

Wees, H. van (1998a). The law of gratitude: Reciprocity in anthropological theory. In C. Gill et al. (Eds.), *Reciprocity in ancient Greece* (pp. 13-49). Oxford: Oxford University Press.

Wees, H. van (1998b). The Mafia of early Greece: Violent exploitation in the seventh and six centuries BC. In K. Hopwood (Ed.), *Organised crime in Antiquity* (pp. 1-51). London: Duckworth.

Wehrfritz, G., & Vitisca, G. (2000). Raiding the Love Bug. *Newsweek, 135*(21), 44-45.

Weinberg, G. M. (1975). *An introduction to general systems thinking*. New York: Wiley.

Wellman, B. (2005). Community: From neighborhood to network. *Communication of the ACM, 48*(10), 53-55.

Wellman, B., & Berkowitz, S. D. (Eds.) (1988). *Social structures: A network approach*. Cambridge, MA: Cambridge University Press.

Wenger, E. (1998). *Communities of practice: Learning, meaning, and identity*. Cambridge, England: Cambridge University Press.

Wenger, E., McDermott, R. A., & Snyder, W. (2002). *Cultivating communities of practice: A guide to managing knowledge*. Boston: Harvard Business School Press.

Wengraf, T. (2001). *Qualitative research interviewing: Semi-structured, biographical and narrative methods*. Thousand Oaks, CA: Sage Publications.

West, R., & Turner, L. H. (2000). *Introducing communication theory*. Mountain View, CA: Mayfield Publishing Company.

Whitby, M. (1998). The violence of the circus factions. In K. Hopwood (Ed.), *Organised crime in Antiquity* (pp. 229-253). London: Duckworth.

Wiener, N. (1961). *Cybernetics*: *The control and communication in the animal and the machine*. Cambridge, MA: MIT Press.

Wigand, R. (1997). Electronic commerce: Definition, theory and context. *The Information Society, 13*, 1-16.

Williams, K. (2001, October 11). U.S. seeks to build secure online network. *Washington Post*, p. A10.

Williams, K. (2003). *Understanding media theory*. London: Arnold.

Williams, L., & Sewpaul, V. (2004). Modernism, postmodernism, and global standards setting. *Social Work Education, 23*(5), 555-565.

Williams, P. (2001). Transnational criminal networks. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars* (pp. 61-97). Santa Monica, CA: RAND.

Winograd, T., & Flores, F. (1986). *Understanding computers and cognition: A new foundation for design*. Norwood, NJ: Ablex.

Wood, J. T. (1994). *Gendered lives: Communication, gender, and culture*. Belmont, CA: Wadsworth.

World Health Organization (1998). *Health promotion glossary*. Geneva: WHO/HPR/HEP/98.1.

Wright, M. M. (2005). Finding a place in cyberspace. *Frontiers: A Journal of Women Studies, 26*(1), 48-59.

Yarbrough, B. V., & Yarbrough, R. M. (1999). Governance structures, insider status, and boundary maintenance. *Journal of Biometrics, 1*, 289-310.

Yorke, J. (2005). The world's biggest ideas: Chaos. *New Scientist, 187*(2517), p. 37.

Young-Ybarra, C., & Wiersema, M. (1999). Strategic flexibility in information technology alliances: The influence of transaction cost economics and social exchange theory. *Organization Science, 10*(4), 439-459.

Zangrilli, A. (2002). Twenty questions with an electronic evidence expert. *Modern Practice, 4*(1), 10-21.

Zanini, N., & Edwards, S. J. A. (2001). The networking of terror in the Information Age. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars* (pp. 29-60). Santa Monica, CA: RAND.

Zarefsky, D. (1994). The postmodern public. *Vital Speeches of the Day, 60*(10), 308-315.

Zeeuw, G. De (1992). Autopoiesis and social systems. *International Journal of General Systems, 21*(2), 185-186.

Zehr, H. (1978). *Crime and the development of modern society*. London: Penguin Books.

Zeleny, M. (Ed.). (1981). *Autopoiesis: A theory of living organization*. New York: North Holland.

Zepp, C. (1999). Virtuality community: Hackers. *Sociology and the Internet, 4*(3), 1-14.

Ziff, D. J. S. (2005). Fourth Amendment limitations on the execution of computer searches conducted pursuant to a warrant. *Columbia Law Review, 105*(3), 841-872.

Zivkovic, M., Buddhikot, M. M., Van Bemmel, J., & Lagerberg, K. (2005). Authentication across heterogeneous networks. *Bell Labs Technical Journal, 10*(2), 39-56.

Appendix A

INFORMED CONSENT
TO PARTICIPATE IN A RESEARCH STUDY

PROJECT TITLE:	Cyberterrorism: A Postmodern View of Networks of Terror and How Computer Security Experts and Law Enforcement Officials Fight Them
PRINCIPAL INVESTIGATOR:	Jonathan Matusitz
CONTACT INFORMATION:	(405) 579-8679, matusitz@ou.edu

You are being asked to volunteer for a research study. This study is being conducted at the University of Oklahoma. You were selected as a possible participant because your supervisor told me that you were a computer security expert and that you would be willing to participate in my study on computer security. Please read this form and ask any questions that you may have before agreeing to take part in this study.

The sponsor of the study

The sponsor of the study is the Department of Communication at the University of Oklahoma. I, Jonathan Matusitz, am the principal investigator.

Purpose of the Research Study

The purpose of this study is to investigate how cyberterrorists create networks in order to engage in malicious activities against the Internet and computers. By the same token, the purpose of my study is also to understand how computer security labs (i.e., in universities) and various agencies (that is, law enforcement agencies such as police departments and the Federal Bureau of Investigation) create joint networks in their fight against cyberterrorists. This idea of analyzing the social networks of two opposing sides rests on the premise that it takes networks to fight networks.

Procedures

If you agree to be in this study, you will be asked to do the following things. I will use the method of interviewing. I will ask you to answer general questions about cyberthreat and about networks of cyberterrorists. The interview will last for about one hour. An audio-tape recorder will be used to record the interview because I need to transcribe the information that you will give me. Your name will NOT be mentioned. Your participation is totally anonymous. You can use a nickname.

Risks and Benefits of Being in the Study

The study has no risks involved. If you feel uncomfortable answering my questions, feel free not to answer them.

There are no benefits involved regarding your participation in my study.

Compensation

Participation in this study is free and no monetary or any type of compensation is given to the participants.

Voluntary Nature of the Study

Participation in this study is voluntary. Your decision whether or not to participate will not result in penalty or loss of benefits to which you are otherwise entitled. If you decide to participate, you are free to not answer any question or withdraw at any time.

Confidentiality

The records of this study will be kept private. In published reports, there will be no information included that will make it possible to identify the research participant. Research records will be stored securely. I will store the transcriptions of the data on my computer and keep these transcriptions safe by locking them into a program file that can only be opened with a password. I will keep the audio-tapes in a private room that has a safe. I will destroy the audio-tapes as soon as I transcribe all the information recorded on those tapes. Only approved researchers will have access to the records. When the tape recordings are made, only my advisor will have access to them. He will use them for educational purposes. Again, these tapes will be erased as soon as I transcribe the information that you will give me.

Audio Taping of Study Activities:

To assist with accurate recording of participant responses, interviews may be recorded on an audio recording device/video recording device. Participants have the right to refuse to allow such taping without penalty. Please select one of the following options.

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

Contacts and Questions:

The researcher(s) conducting this study can be contacted at (405) 579-8679 or matusitz@ou.edu (for Jonathan Matusitz, the principal investigator) and (405) 325-2349 or kramer@ou.edu (for Dr. Eric Kramer, the faculty sponsor). You are encouraged to contact the researcher(s) if you have any questions.

If you have any questions about your rights as a research participant, you may contact the University of Oklahoma – Norman Campus Institutional Review Board (OU-NC IRB) at 405.325.8110 or irb@ou.edu.

You will be given a copy of this information to keep for your records. If you are not given a copy of this consent form, please request one.

STATEMENT OF CONSENT

I have read the above information. I have asked questions and have received satisfactory answers. I consent to participate in the study.

Signature _____ Date _____

Appendix B

Interview Protocol

In this study, about twenty interview questions were asked to each of the twenty-seven participants. Below is the interview protocol that lists all the questions:

What is cyberterrorism?

What are the motivations to engage in cyberterrorism?

What does a network of cyberterrorists look like?

What do cyberterrorists do in those networks of terror?

Describe the role of nodes and hubs [minor and important actors] in the networks of cyberterrorists.

Describe the degree of centrality in cyberterrorist networks.

Describe the culture or way of life of cyberterrorist networks.

What types of networks do you use to combat cyberterrorism?

What do you do in those networks?

Is it necessary to create networks against networks? Explain.

Describe the downsides to networking with other agencies.

Are those networks formal or informal? Explain.

Describe the role of nodes and hubs [minor and important actors] in your networks.

Describe the degree of centrality in your networks.

Describe a direct interaction or conflict between cyberterrorist networks and cyber forensics experts' (and law enforcement agents') networks?

How can a network knock down another network?

What game or strategy do cyberterrorists use?

What game or strategy do cyber security experts and law enforcement officials use?

Could you give me an example of a collaborative game strategy between the two sides?

Could you give me an example of a non-collaborative game strategy between the two sides?

Do cyberterrorists make the rules of the game or do they go along?