GLOBAL RESPONSE TO CYBERTERRORISM AND CYBERCRIME: A MATRIX FOR INTERNATIONAL COOPERATION AND VULNERABILITY ASSESSMENT

Suleyman Ozeren, B.A., M.S.

Dissertation Prepared for the Degree of

DOCTOR OF PHILOSOPHY

UNIVERSITY OF NORTH TEXAS

August 2005

APPROVED:

Samantha K. Hastings, Major Professor and
Interim Dean of School of Library and
Information Science
Brian O'Connor, Committee Member
Kall D. Loper, Committee Member
Sandra L. Terrell, Dean of the Robert B.
Toulouse School of Graduate Studies

Ozeren, Suleyman, *Global response to cyberterrorism and cybercrime: A matrix for international cooperation and vulnerability assessment*. Doctor of Philosophy (Information Science), August 2005, 239 pp., 26 tables, 7 figures, references, 211 titles.

Cyberterrorism and cybercrime present new challenges for law enforcement and policy makers. Due to its transnational nature, a real and sound response to such a threat requires international cooperation involving participation of all concerned parties in the international community. However, vulnerability emerges from increased reliance on technology, lack of legal measures, and lack of cooperation at the national and international level represents real obstacle toward effective response to these threats. In sum, lack of global consensus in terms of responding to cyberterrorism and cybercrime is the general problem.

Terrorists and cyber criminals will exploit vulnerabilities, including technical, legal, political, and cultural. Such a broad range of vulnerabilities can be dealt with by comprehensive cooperation which requires efforts both at the national and international level. “Vulnerability-Comprehensive Cooperation-Freedom Scale” or “Ozeren Scale” identified variables that constructed the scale based on the expert opinions. Also, the study presented typology of cyberterrorism, which involves three general classifications of cyberterrorism; Disruptive and destructive information attacks, Facilitation of technology to support the ideology, and Communication, Fund raising, Recruitment, Propaganda (C-F-R-P). Such a typology is expected to help those who are in a position of decision-making and investigating activities as well as academicians in the area of terrorism.

The matrix for international cooperation and vulnerability assessment is expected to be used as a model for global response to cyberterrorism and cybercrime.

ACKNOWLEDGMENTS

First of all, I would like to express my deepest gratefulness and thanks to my patient and loving wife, Sena, who has been a great source of strength all through this work, and my children, Neriman Beyza and Selman. Their love and support during long days and nights of work was of immeasurable value to me.

I would also like to take this opportunity to express my appreciation to the Turkish Nation as whole and in particular to the Turkish National Police for providing me ample opportunity to get this degree. During the course of my dissertation work, there were many people who were instrumental in helping me. Without their guidance, help and patience, I would have never been able to accomplish the work of this thesis. I would like to take this opportunity to convey my deepest appreciation to my dissertation chair, Professor Sam Hastings, committee members Professor Brian O'Connor, and Professor Kall Loper, all of whom were driving factors to the successful completion of the dissertation.

Finally, I would like to express my appreciation to other people who helped me throughout my study, Professor Robert W. Taylor, at the Department of Criminal Justice, at UNT, Professor Susan Brenner, at the School of Law and Technology at Dayton University, Professor Mehmet Ozcan at the Institute for Security Sciences in Turkey, and members of the Turkish National Police.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Introduction

Over the past several years, terrorism has been one of the complex issues faced by government policy makers, analysts, and the public. The complexity of terrorism has emerged not only from the definition of the concept itself but also the tactics that terrorist groups use, the countries that support terrorist groups, and the policies and procedures that have been used to counter terrorist actions by the target countries.

The information age is shaping not only the types of weapons and targets the terrorists select, but also the ways that terrorist groups structure and operate their organizations (Zanini and Edwards, 2001, p. 30). According to Zanini and Edwards, large terrorist organizations are using information technologies, such as computers, telecommunication devices, software, and the Internet to organize and coordinate activities (2001, p. 30).

Criminality originating from new technologies, such as the Internet, wireless communications, and other computer networks creates many challenges for law enforcement around the world (Sussmann 2000). Responding to cyberterrorism and investigating computer-- related crimes pose challenges for law enforcement, as well as the legal system.

The objective of this chapter is to provide a general overview of the research, and it involves several components. First of all, this chapter revealed the definitions of the critical concepts of this research. These concepts are terrorism, cybercrime, information warfare, and cyberterrorism. The first chapter also stated the hypothesis of the research. Finally, it introduced the issue of responding to cybercrime and cyberterrorism and the issue of international cooperation.

Definition of the Concepts

Terrorism

Defining terrorism itself constitutes problems. The most important aspect of defining terrorism is the difficulty to have an agreed upon definition of terrorism. In other words, there is no consensus in the international arena as to what terrorism comprises. The problem emerges from the fact that terrorism is solely a political issue which means a terrorist for one country could be a freedom fighter for another. Furthermore, as Laqueur claimed in 1977

> It can be predicted with confidence that disputes about a comprehensive, detailed definition of terrorism will continue for a long time, that they will not result in consensus and that they will make no noticeable contribution to the understanding of terrorism.

While Laqueur seems to be pessimistic about defining terrorism, time has proven that his statement in fact was true. The ambiguity about the conceptual definition of terrorism leads problems. First of all, it avoids any internationally recognized response policies. Of course Declaration of Human Rights and other international agreements set the scene for the standards in terms of human rights; however, lack of internationally recognized standards in terms of responding terrorism creates confusing, irregularity, and even turmoil. Furthermore, efforts taken by a country which is targeted by terrorists may not create a desired effect since other countries may not consider that group as a terrorist organization. In terms of legal issues, not having a standard as to what terrorism constitutes, while A country criminalize a specific act as terrorism, B country may not have such a law and this will make it impossible for the target country to follow up the investigation and ask for assistance from the B country.

Nevertheless, every country has its own definition of terrorism, even though it may enable them to impose anti-democratic laws and policies. The concept of terrorism has been defined in several ways, and there are different typologies of definitions. In his article, " Terrorism: The Problem of Definition Revisited," Cooper defines terrorism as "intentional generation of massive fear by human beings for the purpose of securing or maintaining control over other human beings" (2001, p. 883).

Enders and Sandler define terrorism as "the premeditated use –or threatened use –of extra-normal violence or force to gain political objectives through intimidation or fear" (1993, p. 829). The US Department of State defines terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience" (1999).

Information Warfare

The definition of information warfare involves different forms. One definition of information warfare is "Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries" (US Department of Defense 1999). This definition focuses on the military side of information warfare. Another military perspective is that information warfare involves "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions, protecting ourselves against those actions, and exploiting our own military information functions" (Fogleman and Widnall, 2002, p. 3). Algiers, on the other hand, defines information warfare as “Actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending one’s own information, information based processes and information systems” (as cited in Galley, 1996). This definition is a general one and may be applicable to wider areas.

According to Nitzberg (2002), from a computer technology perspective, information warfare is defined as “the use (and abuse) of computers and high technology appliances to undermine the computing resources of an adversary.”

Classification of Information Warfare

In his book, *Chaos on the Electronic Superhighway: Information Warfare*, Winn Schwartua, related the concept of information warfare to everything including politics, economy, power, fear, and survival. He even claims that “in information warfare, information age weaponry will replace bombs and bullets,” which are not restricted to the governments of superpowers (Schwartua 1996, p. 16).

He also proposes classification of information warfare. According to him there are three types of information warfare:

Class 1: Personal Information Warfare. This includes attacks against individual privacy. Attacks on the personal computer or use of private information about an individual are possible examples of personal information warfare.

Class 2: Corporate Information Warfare. This classification involves corporate companies and focuses on the issues of competition between companies, industrial espionage, misinformation and the like.

Class 3: Global Information Warfare. This type of warfare is “waged against industries” (p. 195). This level of warfare is waged by the most elite individuals through Internet and other computer network systems according to Schwartau (1996).

Cybercrime

Cybercrime can be regarded as “computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks” (Thomas and Loader,2000, p. 3). In general, cybercrime can be defined as a crime committed in a cyber environment, including the Internet, computer networks, and wireless communication systems. In other words, cybercrime involves crime committed through use of the computer. This brings us to the issue of defining computer crime. Computer crime is broadly defined by the Department of Justice (DOJ) as “any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution” (1989).

Although there are some overlaps in the classification of computer crime, two different approaches to typology of computer crime are presented. The first involves DOJ typology, which considers the role of a computer in a crime. According to this typology, there are three types of computer-related crimes: a) A computer may be the “object” of a crime. This may involve theft of a computer software or hardware. b) A computer may the “subject” of a crime. The computer in this category may be the subject for an attack. c) A computer may be an “instrument” to commit traditional crime (Jacobson and Green, 2002, p. 276-277). Traditional crimes, including child pornography, identity theft, and copyright infringement, can be committed by using computers.

Another typology of computer crime recognizes four types of computer crimes (Carter, 1995):

- Computers as the target: This type of crime is committed when the action prevents the legitimate user from receiving the service (Taylor and Loper, 2003, p. 586). These types of crimes include theft of marketing information, theft of intellectual property, and they may entail sabotage of personal data, intellectual property, or operating systems (Carter, 1995).

- Computers as the instrumentality of the crime: Similar to the first typology, this category involves the use of computers as a means to commit traditional crimes (Bakewell, Koldaro, and Tjia, 2001). For example, a computer can be used to collect credit card information for fraudulent purchases.

- The computer as incidental to the crime: This category of crime is committed when “a pattern or incident of criminality uses a computer simply for ease in maintaining the efficacy of criminal transactions” (Carter and Bannister, 2000). Crimes, such as money laundering and child pornography are examples of this type of crime.

- Crimes associated with the prevalence of computers: This category of crime involves piracy issues, such as copyright violations of computer software and other misuse of electronic services, including telephone systems.

Cyberterrorism

While the discussion of what constitutes cyberterrorism is presented in the second chapter, the definition of the term is given here to introduce the concept. Cyberterrorism can simply be defined as coercing others for a political cause, by using computing resources in cyberspace. More comprehensively, cyberterrorism refers to

> the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political and social objectives (Denning 2000).

Pollitt (1997) defines cyberterrorism as “the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents.”

To clarify the difference between information warfare and cyberterrorism, it should be understood that cyberterrorism can be a component of information warfare, in other words, information warfare encompasses cyberterrorism (Taylor, Caeti, Loper, Fritch, and Liederbach, 2004, p. 20).

According to Ron Dick, Director of NIIPC in 2002, cyberterrorism means any “criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies.” (as cited in Berinato, 2002).

By combining the above concepts, cyberterrorism may also be defined as the politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies.” (Wilson, 2003, p. 4.)

Typology of Cyberterrorism

There are different approaches in terms of the typology of cyberterrorism. For example, Collin (1999) identifies three types of cyberterrorist acts: Destruction, alteration, and acquisition and retransmission. Grabosky et al. (1998) also identifies three major forms of cyberterrorist acts: destruction of the files, impeding accessibility to data files by encrypting it, and significantly overloading a system, thereby impairing the system's capability.

Another classification of cyberterrorism, "information operations" is presented by Zanini and Edwards (2001, p. 41). The term they used, in fact, has the same meaning as "cyberterrorism." According to Zanini and Edwards (2001, p. 41), there are three types of offensive activities terrorists can use: First, terrorists can use information technologies, such as the Internet for perception management and propaganda. Second, by using the Internet and other computer networks, terrorists can carry out disruptive attacks. Finally, they can use them for destructive purposes (2001).

Perception management and propaganda involve both influencing public opinion and recruitment of new members. The final type of attack is the destructive attack, which is carried out to cause actual destruction of virtual and physical systems, including power, water, or traffic control systems (2001, p. 45). However, some analysts argue since these attacks may not result in loss of human life they may not produce the same emotional reaction as traditional attacks do (Denning, 2001).

On the other hand, Ballard et al. conceptualized a more comprehensive typology of cyberterrorism called "cyber incident typology" (see Table 1) (Ballard, Hornik, and McKenzie, 2002, p. 1009). In the next section, these typologies are analyzed in detail.

Table 1

Cyber Incident Typology

Category	Definition and Explanation
Information attacks	Cyberterrorist attacks focused on altering or destroying the content of electronic files, computer systems, or the various materials therein.
Infrastructure attacks	Cyberterrorist attacks designed to disrupt or destroy the actual hardware, operating platform, or programming in a computerized environment.
Technological facilitation	Use of cyber communications to send plans for terrorist attacks, incite attacks, or otherwise facilitate traditional terrorism or cyberterrorism.
Fund raising and promotion	Use of the Internet to raise funds for a violent political cause to advance an organization supportive of violent political action, or to promote an alternative ideology that is violent in orientation.

Source: Ballard, J. D., Hornik, J. G., & McKenzie, D. (2002). Technological facilitation of terrorism: Definitional, legal and policy issues. *American Behavioral Scientist, 45*, (6), 989-1016.

Information Attacks

Defacing Web sites. Defacing Web sites allows attackers to change the appearance of the Web site and to add whatever the message they want to leave. Even though Web site defacement does not result in any financial losses or information breach regarding the specific governmental or private Web site, it can create a great deal of embarrassment for the Web site owner (Furnell 2002, p. 103).

Several high profile organizations, including the Central Intelligence Agency (CIA), the US Department of Justice, the United Kingdom Labor Party, and the New York Times have suffered from such attacks (Furnell, 2002, p. 104). The hacker group, “Power Through Resistance,” hacked the CIA Web site on September 1996 The group deposited links on the site to various Web sites. To cover embarrassment, the CIA had to announce that “No security breach of private files” occurred (CNN, 1996). Another example involves an Israeli teenager named Ehud Tenebaum, who was arrested by Israeli National Police for "illegally accessing computers belonging to the Israeli and United States governments” (Glave 1998).

Defacing government Web sites, particularly those such as the CIA and Federal Bureau of Investigation (FBI) Web sites could lead people to assume that all of the secret intelligence and other related information have been accessed by attackers, and in the case of cyberterrorism, by terrorists. The impact of such perception could be a very powerful force multiplier especially if it is initiated just before or following a conventional terrorist attack.

Another example involving Web site defacement was between attackers from India and Pakistan. During bloody fighting between Indian and Pakistani soldiers in Kashmir in 1999, both countries’ computer experts also fought in the cyber world. Pakistan’s experts hacked the Indian Army Web site www.atmyinkashmir.org and left anti-Indian statements about the Kashmir issue. The Indian Government, in turn, cut off all network access to the Web site of the prominent Pakistani newspaper, Dawn (Varma, 1999).

Denial of service attacks. Denial of service (DoS) means hindering the user from using the Internet or a related system (Kovacich and Boni, 2000, p. 80). “Multi-user, multi-tasking operating systems are subject to “denial of service” attacks where one user can render the system unusable for legitimate users by “hogging” a resource or damaging or destroying resources so that they cannot be used (Barkley, 1994). DoS attacks do not require any significant skill to execute (Furnell, *2002, p. 109).* These attacks are non-lethal attacks, yet they can cause significant damage in terms of the economy and may demoralize the public about their financial future. According to Barkley, there are three common types of DoS attacks on networks: service overloading, message flooding, and signal grounding (1994).

- Service overloading: The Internet uses Transmission Control Protocol/Internet Protocol (TCP/IP) to communicate. In a network, the client computer sends a message to the server requesting connection to the network. The purpose is to exchange data between two computers. This process is achieved by sending SYN (synchronize) messages. People with malicious purposes can "exploit this process by sending numerous messages to a target server, but then ignore the resulting SYN+ACK (Furnell, 2002, p. 109). Service overloading can be used as a first step for a multi- step attack, such as IP spoofing.

- IP spoofing: After overloading the system, an attacker can pretend to be an authorized system, while blocking the actual system's service. Since the flooded system cannot respond to the inquiries, the unauthorized system will receive all of the legitimate computers' packets (Stephenson, 2000, p. 46).

- Message flooding: Message flood occurs when messages are sent to a target in such a high volume that the target cannot handle it. E-mail flooding and log flooding are the primary types of message flooding (Stephenson, 2000, p. 46). Terrorists can use such techniques for both propaganda and obstructing the service that the target provides for legitimate users. For example, Sri Lankan Liberation Tigers of Tamil Eealam used e-mail attacks to block the e-mail services (Borland, 1998). The messages read, "We are the Internet Black Tigers and we're doing this to disrupt your communications” (Denning, 1999). Similarly during the Kosovo war, Belgrade hackers attacked NATO’s Web site with e-mail bombs such that the Internet service provider cut off the Internet service because of massive e-mail attacks (Denning, 2001).

Signal grounding. Signal grounding requires physical access to the system. It involves interruption of the flow of data in the computer network (Stephenson, 2000, p. 47).

Malicious code attacks: “Malware.” The term malware represents the combination of “malicious” and “software” (Furnell, 2000, p. 143). There are different types of malware attacks. The common forms of malware attacks are viruses, worms, Trojan horses, and software bombs. These are examined in detail in the following section.

- Viruses: Brunnstein, Fischer-Hubner, and Swimmer define a virus as “a non-autonomous set of routines that is capable of modifying programs or systems so that they contain executable copies of itself” (as cited in Furnell, 2000, p. 144). Viruses are malicious software that can replicate themselves. They attach themselves to other software applications and spread as infected files and disks are used. In every new host, the virus inserts itself and executes its payload, which can be a strange warning message or which can wipe all the files from the disk (Taylor et al., 2004). One good example of how a virus can be costly is the I LOVE YOU virus. ICSA, a computer security company estimated the cost of the I LOVE YOU virus to be up to 1$ billion (Miastkowski, 2000).

- Worms: Worms, unlike viruses, do not attach themselves to other programs. They exist as separate programs; in other words, they can spread themselves automatically (Stephenson, 2000, p. 37). They take advantage of automatic file sending features available in computers.

- Trojan horses: Attackers may use Trojan horses to gain access to important information, for example, the target's password, replicate it, and forward it to themselves.

There are differences between viruses and Trojan horses. First of all, Trojan horses do not replicate or infect other files in the disk. Secondly, they can stand alone without any attachment to other programs. Finally, the target may not be aware of the fact that a maliciously intended Trojan horse was sent to him or her. In other words, Trojan horses can be sent with alternative meanings in which the target perceives its intent to be anything but malicious. For example, the attacker may send a message that may be interpreted as friendly information for the receiver, such as a link to a monetary reward.

Software bombs. This software acts like a bomb connected to a detonator, which may contain an execution of a program. The malicious code may be hidden in a program, and once the program is activated, malicious code becomes activated. For example, a disgruntled employee might hide a software bomb in the company's payroll program (Stephenson, 2000, p. 38).

Infrastructure Attacks

Critical infrastructures in a given country provide attractive target for terrorists because of the large-scale economic and operational damage that could occur with a major power failure (Taylor, 2004).

> Several studies have shown that critical infrastructures are potentially vulnerable to a cyberterrorist attack. This is not surprising, because systems are complex, making it effectively impossible to eliminate all weaknesses (Denning, 2001).

While cyber attacks against critical infrastructures in the US are analyzed extensively in the second chapter, this section shows that terrorist groups are considering use of cyber attacks to disseminate propaganda of their ideology.

In the United States, there have been several attacks against critical infrastructures. For example, in March of 1997, a juvenile hacker disabled vital services in the Worcester Airport air traffic control tower for six hours (CCIPS, 1998). The hacking resulted in disabling of telephone services to the tower, airport fire department, security and other departments at the airport (Cilluffo, 2000).

In another act of disruptive attack against a critical infrastructure, an employee fired from Chevron's emergency alert network disabled the firm's alert system by hacking into computers in New York and San Jose, California. He then reconfigured them so they would collapse. The attack was not discovered until an emergency occurred at the Chevron refinery in Richmond, California. The system could not be used to notify the neighboring community of a poisonous gas release; consequently, during the ten-hour period in 1992 when the system was down, thousands of people in twenty-two states and six unspecified areas of Canada were put at risk (Denning, 2000).

Furthermore, according to W. Church, former US Army intelligence officer, the Irish Republican Army had computer-oriented cells, and was very close to engaging in cyberterrorism before they made peace. They were already attacking the London electricity infrastructure by placing real or phony bombs in electricity plants (Borland, 1998). Evidence of dissemination of sensitive details about British Army Intelligence installations, military bases and police stations in Northern Ireland on the Internet by Sinn Fein supporters at University of Texas at Austin supports Church's argument (Devost et al., 1996). Another example is the Italian Red Brigades who characterized the attacks on governmental computer systems as a "strike at the heart of the state" (Devost et al., 1996).

In addition to those, some of the other potential acts of cyberterrorism are (Collin, 1999):

- Remote access to the process control system of a food or a pharmaceutical factory such that the medication or food produced may be contaminated.
- Disrupt the national telecommunication network so that all communications, including financial transactions are disrupted. Such attacks can be so harmful that the citizenry may lose confidence in economic system.
- Attack the air traffic control system remotely and collide two civilian aircraft.

Technological Facilitation

The use of advanced technology in terms of computers and telecommunication devices enables terrorist organizations to operate with greater flexibility, and shapes their organizational structure toward more decentralized structure. The use of technology by terrorists "is not an attack, per se, but rather the use of the Internet to facilitate traditional terrorism and cyberterrorism" (Ballard et al., 2002, p. 1010). It involves the use of the Internet as a communication tool.

According to Monge and Fulk (1999, p. 84), the extended use of new computing technologies and other communication devices led to the establishment of networks in three ways: First, new technologies have enabled terrorist groups to reduce transmission time so that members of the organization can communicate faster. Secondly, new technologies also significantly reduced communication expenses. Not only have new technologies reduced the transmission time and expenses, but also, they have significantly increased the complexity and scope of the information through the combination of computing and communication. In other words, “the rise of networked arrangements in terrorist organizations is part of a wider move away from formally organized, state-sponsored groups to privately financed, loose networks of individuals and subgroups that may have strategic but that, nonetheless, enjoy tactical independence” (Zanini and Edwards, 2001, p. 32).

Zanini and Edwards compare the Palestine Liberation Organization (PLO), which they consider a bureaucratic, hierarchical organization to Hamas and the Palestinian Islamic Jihad and al-Qaeda, all of which they consider to be newer and less hierarchical groups.

Information technologies are very advantageous for dispersed groups and may eliminate the disadvantages created by distance. In particular, using the Internet for communication among the members can not only increase the mobilization but also give more flexibility by allowing more dialogue to make adjustments of the operations. In fact, these technologies may enable terrorists to operate from nearly any country in the world (Zanini and Edwards, 2001, p. 38).

In particular, the Internet provides extremely effective communication between the terrorist organization and its members. Weimann identifies eight different ways that terrorists use the Internet: psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, sharing information, and planning and coordination (2004).

Depending on the ideology of the terrorist organization, Web sites, for example, can serve as a mechanism or communication channel between the members of the organization and the sympathizers to the organization, or the public who may not have direct concern or interest about the organization whatsoever. Through this channel, terrorist organizations can convey their messages to the public and inform them about their recent activities. They may use the Web site as a platform to justify their actions, even though they involve brutal violence. They will attempt to convince at least their followers, if not the general public, that violence is the only option they have to convey their message or to confront government forces (Weimann 2004). By doing so, they seek to legitimize their actions. The audiences of these Web sites involve current or potential supporters, and target population or government entities (Weimann 2004).

In addition to being a communication mechanism between terrorists and the public, technologically advanced tools, such as cryptography and steganography can be used by the terrorists to convey their messages, which may involve attacking targets. The next section briefly explains two types of tools available to terrorists.

Cryptography. Cryptography is defined by Bruce Schneier as “the art and science of securing messages” (as cited in Taylor et al., 2004, p. 29). It involves “extremely strong encryption” of the data transmitted from a source to a target. Although this technology is a powerful tool for the private and public sector, it is also a powerful weapon to hide information from law enforcement (Slambrouck, 1998). Terrorists can send hidden data to members that is intended direct their activities and operations.

Denning summarizes the threat encryption technology poses to law enforcement and the intelligence community. She reveals that there are four ways that the encrypted data presents danger: 1) It may avoid the law enforcement from gathering evidence to convict offenders, 2) The intelligence community will have hard time retrieving vital information about any given investigation, 3) The law enforcement community may be unable to avoid attacks or any harm, and 4) It will hinder the intelligence community from getting foreign intelligence critical to national security (Denning, 1997).

Al-Qaeda members have been using computer technologies to communicate and disseminate information (Kelly, 2000). Thomas states that "… with some certainty, Al-Qaeda loves the Internet" (2003, p. 112). According to Thomas, evidence collected after September 11, 2001 strongly shows that terrorists used the Internet to plan these attacks (2003, p. 112). Further, Thomas claims cyber planning is an important aspect of how terrorists use the Internet, and it may be even more important than cyberterrorism (2003, p. 112).

According to an Al Jazeera TV report, the final message sent to Mohammed Atta by the two senior members of Al- Qaeda three weeks before September 11th, 2001 was a simple code indicating the four targets - the Twin Towers, the Pentagon and Capitol Hill – which were referred to as "faculties" in the message. The communication said, "The semester begins in three more weeks. We've obtained nineteen confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts and the faculty of engineering."

Animal Liberation Front (ALF) cells in Europe and North America use the encryption program Pretty Good Privacy (PGP) to send coded emails to share intelligence (Iuris, 1997, p. 64). These types of encryption programs may make the investigation process extremely difficult.

Steganography. Steganography is the method of hiding data in objects such as pictures, documents, other types of files (Collin, 1997). It is a common technique of hiding information from those who do not have the authority to view it, yet it is a technique terrorists can exploit. This technology relies on “security-by-obscurity,” meaning if the person who receives such a message knows that another message is hidden in, for example, a picture he access the veiled information. (Collin, 1997). From outward appearance, a picture can be perceived as a normal picture, but an embedded message can be extracted from that picture.

Of course, from the point of view of the terrorist, there are some drawbacks to these technological advancements in communication. It is not suggested that face-to-face relations will be replaced with new information technologies. Although, information technologies have provided advantages to these groups, information and communication flow through the Internet and other communication devices can also increase the risk of being traced by law enforcement. The advantages of digital power can turn into a disaster for terrorist organizations. For instance, in Turkey, by the fall of 2000, nearly a thousand alleged members of the radical group, Hizballah, were taken into custody, and about twenty- thousand pages of documents were also recovered from computer archives (Aras & Bacik, 2002). Another example is the encrypted computer records obtained from Aum Shinrikyo, another terrorist organization in Japan (Denning and Baugh, 1997).

Fund Raising and Promotion

Not only can information technologies improve the ability of terrorists to collect and analyze intelligence, but also they can use these technologies for what Zanini and Edwards call “information operations” (2001, p. 41). This term has the same meaning as cyberterrorism. According to Zanini and Edwards (2001, p. 41), there are three types of offensive activities terrorists can use, one of which is the use information technologies, such as the Internet for their perception management and propaganda activities (Thomas, 2003, p. 115). Perception management and propaganda involve both influencing public opinion and recruitment of new members. The Internet, in particular, expands the opportunities to publicize and expose terrorist activities beyond the traditional limits of the media and TV (Thomas, 2003, 115).

Today, almost all of the active terrorist organizations have Web sites and use several languages to reach out to more and more people (Weimann, 2004).

The content of the Web sites typically gives information about the history of the group, their activities, social and political background of the movement or ideology, detailed information about their leaders’ lives, notable personalities or heroes of the organization, current news regarding their activities, as well as information about their targets. For example, just after arresting Kurdish rebel leader Abdullah Ocalan, Kurdish rebels throughout the world were mobilized in less than an hour. They started massive demonstrations in almost every country throughout Europe and enacted an intense propaganda movement on the Internet in an effort to defame the Turkish government (Denning, 1999).

The use of the Internet to raise money by terrorist organizations is a good example as to how information technology can provide new ways to fund their operations. For example, In Pakistan, a group, named Lashkar-e-Taiba (Army of the Pure) has used the Internet to raise money (Stern, 2000). Some even ague having such ability may reduce terrorists' reliance on state support (Soo Hoo, Goodman, and Greenberg, 1997, p. 142).

Cost of cyberterrorism. Between 1993 and 1995, there were forty reported threats made to banks in the US and Britain. For example, in January 1993, a brokerage house paid ten million pounds after receiving a threat and one of their machines crashed. It is estimated that in United Kingdom, during 1993, 1994 and 1995, terrorists gained more than 400 million pounds (Statistics on Cyber-terrorism, 2000).

The 1999 Security Industry Survey indicates that the number of companies penetrated increased from 12 % in 1997 to 23 % in 1998. Another example could be the impact of malicious code attack by hackers. The most costly malicious code attacks were Low Bug in 2000 at $ 8.75 billion and Code Red at $ 2.62 billion (Wiederin, Hoefelmeyer, and Phillips, 2002)

The consequences of cyberterrorist attacks are not as devastating as the physical terrorist attacks, at least until now. For example, cyberspace provides opportunities for e-bombs and cracking down a Web site but the ramifications of these acts seem less significant than the effect of a physical bomb killing hundreds of people in a matter of seconds, such as the bomb attack in Nairobi in 1998 and Oklahoma City in 1995. Regarding the potential attacks outlined by Collin, they would be difficult to execute, because of the human factor in these processes. For example, even if it is possible to hack an air traffic control station, there are pilots who have been trained to double-check unusual commands.

Who are the Cyberterrorists?

A terrorist does not usually spend his or her entire life working at a computer. However, there are crackers and some other people who are in that business. These people are potential candidates for becoming cyberterrorists. This conversion from cracker to terrorist may be motivated by money, prestige, and/or ideology (Collin 1997). However, some analysts suggest that as terrorists are becoming more familiar with technology, a new generation terrorists who are more computer-savvy may be growing, and they may focus on using this technology to carry out cyber attacks (Denning 2000).

The Theoretical Relation of the Study to Information Science

This study has two major components with respect to its relation to information science theory. First of all, this research explores fundamental concepts of a communication model, presented by Shannon and Weaver. The Communication Model consists of an information source, the source's message, a transmitter, a signal, and a receiver: the receiver's message, and a destination (Shannon and Weaver 1949). Cyberterrorism, in fact, involves any attempt to disrupt or destruct the communication between legal users and legal service providers. From cyberterrorism and cybercrime point of view, this research focused on the components of the communication model; however, it examined illegal use of or disruption of communication and tried to come up with solution which involves international cooperation.

While this study deals with three major variables-- vulnerability, comprehensive cooperation, and freedom-- in fact, the underlying concepts of this study are related purely to communication and information use. In other words, part of the study attempted to identify the factors motivating cyber criminals and cyberterrorists to unlawfully use information technologies to intervene in communication between the service providers and legitimate users. Specifically, this research deals with the criminal aspect of information consumption, which involves unlawful acts on the side of the criminals and members of a terrorist organization. The concepts, cyberterrorism and cybercrime address the unlawful activities, which hinder the communication process. In particular, information attacks, including disruptive and destructive information attacks obstruct legitimate users from accessing their information. Also, activities, including communication and propaganda in favor of an organized crime group or terrorist organization represent the criminal aspect of information consumption.

The second major component deals with the policy aspect of information science. As a field, information science also deals with the policy, programs, and strategies that are carried out by public and private sector entities. In that sense, this research deals with one of the most critical aspects of policy: dealing with responding to threats coming from cyber criminals and cyberterrorists. In particular, this research focuses on how we can respond to these threats in terms of deterring the perpetrators and avoiding such attacks before they are carried out.

Summary

“Terrorism is a rapidly evolving and responsive phenomenon” (Devost et al., 998). If we consider terrorists as rational people who calculate the necessary preparation and consequences of their actions, cyberterrorism provides ample opportunity for terrorists because the attacks are cost-effective and may potentially disrupt and destroy enough lives to serve their political agenda. As Robert Kupperman, the former Chief Scientist of the US Arms Control and Disarmament Agency states “increasing societal reliance upon technology changes the nature of the threat posed by terrorists” (as cited in Devost et al., 1998).

The vulnerabilities of the information infrastructure can be exploited by terrorists. Although the issue of vulnerability will be analyzed in detail in Chapter II, it is necessary to state that vulnerability does not emerge only from increased reliance on technology. Lack of legal measures, lack of cooperation at the national and international level, and cultural boundaries may keep individuals, public and private, from taking necessary steps to ensure that the critical infrastructure is protected from attacks coming from cyberspace.

Of course, while taking necessary measures; governments should also be aware that the fundamental rights of individuals are also protected from intrusive acts. There is always tension between protecting the rights of a person and enforcing laws. The numerous benefits that technology has brought to us also have created new risks. These risks range from national security and national infrastructure vulnerabilities to personal security, privacy, and integrity of personal information (Cilluffo, 2000).

In addition to technical difficulties in terms of investigating such crimes, transnational characteristics of such attacks create other problems. For example, legal issues represent another set of problems faced by law enforcement and other criminal justice entities. Since prosecution of such crimes may involve multi-jurisdictions, legal issues surrounding cyberterrorism investigation in terms of pursuing and prosecuting criminals will exacerbate the problem (CERT, 2002).

How, then, should governments, especially, security agencies and law enforcement community respond to such complex criminal activity?

The purpose of this study was to identify major factors affecting or constructing the major variables: vulnerability, comprehensive cooperation, and freedom. The study also aimed at identifying the relationship between major variables of the research. Furthermore, the research attempted to develop a scale which involves vulnerability, freedom of society, and comprehensive cooperation. Finally, it came up with a typology of cyberterrorism based on expert opinions. The following chapter revealed the in-depth literature review for this study.

CHAPTER 2

ANALYSIS OF CONCEPTS RELATED TO CYBERTERRORISM AND EXPLORATION OF NATIONAL AND GLOBAL EFFORTS TOWARD COUNTERING CYBERTERRORISM

Introduction

Responding to terrorism, especially, cyberterrorism, requires special treatment in terms of developing overreaching strategies and policies that need to be as inclusive as possible. In other words, responding to terrorism does not only include law enforcement efforts, which may even require conventional military options; it also includes bringing about efforts from all parties, including governments, private sector, and multinational agencies-- all of which have vested interest in answering this call. These efforts may range from developing new tactics and strategies for effective terrorism response, to creating legislation and establishing bilateral and multilateral cooperation which aim at creating a "global consensus" [1] as to what needs to be done within the universally accepted principles of law and justice.

As the world has become more and more reliant on technology and networked systems, not only have legitimate entities benefited from this trend, but also illegal groups, such as terrorists, organized crime groups, and other criminal entities have been using cyberspace for their own benefits.

The objective of this chapter has several components. First, it examined the conceptual definition of cyberterrorism by reviewing the literature and attempted to

[1] According to Putnam and Elliott, consensus "as it is used in this discussion is defined broadly as a state of 'general agreement.' To find consensus on an issue, therefore, does not demand an identity of opinion on every aspect of the question; rather, it merely suggests that there is enough agreement among enough states to permit consideration of a multilateral effort" (2001, p. 5).

come up with an acceptable definition for the sake of this research. Also, it defined the concept of vulnerability, and explored the concept under four major subtitles: a) technical vulnerability, b) legal vulnerability, c) Political vulnerability- Special circumstances of the target state, and d) Cultural vulnerability. Third, this chapter explored overall efforts to counter criminal activities in cyberspace, including cybercrime and cyberterrorism. Due to the broad nature of this topic, this research focused on three major areas: a) Individual Governments: This section will focus on the efforts by the US and United Kingdom, b) Multilateral cooperation: This section revealed some of the activities engaged in by the multilateral agencies, including the United Nations (UN), the Group 8 (G-8), the Council of Europe (CoE), European Union (EU), Interpol, and c) Government- Private cooperation. Fourth, some of the models, presented in the area of responding to cyberterrorism will also be revealed in this chapter. Finally, the issue of privacy was analyzed in detail with respect to countering cyberterrorism and possible consequences of these efforts.

Analysis of the Definition of Cyberterrorism

The concept of cyberterrorism is complex. There are implications regarding the definition of cyberterrorism. Ballard et al. discuss some of the issues related to the definition of cyberterrorism. They present three points that may explain the difficulty in defining cyberterrorism. First, because the technology develops so rapidly the operational definition of cyberterrorism may change (Ballard et al., 2002, p. 993). Second, the definition of cyberterrorism may be biased because of researchers' personal perspectives as to what cyberterrorism is. They may define cyberterrorism based solely on their specialized areas of expertise (Ballard et al., 2002, p. 993). Finally, there might be legitimate concerns regarding the validity, reliability, and accuracy of the research (Ballard et al., 2002, p. 993).

By stating, “no single or globally accepted definition of terrorism exists”, indeed Ballard et al. (2002, p. 990) indicate the difficulty of defining cyberterrorism in the first place. Nevertheless, they identified three different methods used by researchers to define cyberterrorism: 1) adapting the existing definition of terrorism to define cyberterrorism, 2) using the existing laws and authorities to define what actions represent cyberterrorism, and 3) defining cyberterrorism by using specific actions (Ballard et al., 2002, p. 992-993).

As a reflection of these methods, there are different types of definitions of cyberterrorism, some of which were revealed in the first chapter. This section focuses on different approaches other than just revealing the definitions, which has been already done.

In her article, “What Is Cyberterrorism?” Conway defines the cyberterrorism as “premeditated, politically motivated attacks by sub-national groups or clandestine agents against information, computer systems, computer programs, and data that result in violence against noncombatant and targets” (2002, p. 436). By this definition, Conway excludes cybercrime activities, including stealing credit card information, sending emails having pornographic content, or hacking a Web site. Some researchers in this area characterize an act as cyberterrorism only if the act results in destruction, death, and/or injury, and creates fear among the public (Denning 2000, Convay, 2002). Furthermore, some also claim that we have not witnessed the destructive aspect of cyberterrorism yet, and therefore, they suggest that cyberterrorism does not exist at all (Denning 1999).

In terms of witnessing cyberterrorism, the claim might be considered to be an accurate one; however, there is also evidence indicating that terrorist organizations have been considering attacking information infrastructures and other communication networks by engaging in cyberterrorism (Devost 1995). In their article, “In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks,” Brenner and Goodman attempt to answer the question “why has cyberterrorism not yet manifested itself?” As an answer to that question, they review the literature. The concluded that for some people, the reason why international terrorists have not mounted cyber attacks yet is that they do not have the capability in terms of the technical background. That explanation is called the “there are not enough good terrorist hackers theory,” which claims that the terrorists do not have the computer expertise to launch such attacks, and this perspective gives the target countries, in particular, Western countries, comfort to think that they are safe (Brenner and Goodman, 2002, p. 46). Brenner and Goodman consider two problems with respect to that theory: First, this theory ignores the fact that the countries where the terrorists are active have the sophistication that is necessary to launch cyber attacks against the information infrastructure of the countries. For example, the Pakistani hacker groups, G-Force Pakistan and The Pakistani Hackers Club and the Sri Lankan Internet Black tigers, a special unit of Sri Lankan Tamil Tigers of Tamil Eelam, are credited with executing attacks what seem to be a cyberterrorism campaign (Brenner and Goodman, 2002, p. 47). The second problem with the theory is that the imminent possibility that terrorists can recruit “hacker mercenaries,” who have the expertise and motivation to launch cyber attacks if they are paid, is underestimated (Brenner and Goodman, 2002, p. 48). Another explanation of why we have not seen cyberterrorism is that the leaders of the terrorist organizations came from an older generation; therefore, they may not see that type of attack as an alternative (Brenner and Goodman, 2002, p. 48).

Brenner and Goodman strongly assert "the fact that cyberterrorism is a real possibility, if not an imminent probability…and … it is necessary to consider both the threat level of the target and the sophistication of the perpetrator" (Brenner and Goodman, 2002, p. 52).

Another perspective of defining cyberterrorism is presented by Devost, Houghton, and Pollard. They define information terrorism as the "intentional use of a digital information system, network or component toward an end that supports or facilitates a terrorist campaign or action" (1997). The importance of such a definition is reflected in their statement that cyberterrorism is the "nexus between criminal information system fraud or abuse, and the physical violence of terrorism" (1997). They are fully aware of the fact that one of the most important aspects of defining terrorism is to include politically motivated violence instead of defining the term with actions which may have nothing to do with violence. However, with this definition, they want to "allow for the inclusion of pure information-system abuse" as a new face of terrorism (as cited in Conway, 2002, p. 437). Of course that kind of approach results in including cybercrime activities within the context of cyberterrorism only if they are politically motivated.

In addition to these perspectives, a guide, prepared by the Federal Emergency Management Agency (FEMA) discusses the concept of cyberterrorism and presents its own perspective as to what cyberterrorism is. According to the FEMA, in order for an attack to be qualified as cyberterrorism, an attack should cause violence against property or person, or “at least cause enough harm to generate fear” (FEMA 2002).

Also, FEMA reveals the distinction between cybercrime and cyberterrorism (2002).

> Cyberterrorism is distinct from computer crime, economic espionage, and "hactivism," although terrorists may employ any of these forms of computer abuse to further their agendas. The weapons of cyberterrorism computers differ from weapons of mass destruction such as biological agents, chemical agents, and radiological agents in that they don't directly cause death and injury. However, acting indirectly, they can cause serious consequences to individuals, businesses, industry, government, and the public at large. Depending on how they are used, they can lead to injury and death.

The definition, revealed by the FEMA has an important component which underlies the definition of terrorism and cyberterrorism. An action that generates fear in the public may become a means for terrorists; in other words, a politically motivated attack which results in a tremendous amount of fear and panic in the public may well be characterized as cyberterrorism even though it does not lead to physical injury or death.

The final discussion on defining cyberterrorism is presented by Whiteman. With respect to the probability of cyber attack by terrorists, Whiteman claims that such a threat is possible, but with many qualifications (2001). Whiteman’s approach to a definition of cyberterrorism is fundamentally different than most of the experts and academia in the field. He appreciates the importance of defining traditional terrorism within a realm which involves politically motivated violence. Yet he also realizes the thin line between traditional terrorism and cyberterrorism. Therefore, he asserts that

> if we limit ourselves to the realm of what I shall refer to as traditional terrorism, we risk focusing on highly unlikely occurrences that constitute the worst-case scenarios. Such focus adds little value in developing a risk-management approach to dealing with the problem. Cyberterrorism must be considered to include the full range of threats, vulnerabilities, risks, and technological matters that anyone employing IT systems at the core and even on the periphery of their business must contend with today (Whiteman, 2001, p. 75).

The fact is “Anyone who could learn to fly a commercial airliner could probably acquire the expertise to penetrate one of our critical information systems” (as cited in Brenner and Goodman, 2002, p. 45). It is not a reasonable assumption that today’s terrorists do not have the capability of carrying out cyber attacks. Cyber attacks by individuals, such as hackers and other criminal entities provide strong evidence that the Internet can be a tool for terrorists who attempt to exploit every possible means available to them for their cause.

Cyberterrorism as a Force Multiplier

Conventional terrorist tactics, such as car bombings, assassinations, suicide bombings, kidnapping, and hijacking may never be replaced by cyber attacks. However, as a force multiplier, cyberterrorism can create more effect if it is executed in concert with other traditional terrorist actions. A good example can be the scenario created by CSIS involving detonation of a bomb as a conventional terrorist act and a denial of service attack as a force multiplier (Cilluffo, 2000).

Brenner and Goodman analyze the characteristics of cyberspace and the advantages that it provides for terrorists and other criminal entities. The first characteristic of cyberspace is that “cyberspace is borderless” (Brenner and Goodman, 2002, p. 12). As the CIA Director George Tenet affirms, cyberspace gives terrorists the operational flexibility and greater security which could be capitalized by them in many ways, including establishing networks with other terrorist organizations and members, communicating between members, and facilitating use of the Internet as a propaganda mechanism (as cited in Brenner and Goodman, 2002, pp. 13-14). Also, cyberspace enables terrorists to attack multiple targets at the same time, which can increase the significance of the attack. An interesting perspective by two authors, Brenner and Goodman, is that cyber attacks can act as “terror multipliers,” which is a term for force multiplier (2002, p. 26). Terror multiplier can be explained as an effect of cyber attack which is created by the anonymous nature of the attack source and the consequences of the attack.

Terrorists will attack vulnerable targets, as opposed to the well- protected ones, in order to be successful in their actions and create appropriate conditions which will serve their cause. Vulnerability represents one of the most important concepts of this research. Therefore, the next section focuses on the definition and detailed explanation of vulnerability.

Vulnerability

Definition of Vulnerability

Vulnerability has been defined in several ways. In a general sense, vulnerability can be defined as “a point where a system is susceptible to attack” (Icove and Seger, 1995, p. 89). Vulnerability in military terminology, on the other hand, can be defined as the possibility of being “liable or exposed to attack (WordReference.com Dictionary, 2000). Two different versions of vulnerability definitions by the US Military are thus:

- The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished.
- In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system (as cited in Ford, 2002).

In terms of computer systems and networks, on the other hand, vulnerability is defined as “a weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate the system’s security policy” (Glossary of Vulnerability, 2004).

Another important concept is vulnerability assessment, which is defined as “a measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack” (Glossary of Vulnerability, 2004).

In addition to vulnerability assessment, threat is another important term, defined as “a possible danger to your system; the danger might be a person (a spy, a professional criminal, or a cracker), a thing (faulty hardware or software), or an event (a fire, a lightening strike, or an earthquake) that might attack the system (Icove and Seger, 1995, p. 89).

In order to assess the potential threat of cyberterrorism, Denning identifies two factors: “first, whether there are targets that are vulnerable to attacks that could lead to severe harm, and second, whether there are actors with capability and motivation to carry them out” (2001). The second factor, whether there are individuals who have the technical ability and motivation to execute such an attack, needs to be explained. According to Denning, although hackers may have the ability to execute such action, they may not have a motivation to carry out these attacks. Whereas a terrorist has the motivation, but may not necessarily have the ability to use cyberterrorism. She, on the other hand, claims that the next generation of terrorists “will grow up in a digital world, and they will have more powerful and easy-to-use hacking tools available to them” (Denning, 2001).

Vulnerability may exist for several reasons. Vulnerability emerges not only from increased reliance on technology, but also lack of consensus as to which act will be criminalized, lack of bilateral and multilateral cooperation among nations, and cultural differences in terms of attitudes about the risk of cybercrime and cyberterrorism.

The next section summarizes the literature about different types of vulnerabilities and some of the strategies and policies implemented to overcome these vulnerabilities.

Sources of Vulnerabilities to Cyber Attacks

According to Sofaer and Goodman, there are two major weaknesses that the transnational nature of information infrastructures generate: 1) a worldwide target of computer networks, the users to attack and victimize, and attackers’ ability to create damage worldwide with no more effort than could be necessary in attacking users or computers in a single state, 2) the widespread lack of agreement among states, in the regulatory, legal, or policy arenas regarding cybercrime and the lack of a satisfactorily high degree of international cooperation in deterring and prosecuting such crime (Sofaer and Goodman, 2001, pp. 6-7).

The next section discusses four general sources of vulnerability: a) technical aspects of vulnerability, b) legal aspects of vulnerability, c) cultural aspects of vulnerability, and d) political aspects of vulnerability.

Technical Aspects of Vulnerability

“The global dependence on interconnected computers and the vulnerabilities thereof fostered the emergence of cyberterrorism” (National Communication System 2000).

According to Lewis, “the premise of cyberterrorism is that as nations and critical structures became more dependent on computer networks for their operation, new vulnerabilities were created” (2002). In other words, Lewis claims that as the world has become more dependent upon technology through facilitation of computer networks and other communication infrastructure, it is more likely that the terrorists will use cyberterrorism as a tactic to accomplish their political objectives.

Similar to that position, in his analysis of vulnerability, Vatis points out three factors that exacerbate the problem. First, Vatis reveals the fact that most of the infrastructures rely on “commercially available, off-the-shelf-technology,” meaning vulnerability stemming from the use of hardware and software that are not limited to one company, government entity, or individual; rather, everybody using these technologies become equally vulnerable (Vatis 1998). Secondly, the infrastructures of countries, the developed countries, such as the US, Britain, or Japan, in particular, are increasingly interconnected and interdependent which makes it difficult to gauge the consequences of an attack against one infrastructure (Vatis 1998). Finally, telecommunication infrastructure is “now truly global,” which almost “undermines the notion of a “National” information infrastructure” (Vatis 1998).

In his article, “Under Siege: The Jurisdictional and Interagency problems of Protecting the National Information Infrastructure,” Persico points out the rising threat emerging from the growing computer and other communication networks. He asserts that while traditional threats have been emerging from possible attacks against physical targets of the government infrastructures, today a new type of threats has emerged in conjunction with the increased reliance on the national information infrastructures (Persico, 1999, p. 157).

In 1998, the Director of the CIA George Tenet, in his testimony, conceded that

> We rely more and more on computer networks for the flow of essential information. Like electricity, we now take information infrastructures for granted. Reliability breeds dependence - and dependence produces vulnerabilities. Today, as a result of the dramatic growth of and dependency on new information technologies, our infrastructures have become increasingly automated and inter-linked.

He further explained that the US is at risk of being attacked because of:

- trillions of dollars in financial transactions and commerce moving over a medium with minimal protection and sporadic law enforcement
- increasing quantities of intellectual property residing on networked systems
- the opportunity to disrupt military effectiveness and public safety, with the elements of surprise and anonymity (1998).

Vulnerability may exist not only from existing software programs. Vulnerabilities within the current programs and software can be exploited by the hackers, other cyber criminals, and even by the cyberterrorists.

Goodman examines the transportation system and its vulnerability to attacks. According to Goodman, transportation systems are attractive targets for malicious attacks since they are critically important national and international infrastructures which are also increasingly dependent upon technologies (Goodman, 2001, p. 70). Higher dependency creates more vulnerability for hostile information operations (Goodman, 2001, p. 70).

Goodman summarizes four major reasons why civil air transportation might receive significant attention with respect to international cooperation to respond to cybercrime and cyberterrorism: 1) Civil aviation is one of the most widespread and extensively interconnected international infrastructures, 2) The civil aviation infrastructure is extraordinarily reliant upon computer-telecommunications information systems, 3) Civil aviation has a long history of being attacked by terrorists, and 4) There is a well-known cooperation in air transportation already in existence (Goodman, 2001, p. 71).

To reduce technical vulnerabilities there are a variety of techniques and great deal of literature is also available. For the sake of this research, these techniques are revealed briefly. There are three broad approaches all of which can be used to reduce the vulnerability to cyberterrorism: isolation, encryption, and security (FEMA 2002). Isolation involves separation of the network system from an outside connection so that the vulnerability of the system can be ensured. Isolation also prevents individuals who do not have the authority to access the system from reaching the data base. Encryption technology is critical in order to have a secure and trusted global information infrastructure for electronic commerce and communication (Denning and Baugh, 2000, p. 105). Furthermore, to lessen the vulnerabilities of computer systems, individual computers, and the Internet, public and private organizations, including individuals, need to adopt protective measures, such as encryption, proxy servers, and other technologies (Lukasik, 2001).Security involves the protection of the system from disasters, mistakes, and the like by building the system in a secure area, or taking necessary steps to ensure that the facility is protected against illegal access and natural disasters as much as it can possibly be done (Denning and Baugh, 2000, p. 105). In addition to more secure network protocols, firewalls, and challenge response systems, security management applications should be used to enhance security (Drozdova, 2001, p. 200).

Legal Aspects of Vulnerability

The legal aspects of vulnerability pertain to sources of vulnerabilities in the area of law and practice of these laws. According to Vatis, international cooperation is crucial to investigate criminal activities in cyberspace; however, there are some obstacles: First of all, many countries may not have substantive laws criminalizing computer crimes (2002). Secondly, lack of authority limits the power of the target state's ability to investigate criminal activity in cyberspace due to lack of jurisdictional authority. Finally, he claims that even though the former two things are present, unlike traditional criminal investigation procedures, cyberterrorism and cybercrime investigation requires swifter action, which could be very difficult at the international level (Vatis 2000).

Sofaer and Goodman also consider similar factors as obstacles confronting an effective response to cyberterrorism. They state that the disparity among the states in the laws and practices essential to authorize them to investigate and prosecute cybercrime is a significant weakness of the current system (Sofaer and Goodman, 2001, p. 15). They assert that even though individual states have agreements or treaties, no international agreement as yet exists on cooperation for criminals who attack computer systems or other information infrastructures for either political or apolitical agendas (Sofaer and Goodman, 2001, p. 16).

In the legal front, there are important steps toward creation of an effective legal framework that address cybercrime and cyberterrorism. Two researchers, Putnam and Elliott, analyze a survey, done by Ekaterina Drozdova. In his research, Drozdova identifies 7 types of computer related crimes which are taken into consideration by the countries surveyed (1999). Putnam and Elliott refer them as "consensus crimes" listed them as:

1. Unauthorized access;
2. Illicit tampering with files or data (e.g., unauthorized copying, modification, or destruction);
3. Computer or network sabotage (e.g., viruses, worms, Trojan horses, denial of-service attacks);
4. Use of information systems to commit or advance "traditional" crimes (e.g., fraud, forgery, money laundering, acts of terrorism);
5. Computer-mediated espionage;
6. Violations against privacy in the acquisition or use of personal data;
7. Theft or damage of computer hardware or software. (2001, p. 38)

The survey examines the legal codes of fifty countries. The study revealed that 70% of the countries for which data were found have enacted or were planning to enact laws which prohibit computer-related crimes, and 30 % of the countries in the survey had few or no laws concerning computer-related crimes (as cited in (Putnam and Elliott, 2001, p. 37).

This survey is important for several reasons. First of all, it shows that in the world, awareness against cybercrime is significant, and more and more countries are addressing that issue in their legal system. Secondly, it also shows variations among the countries in terms of their definition of computer-related crime. That kind of variation may result in complications in terms of responding to cybercrime and terrorism (Putnam and Elliott, 2001, p. 38). Putnam and Elliott discuss the importance of having a consensus concerning an international response to cybercrime and cyberterrorism. To an extent, this variation in states' reactions in terms of enacting procedural and regulative laws concerning the growing potential for cybercrime and cyberterrorism can be explicated with reference to two dimensions: a) Countries differ extensively in their vulnerability to illegal activity carried out against or by means of computers and network systems, b) They also differ extensively according to the degree of threat they face from terrorists, criminal groups, or individuals (Putnam and Elliott, 2001, p. 50).

Putnam and Elliott assert that the countries that have laws directed explicitly against cybercrime are also "the most highly industrialized countries, which, as a rule, are also the most dependent upon computers and computer networks" (2001, p. 51).

Cultural Aspects of Vulnerability

The vulnerability of a system, whether it is owned by the government or the private sector, can also exist from different perceptions about the necessity of taking steps to respond to vulnerabilities. In this respect, Sofaer and Goodman propose a different source of vulnerability, which they call "cultural vulnerability", and define as the perceptional differences between the government and the private in terms of handling the issue of cybercrime and cyberterrorism. According to them, the vulnerability of information infrastructure also stems from the insufficiency of systems' security measures (2001, p. 20). Since the goal of business is significantly different than that of the government, the issue of security for business is also fundamentally different than that for the government (as cited in Sofaer and Goodman, 2001, p. 21). In his comparison between the perception of the government and business about cyber security, Parker claims (1999, pp. 2-4).

> Business survives and grows by managing risks, including security risks, to achieve profit and productivity and views security as a necessary enabler to achieve its goals…
>
> Governments, and especially military and law enforcement departments, in contrast to business, have security as their goal, and it in contrast to business, have security as their goal, and it is enforced by law and motivated by significant rewards and penalties.

This clearly indicates that even though the government, law enforcement entities in particular, perform their duties and try to respond to cyber threats and try to minimize vulnerabilities of the information infrastructures, they may not necessarily receive equal attention from their private counterparts due to differences in their reasons of existence. This issue may become more evident, especially when it comes to cyberterrorism. Due to fact that we have not seen a destructive cyberterrorism yet, it will be more difficult to convince the private sector to consider the possibility of cyberterrorist attacks and the consideration of appropriate security measures. Therefore, it is imperative to understand the cultural differences between business and government to achieve information sharing and cooperation among them (Parker, 1999).

An attitude of “It will never happen to us” and lack of awareness for ownership and responsibility are other critical sources of cultural vulnerabilities (Nosworthy 2000, p. 338). Cilluffo and Pattak present an interesting perspective with respect to the reality of cyber attacks. Interestingly, they claim that “It is a tenet of human nature to sometimes believe that what has not happened cannot happen” As a result, individuals, the private sector, and the government continue happily along and avoid the expense and time of taking the essential prudent steps to diminish and manage the risk for themselves and their vulnerable sources from cyber or physical attack (2000, p. 136-137).

Cilluffo and Pattak also reveal some the issues that make systems, and consequently governments, and the private sector vulnerable:

1. A widespread, though not total, lack of awareness and action on the part of managers to protect critical systems
2. The ever-decreasing cost of the hardware, software, and access to knowledge on how to attack or disrupt systems
3. The sheer volume of information concerning targets available on the Internet, and the ability of powerful search engines to go through and compile this information (2000, p. 143)

Political Aspects of Vulnerability

The political aspect of vulnerability has several components. First of all, vulnerability, in terms of cyberterrorism, constitutes a similar complexity in responding to terrorism. "Terrorism, in the most widely accepted contemporary usage of the term, is fundamentally and inherently political" (Hoffman, 2004, p. 4). In other words, responding to phenomena that is inherently political will ultimately involve political issues. This reminds us of the so-called `One's terrorist is another's freedom fighter` concept, which is also the most critical obstacle in front of counterterrorism efforts. In other words, individual countries may not be willing to help another country if they do not consider a specific group as a terrorist organization. Secondly, political vulnerability involves different levels of potentiality of being the target of a cyber attack by terrorists. Finally, political vulnerability is related to cooperation between governments, as well as inter-agency cooperation within a single country.

In terms of the potentiality of being a target of a cyber attack, there is variation between countries. Terrorist organizations may not be equally motivated, or they may not have the capability, even though they are motivated. To have a more comprehensive perspective on this issue, it is necessary to define two concepts--motivation and capability.

Motivation can be defined as “the extent to which the threatening actor wants to take an action (Communication System 2000, p. 20). Capability is defined as “the extent to which the threatening actor has the knowledge, skills, tools, and other resources required to take the action” (Communication System, 2000, p. 20). At first glance, not all countries around the globe are targeted by the terrorists. Moreover, not every terrorist organization has interest in using cyberspace as a tool to carry out attacks.

Finally, while one country can be vulnerable to cyber attacks, one may not be a target of such attack at all. For example, “the United States is at a particular risk for cyber attack, whether related to information warfare or cyberterrorism” (Taylor et al., 2004, pp. 23-24). One significant source of risk is that several radical terrorist groups, in particular, terrorist organizations of Middle Eastern origin, perceive the US evil, and thus, the main target for their attacks. The second fundamental reason for risk is the unique reliance of the US upon information infrastructure (Taylor et al., 2004). On the other hand, Switzerland, for example, may not be a target.

Cooperation Issues and Vulnerability

Cooperation with other countries must be a central part of building cyber security (Lewis, 2003, xii). However, “The Internet does not yet have the Web of cooperation that has been built up elsewhere" (Lewis, 2003, p. xii). There are reasons behind this lack of cooperation. First of all, it is new to some states, secondly some states may not know what is needed, and finally, it touches on many sensitive issues ranging from economic competition, privacy, access, and national security (Lewis, 2003). In particular, the difficulty with respect to national security and cyber security is that it is always a question as to what extent free states are willing to cooperate with other nations in national security issues while they may be required to advertise their vulnerabilities (Lewis, 2003, p. xix). With advances in technology, financial and banking systems, telecommunication networks, aviation systems, and air traffic control become more reliant on computer and telecommunication networks, which serve many countries but are not controlled by a single country. Therefore, it may be reasonable to claim that it may be easier to facilitate international cooperation in critical infrastructure protection by starting with areas where the transnational connections are very large, such as financial services (Lewis, 2003, p. xix).

Analysis of Cyberterrorism Response Models

There are various approaches to the problem of responding to cyberterrorism. In this section some of them will be presented briefly.

Devost's Realistic Approach vs. Liberal Approach

Devost (1995) argues that cyberterrorism fits into traditional national security debates. Several correlations can be drawn between cyberterrorism and the technologies influencing national security. There are basically two approaches: realist and liberal (Devost 1995).

Realist approach. Realists consider security a relative concept. The realist perspective focuses on ways to increase the nation's relative security. Under this perspective, the international political system is anarchic and it is based upon distrust to other nations; therefore, international cooperation is not an effective way of deterrence in terms of international and transnational terrorism. The realist approach pursues the following objectives:

1. Increase security of information systems at home through training, developing security procedures, and greater vendor accountability
2. Constant evaluation of information systems and comparison of information systems with the systems of other countries, in terms of level of security
3. Formation of possible responses. This objective creates a deterrence effect
4. Develop methods for measuring offensive and defensive capabilities
5. Decrease the level of interdependence
6. Create more autonomous networks to minimize the domino effect of damages (Devost, 1995)

The realist approach has serious difficulties because it contradicts the global and convergent nature of technologies. It promotes isolation by pursuing the decrease in interdependency. Decrease in interdependence is not acceptable in today's global economy because interdependence produces great economic benefits.

Liberal approach. Under a liberal approach, the international political system is not as anarchic as it is for the realists, and counter-cyberterrorist efforts should be based more on cooperative efforts than offensive and defensive efforts. The liberal approach pursues the objectives of increasing the level of interdependency and promoting international cooperation. International cooperation creates a relatively more stable environment that generates more opportunities for terrorists than an unstable environment (Devost,1995).

The liberal approach promotes interdependency, and disregards offensive intentions of other countries. On the other hand, an increase in inter-governmental dependence decreases the threat from other countries, and it has little effect on counter cyberterrorism. In fact, it can produce a deterrent effect for state- sponsored terrorism. As a result, promoting interdependency is criticized as an ineffective way of countering cyberterrorism.

Another objective of liberal approach is promoting international cooperation. According to Devost (1995), this is an incredibly difficult objective to achieve. He argues that the possible damage to countries is significantly different in the first place. For example, an unauthorized intrusion into the American stock exchange systems generates greater impact than the intrusion into the Hungarian stock exchange system.

The major conflict between realist and liberal approaches is on the issue of international cooperation. The global nature of the Internet makes the international cooperative agreements essential in fighting cybercrime. Both decreases and increases in interdependence have their own advantages. Decreasing it reduces the vulnerabilities, however it causes economic disadvantages. Both realist and liberal approaches have their own pros and cons.

In another perspective on responding cyberterrorism, Drozdova proposes a similar approach: Protective approach vs. reactive approach.

Drozdova' s Protective Approach vs. Reactive Approach

According to Drozdova, there are two basic approaches to the issue of cyber security: protective and reactive approaches. The protective approach seeks to deter attacks through measures which deny access by the criminals, and/or it aims to lessen the vulnerability of the targets so that criminals cannot successfully carry out their attacks. The reactive approach, on the other hand, aims to deter any attack through effective investigation, prosecution, and sentencing (Drozdova, 2001, p. 186). They both are similar in monitoring, and identifying abnormal or criminal activity. Yet, they have fundamental differences in the outcome. While the protective approach depends heavily on automation and decision making of the computer security experts, the reactive approach depends on law enforcement involvement which could be "more intrusive and more threatening to civil liberties" (Drozdova, 2001, 187). The reactive approach could be more effective in cases where users are unable to defend themselves, or do not have sufficient protective measures (Drozdova, 2001, p. 187).

Cooperative Response to Cyberterrorism

The lack of a legal framework creates more vulnerability for individuals, companies, and states (Lewis, 2003). "… while national efforts can improve cyber security, they must be complemented by bilateral or multilateral efforts" (Lewis, 2003, p. xiv).

Cyberterrorism and cybercrime could also overlap in damaging ways; groups can steal credit card numbers or important data in order to damage economies and for their own gain" (Lewis, 2003, p. xv). Localized law enforcement efforts toward cyber criminal activities are at a disadvantage in an interconnected world due to limited jurisdiction that every law enforcement agency has.

Cooperation may involve several categories, three of which are national level, international level, and public-private cooperation. The next section will analyze these categories.

International Cooperation

According to Miyawaki (1999), “The ease with which the origins of cyber attacks can be hidden, and the fact that cyber attacks on one nation can come from anywhere on the globe, mean that cybercrime and cyberterrorism are truly international threats.” Ever since terrorism and other types of transnational criminal activities have become the main topics in the international arena, the term `cooperation` has become a focal point for every government. In particular, bilateral and multilateral cooperation have been shown as the most effective method to respond to transnational cybercrime and cyberterrorism. The next section will reveal strategies, attempts, and efforts with respect to countering cyberterrorism and cybercrime.

Lukasik presents a detailed analysis of responding transnational cybercrime and cyberterrorism. Lukasik asserts that in order to have a successful global response, the following elements should be in place:

- A common terminology between parties involved in the incident to include identification of the intruder’s modus operandi, the technical attack details, and the identification of the targets
- Knowledge of the technical skills of all parties involved in resolving the incident
- Existing agreements on how incidents of a variety of types will be handled

- An understanding of the common and conflicting societal issues surrounding the incidents (2001, pp. 152-153).

Later he lists the critical elements that have to be in place in order to have what he calls a "framework for international cooperation"

- Broad membership, consisting of both the world's most technologically advanced nations as well as developing nations, all of whom share the benefits and the risks of global information architectures
- A voluntary and non-coercive environment based on concepts of consensus and practical experience
- Open technical standards that prevent the manipulation of information technology for unilateral gain
- An open organizational structure that provides opportunities for all constituencies to express their concerns
- A mechanism for providing continuous monitoring of actions that can adversely impact privacy
- Mechanisms for reviewing the state of information technology and its practical implementations to enable the international framework to remain relevant in the light of changing capabilities and requirements
- Mechanisms that can assist in building trust relationships globally
- Funding arrangements that can assist less developed nations in meeting their responsibilities to protect the information commons (2001, pp. 176-177).

In terms of international cooperation, there are different forms of relationships among governments and their related law enforcement agencies. These cooperative efforts are:

- Formal bilateral cooperation: Mutual legal assistance treaties (MLATs)
- Informal bilateral cooperation: Individual police contacts (inter agency cooperation), CERTs, etc.
- Formal multilateral cooperation: Council of Europe
- Informal multilateral cooperation: G-8 OECD, APEC, CERT collectives.

The necessity of multilateralism emerges because countries have different rules to regulate extradition and legal assistance as well as different substantive laws that govern computer crime (Barkham 2001).

Operational efforts to prevent and respond to computer attacks must be global and so far, the most effective international cooperation to respond to cyber attacks were informal bilateral in nature (Vatis, 2003, pp. 1-2).

There are advantages and disadvantages of all of these four types of cooperation. For example, Vatis reveals some of the obstacles facing MLATs as following: First, the scope of the MLATs is narrow in terms of the number of the countries. For example, the US State Department has mutual legal assistance in criminal matters treaties (MLATs) in force with nineteen countries. Secondly, most of these treaties do not cover cybercrime specifically or in general terms (Vatis, 2003, p. 2). Finally, application of the MLATs can be time consuming since they may involve more paper work and other bureaucratic procedures. This final obstacle may not be a major problem for traditional crime when the issue is physical evidence; however, in cybercrime, time is significant since it may take a few minutes if not seconds to destroy evidence or lose track of criminals (Vatis, 2003, p. 3).

In addition to the issues discussed above, there are more fundamental issues involving international cooperation. First of all, the growth of computer technology and reliance on these types of technologies may differ from country to country. In other words, some countries have not yet seen such a crime while others may have experienced many such crimes; therefore, while some countries may have substantive and procedural laws regarding cybercrime and cyberterrorism investigation, others may not have a clue as to what these concepts represent (Vatis, 2003, p. 3). The second important reason is that it may become very difficult to distinguish cybercrime from information warfare, given the fact that many countries are developing cyber techniques for fighting a war or intelligence purposes (Speeches and Testimony 1998).

Vatis considers bilateral cooperation more feasible and gives some examples:

- In February and March 1998, more than fifty civilian, government, and private sector computer systems in the US were affected when intruders penetrated at least 200 unclassified US military personnel and other government computer systems. The timing of these attacks coincided with the increase of the US military presence in the Middle East. The NIPC, working closely with Israel's law enforcement, identified two people in Cloverdale, CA, and individuals in Israel who were the true perpetrators
- In February 2000, the NIPC received reports that CNN, Yahoo, Amazon.com, e-Bay and other sites had been attacked through Distributed Denial of Service (DDOS), in which intruders took over the networks. The investigation has been carried out by the NIPC along with the cooperation of the companies. The attacks have been traced to Canada. The NIPC has worked with the Royal Canadian Mounted Police (RCMP), to arrest a juvenile, called "Mafiaboy."
- In May 2000, individuals and companies around the world were attacked by the "Love Bug" or "I LOVEYOU" virus. The NIPC investigated the incident and identified the suspect by tracing the attack to the Philippines. The FBI working closely with the Philippines' National Bureau of Investigation identified the suspect, Onel de Guzman (2003, p. 7).

These are real world examples of bilateral cooperation between law enforcement agencies from two different countries. They are promising in a sense that they prove that working together creates results.

Cue´llar, in his article, focuses on the importance of international treaty in terms of responding to cybercrime and cyberterrorism. He summarizes the effect of treaty with respect to its political consequences which may advance underlying goals of security and safety: a) deterrence of specific offenses: treaties among states allow for extradition and prosecution which will marginally enhance deterrence against cybercrime and cyberterrorism. In other words, cyber offenders, in general, will be deterred from committing cybercrime since jurisdictional difficulties to investigate the offense will be removed with treaties. b) International cooperation for legal cooperation: Treaty will encourage cooperation between signatory countries' law enforcement entities. c) Enhancing prospects for technical cooperation beyond the boundaries of treaty: Since treaty will be a starting point to have an international consensus as to which actions define cybercrime or cyberterrorism against civil aviation, eventually law enforcement and other entities responsible for investigating and prosecuting cybercrime and cyberterrorism will go beyond the confines of the treaty (Cue´llar, 2001, p. 121).

Public and Private Cooperation

"The Internet and other aspects of the information infrastructure are inherently transnational" (Sofaer and Goodman, 2001, p. 2). The transnational nature of cybercrime and cyberterrorism mandates that public and the private sectors to work together and cooperate.

"The most active international cooperation for cyber security has been in law enforcement;" however, there has not been large scale cooperation outside of law enforcement" (Lewis, 2003, p. xix).

For example, even though critical infrastructure protection has a law enforcement component, issues can go beyond the capacity of law enforcement and becomes an issue of national security (Lewis, 2003, p. xix).

"Cyber attacks are far less damaging than physical attacks" (Lewis, 2003, p. xiv).

Cyberterrorism and cybercrime could also overlap in damaging ways; groups can steal credit card numbers or important data to damage economies and for their own gain" (Lewis, 2003, p. xv). Localized law enforcement efforts toward cyber criminal activities are at a disadvantage in an interconnected world due to the limited jurisdiction that every law enforcement agency has.

The next section focuses on the efforts aimed at responding to cyberterrorism and cybercrime. The examples are both of national and international level of cooperation between law enforcement agencies as well as international entities. They also include public- private cooperative efforts.

National Level Efforts toward Countering Cyberterrorism and Cybercrime

United States

The United States is one of the leading countries with respect to taking necessary measures to respond to threats coming from cyberspace. Especially since the terrorist attacks on September 11, 2001, both the US and the rest of the world had increased their efforts towards defending against the threats of terrorism, in particular, in the realm of cyberspace (Lawson, 2002, p. 9).

In terms of the critical infrastructure, and in particular, information infrastructure protection, the steps that the US has taken as a response to cyber threats can be divided into four major periods (Westby et al., 2003). The first is the President's Critical Infrastructure Protection Board formed in 1996 by former President Bill Clinton. This board did not have regulatory power; however, it provided a significant amount of information and research specifically focusing on different aspects of critical infrastructures. It shows the willingness to identify the vulnerabilities of the country stemming from its critical infrastructures. In 1996, President Clinton announced of the establishment of the President's Commission on Critical Infrastructure Protection (PCCIP). The purpose of the formation of such a Commission is to assess the vulnerabilities of the nation's life support systems. The Commission identified eight infrastructures: Telecommunications, banking and finance, electrical power, oil and gas distribution and storage, water supply, transportation, emergency services, and government services. The Commission published a report based on the study they conducted. One of the critical findings that the PCCIP concluded was the potential threat which might emerge from cyberspace. They stated that It is not surprising that infrastructures have always been attractive targets for those who would do us harm. In the past we have been protected from hostile attacks on the infrastructures by broad oceans and friendly neighbors. Today, the evolution of cyber threats has changed the situation dramatically. In cyberspace, national borders are no longer relevant. Electrons don't stop to show passports. Potentially serious cyber attacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitered, clandestinely rehearsed, and then mounted in a matter of minutes, or even seconds, without revealing the identity and location of the attacker (1997).

The report has clearly shown the significance and importance of the problem. The evolution of cyber threat not only opens new avenues of operations for terrorists, but also potentially makes the task of the governments -responding to this threat- more difficult. Military installations, power plants, air traffic control centers, banks and telecommunication networks are the most likely targets. Other targets contain police, medical, stock exchanges, water systems, and power plants (Statistics on Cyberterrorism, 2000). As a result of that study, former President Clinton issued Presidential Decision Directives (PPD) which established policymaking and oversight bodies within the executive branch of the federal government (Westby, 2003, p. 16). For counterterrorism purposes, this Directive codifies and clarifies activities in a broad range of US counter-terrorism programs, including apprehension and prosecution of terrorists, increasing transportation security, enhancing response capabilities and protecting the computer-based systems that are at the heart of America's economy (Fact Sheet, 1998).

After going through different stages, the third step involves publication of a document, called, “National Strategy to Secure Cyberspace” in February 2003. In this document, the US government identifies three major strategic objectives:

- Prevent cyber attacks against America’s critical infrastructures;
- Reduce national vulnerability to cyber attacks; and
- Minimize damage and recovery time from cyber attacks that do occur.

Further, this document articulates five national security priorities: 1) establishing a National Cyberspace Security Response System, 2) developing a National Cyberspace Security Threat and Vulnerability Reduction Program, 3) preparing a National Cyberspace Security Awareness and Training Program, 4) securing governments' cyberspace, and 5) establishing national security and International security cooperation (The National Strategy to Secure Cyberspace, 2003, p. x).

This document is significant for this research because of the fact that it touches the heart of the matter: vulnerability. With respect to vulnerability, the ambition to develop a National Cyberspace Security Threat and Vulnerability Reduction Program seems quite promising. In the document, it is claimed that even though it may not be possible to stop every attack and eliminate every type of vulnerability, it proposes a three-part effort a) reducing threats and deter malicious attacks through effective programs to identify and punish them; b) identifying and eliminating vulnerabilities that could be dangerous if exploited, and c) assessing vulnerability of existing systems and developing a new system with less vulnerability (The National Strategy to Secure Cyberspace, 2003, p. 28). Another significance of this document is its emphasis on cooperation between the government and the public. Finally, its detailed analysis of the necessary actions to provide security for cyberspace as well reducing vulnerabilities represented a strong ambition to create a solution for the problem of vulnerability.

In order to achieve those objectives, The US Cyberspace Strategy document proposed eight major initiatives and actions as an attempt to reduce threat and vulnerabilities:

1. Enhance law enforcement's capabilities for preventing and prosecuting cyber-space attacks;

2. Create a process for national vulnerability assessments to better understand the potential consequences of threats and vulnerabilities;
3. Secure the mechanisms of the Internet by improving protocols and routing;
4. Foster the use of trusted digital control systems/supervisory control and data acquisition systems;
5. Reduce and remediate software vulnerabilities;
6. Understand infrastructure interdependencies and improve the physical security of cyber systems and telecommunications;
7. Prioritize federal cybersecurity research and development agendas; and
8. Assess and secure emerging systems (2003, p. xi).

The final step was the enactment of two pieces of legislation: a) Homeland Security Act of 2002, which created the Directorate of Information Analysis and Critical Infrastructure Protection within the Department of Homeland Security, b) the Federal Information Security Management Act (FISMA) of 2002.

Table 2

US Response Chart to Cyberterrorism

<table>
<tr><th colspan="2">Major Steps Toward Effective Response to Cyberterrorism in the United States</th></tr>
<tr><td colspan="2">➢ The President's Commission on Critical Infrastructure Protection (PCCIP)
➢ Presidential Decision Directives (PPD)
➢ Publication of the National Strategy to Secure Cyberspace
➢ Homeland Security Act of 2002</td></tr>
<tr><th>Legal Aspect</th><th>National Security</th></tr>
<tr><td>National Information Infrastructure Protection Act (NIIPA)
Electronic Communication Privacy Act (ECPA)
PATRIOT Act
Federal Information Security Management Act (FISMA)</td><td>Information Analysis and Infrastructure Protection (IAIP) Directorate
National Cyber Security Division
National Infrastructure Protection Center (NIPC)</td></tr>
<tr><th>Law Enforcement</th><th>Public-Private Cooperation</th></tr>
<tr><td>FBI National Computer Crime Squad
US Department of Justice Computer Crime & Intellectual Property Section
US Secret Service</td><td>National Cyber-Forensics and Training Alliance (NCFTA)
High Technology Crimes Task Force
Computer Emergency Response Team/ Coordinating Center (CERT/CC)
Forum of Incident Response and Security Teams (FIRST)</td></tr>
</table>

Legal approach to cyber security in the US. In the US, unlawful activities related to computers and other information systems are criminalized by federal and state statutes. Brenner claims that there are more than forty federal statutes that can be used to prosecute cybercrime (Brenner, 2001, p. 16). The US Congress has followed a dual approach to respond to computer related crimes (cybercrime) since 1984 (Jacobson and Green, 2002, p. 279). If the computers are subject to a crime, the US Congress enacted new legislation. On the other hand, if the computer is used to commit traditional crime, then the US Congress regulates that act by updating the existing legislation. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA) is the first comprehensive Federal legislation addressing the growing concerns of the government and private sector regarding computer fraud and crime (McDonald, 2004). The scope of the CFAA was limited, however, to crimes against "protected computers" used by the federal government and financial institutions, as well as crimes that were interstate in nature (Andreano, 2000, p. 213). The narrow nature of the CFAA resulted in modifications because of the change in the nature of computer crimes. In 1994 and 1996, the US Congress enacted the National Information Infrastructure Protection Act of 1996 (NIIPA). One significant change created by the 1996 Act was "the substitution of the term "protected computers," for "federal interest computers."   This is important because the statute protects any computer attached to the Internet, including all the computers located in any individual state of the Union" (Nicholson, Shebar, and Weinberg, 2000, p. 213).

The NIIPA of 1996, subsection 1030 (a) criminalized seven specific acts:

1. Makes it a crime to access computer files without authorization or in excess of authorization, and subsequently to transmit classified government information.
2. Prohibits obtaining, without access or in excess of authorized access, information from financial institutions, the United States government, or private sector computers that are used in interstate commerce.
3. Proscribes intentionally accessing a United States department or agency nonpublic computer without authorization.

4. Prohibits accessing a protected computer, without or beyond authorization, with the intent to defraud and obtain something of value (Jacobson and Green, 2002).

5. Addresses computer hacking, and criminalizes knowingly causing the transmission of a program, code, or command, and as a result, intentionally causing damage (Nicholson, Shebar, and Weinberg, 2000, p. 215).

6. Prohibits one with intent to defraud from trafficking in passwords which would either permit unauthorized access to a government computer or affect interstate or foreign commerce

7. Makes it illegal to transmit in interstate or foreign commerce any threat to cause damage to a protected computer with intent to extort something of value (pp. 280-284).

As a response to the devastating consequences of the September 11th, 2001, terrorist attacks and to other growing new threats, the US Congress amended the NIIPA of 1996 by introducing the PATRIOT Act of 2002. The Act gives federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence-gathering purposes (Doyle, 2002, p. 1). The Act widens the criminal nature of the actions directed at information systems, in particular, computers. The Act amends Section 1030 (a) (5) (i), (ii), and (iii). The Act prohibits the following:

(i) knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer;

(ii) intentionally accessing a protected computer without authorization, and as a result of such conduct, recklessly causing damage; or

(iii) intentionally accessing a protected computer without authorization, and as a result of such conduct, causing damage.

The subsection 1030 (a) (5) (A) (i) criminalizes knowingly causing the transmission of a program, code, or command, and as a result, intentionally causing damage to a protected computer. This regulation is applied regardless of whether the individual has authorization of access to a computer, in other words, authorized people in companies or in other entities can be prosecuted if they intentionally damage any protected computers (Ditzion, Geddes, and Rhodes, 2003, p. 294). The second fundamental change is that the PATRIOT Act criminalizes any unauthorized access to a protected computer even if the transmission by the user was unintentional, but was reckless (Schemmel, 2003, pp. 930-931).

There are other statutes that address and regulate criminal activities regarding cyberspace. These regulations are fundamentally important in their function to deter criminals from launching attacks against critical information infrastructures. These federal statutes are the Copyright Act and Digital Millennium Copyright Act, the National Stolen Property Act, the mail and fraud statutes, the Electronic Communication Privacy Act (ECPA), the Communication Decency Act of 1996, the Child Online Protection Act, the Child Pornography Prevention Act of 1996, and the Internet False Identification Prevention Act of 2000 (Ditzion et al., 2003, p. 299).

The next section examines efforts in the US toward critical information infrastructure protection and securing information systems and networks. The section focuses on three major components of such efforts: national security, law enforcement, and public-private cooperation.

National security.

- Information Analysis and Infrastructure Protection (IAIP) Directorate

With the enactment of the Homeland Security Act of 2002, the Congress created the Department of Homeland Security (DHS), which is an executive branch responsible for protecting the US from terrorist attacks. Not surprisingly, this task also involves cyber security. In fact, in two separate sections, the Homeland Security Act of 2002 defines responsibility of the DHS in terms of cyber security: Title II, which involves information analysis and infrastructure protection, and Title VIII, which focuses on coordination issues between DHS and non-federal entities (Westby, 2003, p. 83). Title II establishes the Directorate for Information Analysis and Infrastructure Protection headed by the Undersecretary for Information Analysis and Infrastructure Protection.

Among other responsibilities, the following specifically focus on critical infrastructure protection:

1. To access, receive, and analyze law enforcement information, intelligence information, and other information from the federal and local law enforcement agencies in order to determine the scope and nature of the threat to the US homeland, and also identify potential threats within the US.

2. To carry out full assessment of the vulnerabilities of key resources and critical infrastructures of the US

3. To integrate relevant information, analyses, and vulnerability assessments

4. To develop a comprehensive national plan for securing the key resources and critical infrastructure of the US including information and telecommunication systems in the US

5. To recommend necessary steps to be taken to ensure the security of the key resources and critical infrastructures of the US (Homeland Security Act of 2002).

Title VIII also focuses on coordination between the DHS and other entities. Parallel to this Act, the Multi-State Information Sharing Analysis Center (MS-ISAC) was established on January 30, 2003. The mission of the MS-ISAC is to “provide a focal point for gathering information on cyber and physical threats to critical infrastructures,” and its mission includes two-way information sharing on critical infrastructure cyber incidents and threats: a) Providing timely warnings of cyber and physical threats and attacks; and b) Producing comprehensive information and intelligence analyses to support federal, state and local first responders and law enforcement readiness and response efforts (MS-ISAC, 2003).

- National Cyber Security Division

In accordance with the National Strategy to Secure Cyberspace, prepared by the Bush Administration and the Homeland Security Act of 2002, the DHS created the National Cyber Security Division (NCSD) under the Department' s Information Analysis and Infrastructure Protection Directorate (Homeland Security Press Release, 2003). The mission of the NCSD is to "identify, analyze and reduce cyber threats and vulnerabilities; disseminate threat warning information; coordinate incident response; and provide technical assistance in continuity of operations and recovery planning" (Homeland Security Press Release, 2003). The NCSD will work with the US Secret Service, the Science and Technology Directorate, and the Department's Privacy Office. For some, this division will create another layer of bureaucracy (Mark, 2003), while others consider it as a "a strong office to focus squarely on the cyber threats that pose great harm to both the nation's physical and economic security" (Entrust, 2003).

- National Infrastructure Protection Center

The National Infrastructure Protection Center (NIPC) was established in 1998 as a division in the FBI. NIPC was founded as a "joint government and private sector partnership that includes representatives from the relevant agencies of the federal, state, and local government" [2] (NIPC 2001).

[2] The Center currently has representatives from the following federal entities: Navy, Air Force, Army, Air Force Office of Special Investigations, Defense Criminal Investigative Service, National Security Agency, United States Postal Service, Federal Aviation Administration, General Services Administration, Central Intelligence Agency, Critical Infrastructure Assurance Office, and Sandia National Laboratory. In addition,

The NIPC's mission is to detect, warn of, respond to, deter, and investigate criminal acts involving illegal computer intrusions and unlawful acts including physical and cyber, which target or threaten US critical infrastructures (Vatis 1998).

The NIIPC was organized into three major sections:

- Computer Investigations and Operations Section (CIOS): This section is the operational and response part of the NIPC. It provides support for the federal, state, and local agencies involving cyber investigations and other issues related to information infrastructures.
- Analysis and Warning Section: This section is responsible for warning related entities regarding computer intrusions and providing analytical analysis for cyber investigations, threat trends, and vulnerabilities.
- Training, Administration, and Outreach Section (TAOS): The responsibility of this section is to coordinate training and education programs for the FBI personnel, law enforcement personnel from federal, state, and local agencies, as well as individuals from the private sector (Vatis 1998).

As of March 1, 2003, NIPC was transferred to the Homeland Security Department under the Information Analysis and Infrastructure Protection Directorate.

Law enforcement.

- FBI National Computer Crime Squad

The FBI's National Computer Crime Squad (NCCS) is responsible for investigating violations of the Federal Computer Fraud and Abuse Act of 1986. These crimes defined by the Act include intrusions into financial, government, Federal interest

the Center has had state law enforcement officials detailed on a rotating basis. So far, there have been representatives from the Oregon State Police and the Tuscaloosa County (Alabama) Sheriff's Department, as well as international liaison officials who work with the Center.

computers, and most of the medical computers (Computer Fraud and Abuse Act 18 USC. Section 1030). In particular, privacy violations, industrial espionage, major computer network intrusions, and intrusions to other public switched networks are investigated by the NCCS.

- United States Secret Service

The US Secret Service is mandated by executive statute to fulfill two critical missions: protection and investigation. As a primary task, the US Secret Service protects the President, Vice President, their families, heads of the states, and other designated people. In addition to this vital task, the US Secret Service is responsible for investigating crimes, including financial crimes that include, but are not limited to, access device fraud, financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure (US Secret Service, 2002). In recent years, the US Secret Service has initiated new programs and strategies in order to increase cooperation and collaboration between the other law enforcement agencies and the private sector. In particular, the US Secret Service was heavily involved in fighting cybercrime in the early 1990s. It established its first Electronic Crime Squad Special Agent Program (ECSAP) in New York City (Wiles, 2002). Since its establishment, in 1995, the Secret Service has charged over 800 individuals with electronic crimes valued at more than $425 million (Enos, 2001). With the enactment of the PATRIOT Act of 2001, the Secret Service was given responsibility to widen its role in establishing electronic crime task forces nationwide (Westby, 2003).

The Act increases the Secret Service's role in investigating fraud and related activity in connection with computers, and gives authority to the Director of the Secret Service to establish nationwide electronic crimes taskforces in order to assist law enforcement, the private sector and academia in identifying and investigating computer-based crime, computer fraud, and cyberterrorism (US Secret Service, 2002). For instance, the US Secret Service established another Electronic Crimes Task Force in its Dallas bureau to combat regional computer-based crimes *(Dallas News*, 2003). The Secret Service represents a good example regarding cooperation among the federal and local law enforcement and private sectors in combating cyber related offenses. By arranging meetings with the representatives from law enforcement entities and private companies, the US Secret Service performs another important task, which is initiation of active communication between the Secret Service and other entities. In addition to those, the Secret Service also provides other services, such as Cyber Threat/Network Incident Report, which aims to receive timely complaints or service requests from companies, individuals and other entities regarding cyber threats and attacks (US Secret Service, 2002).

- US Department of Justice Computer Crime & Intellectual Property Section (CCIP)

The Computer Crime and Intellectual Property Section (CCIPS), which was created in 1991, is a section within the US Justice Department criminal division. The CCIPS is comprised of twenty-two attorneys who specialize in investigation of cybercrime. They also provide training, advising and coordination for prosecution of computer intrusion and intellectual property cases (CHIP, 2002). Under the CCIPS, there are several units and programs, including Computer and Telecommunications

Coordination Center and the Computer Hacking and Intellectual Property (CHIP). The CCIPS has a significant role in the international arena in terms of cybercrime investigation and responding to cyber related offenses. In particular, the CCIPS chairs the G-8 Subgroup on high technology crime that is responsible for coordination of the efforts in the investigation and prosecution of cybercrime cases (Westby, 2003, p. 112). The CHIP has offices in eight different cities in the US Its primary functions are Prosecution, Regional Prevention and Outreach, and Regional Training. Prosecution involves computer intrusions, copyright and trademark violations, theft of trade secrets and economic espionage, theft of computer and high tech components and other Internet crimes (CHIP, 2002). Regional Prevention and Outreach, on the other hand, focuses on coordination and collaboration between the FBI and other agencies to respond to high- tech crimes in the community and encourage victims of high- tech crime to report such crimes to law enforcement (CHIP, 2002). Finally, regional training involves providing training for other law enforcement agencies to increase knowledge and experience on cybercrime investigation and prosecution (CHIP, 2002).

Public-private cooperation.

- National Cyber-Forensics and Training Alliance (NCFTA)

The National Cyber-Forensics and Training Alliance (NCFTA) was developed as an outgrowth of Pittsburgh High Tech Crimes Task Force (HTCTF). The central idea of that project is the partnership between the FBI, the National White Collar Crime Center (NW3C), Carnegie Mellon University (CMU), and West Virginia University (WVU) (NCFTA, 2004). NCFTA offers advanced certificate programs aiming at digital evidence handling and other types of proactive and reactive response strategies. The new project will closely work with the industry, academia, and other related law enforcement agencies.

- High Technology Crimes Task Force

As a division under the FBI, the High Technology Crime Task Force describes its mission as “to provide forensic examination, intelligence, and technical assistance to agencies encountering computers during the course of their investigations” (High Tech Computer Crime Task Force, 2002).

- Computer Emergency Response Team / Coordinating Center (CERT/CC)

The CERT Coordination Center (CERT/CC) is located at the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania (CERT/CC, 2003). In order to better handle changes in the technology with respect to intrusion techniques and other system management techniques CERT/CC became part of the larger SEI Networked Systems Survivability Program, whose primary goals are to guarantee that appropriate technology and systems management practices are in use to resist attacks on computer networked systems and to minimize damage and make sure continuity of critical services regardless of successful attacks, accidents, or failures ("survivability") (CERT/CC, 2003).

- Forum of Incident Response and Security Teams (FIRST)

The Forum of Incident Response and Security Teams (FIRST) was founded in 1990 when it had only eleven members, but now FIRST has more than 100 incident response and security teams (FIRST 2002). These members are composed of teams from different entities including education, industry, commercial, government, and military.

The goals of the FIRST are:

- fostering cooperation among information technology constituents in the effective prevention, detection, and recovery from computer security incidents;
- providing a means for the communication of alert and advisory information on potential threats and emerging incident situations;
- facilitating the actions and activities of the FIRST members including research, and operational activities; and
- facilitating the sharing of security-related information, tools, and techniques (FIRST 2002).

By fulfilling these goals, FIRST can act as a mechanism for both prevention and recovery from attacks against information systems.

United Kingdom

In order to respond to possible threats against the critical infrastructures, Home Office established the National Infrastructure Security Coordination Center in 1999. The NISCC is responsible for coordinating:

1. dialogue with owners of critical national infrastructures systems to identify the most critical systems and work with them to attain a level of assurance about the security of these systems;
2. alerts of attack;
3. information about the threat;
4. expert protective security expertise and advice;
5. NISCC seeks to establish partnerships with critical national infrastructures providers and it is not regulatory (About NISCC 2001).

There are two other important entities within the NISCC: The first one is the United Kingdom Computer Emergency Response Team –CERT is known as UNIRAS. The critical function of the UNIRAS is to receive reports of major electronic attack incidents, threats, new vulnerabilities and countermeasures from its government, international, and customer base and other commercial sources (About NISCC 2001). The second one is the Electronic Attack Response Group (EARG). The EARG mobilizes the government's technical, security and emergency response resources to respond to serious electronic attack incidents (About NISCC 2001).

Telecommunications, energy, financial, central government, financial, transport, emergency services, water and sewage, and health services are identified as the critical national infrastructures by the British government

The Regulation of Investigatory Powers Act 2000 (RIPA) is one of the examples that United Kingdom has initiated to counter terrorism. It provides for and regulates investigative powers by a variety of public authorities to respond to changes in technology, in particular, the Internet (Crime and Policing 2000). According to the Home Office of United Kingdom, RIPA is consistent with the Human Rights Act of 1998, and creates a system with safeguards. It also reflects the requirements of Article Eight of the European Convention on Human Rights (ECHR) (Crime and Policing 2000). The Act clearly indicates the circumstances where authority may be used, especially Part II[3] of RIPA, which focuses on national security and terrorism coming from the Internet, and crime prevention. RIPA[4] is by far the most useful to law enforcement in analyzing

[3] RIPA Part II – Surveillance and Covert Human Intelligence Sources -Identify which grounds the directed surveillance is necessary:

In the interests of national security
For the purpose of preventing or detecting crime or of preventing disorder
In the interests of the economic well-being of the United Kingdom
In the interests of public safety
For the purpose of protecting public health
For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

[4] Cryptography can, for example, help instill trust in doing business over the Internet. This is because the technology offers the following services: integrity (guaranteeing that data has not been accidentally or

Internet interceptions. It has the power to enable police, customs officials and members of the judiciary to serve notices on individuals or bodies requiring the disclosure of encrypted information or messages (Merl, 2001, p. 275). RIPA provides broader authority for law enforcement in their investigations. In particular, interception, acquisition and disclosure of communication data, encryption, and surveillance are the major areas where the authority of the public has been broadened.

RIPA has been criticized for several reasons. First of all, the law is weak in terms of the protection of privacy and imposition of regulation of electronic communication (Akdeniz, Taylor, and Walker, 2001, p. 90).

International Level

Group of 8

The Group of 8 (G-8) countries is composed of the US, United Kingdom, France, Germany, Japan, Canada, Italy, and Russia. The leaders have been meeting annually since 1975 to discuss issues of importance, including crime and terrorism, and the information highway (Group of 8 2003). The G-8 Subgroup on High-Tech Crime was founded in 1997. In January 1997, the G-8 also set up a 24/7 " 24-Hour-Contact-Group"

deliberately corrupted); authentication (guaranteeing that the originator or recipient of material is the person they claim to be); and confidentiality (protecting a message to ensure that its contents cannot be read by anyone other than the intended recipient); availability (assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them); non-repudiation (preventing the denial of previous commitments or actions).   The confidentiality aspect of the technology also presents opportunities for criminals to protect or "encrypt" the content of their communications (such as emails) or stored data (their computer disks, for example) in an attempt to evade detection. The measures in Part III of the Regulation of Investigatory Powers Act 2000 seek to help ensure that the effectiveness of powers and functions of public authorities are not undermined as the technology concerned becomes more readily available and easier to use. Part III of The Act will be used to allow lawful access to protected information in an intelligible form (plaintext). The request for disclosure of such information will be qualified. The giving of a notice under Part III will ensure that due consideration has been given to the authorization of such a notice RIPA Part III: Investigation of Electronic Data Protected by Encryption.

to facilitate law enforcement communications for investigations (Group of 8 2003). This type of network enabled group members to foster speedy communications between and among the members which allow them to preserve digital evidence until legal processes can be started (Vatis, 2003, p. 3). The idea is to produce global agreements so that there cannot be digital havens where anybody can plan shady business (Hancock 2003).

The G-8 also held meetings between law enforcement and industry representatives, and through these meetings the G-8 aims to foster cooperation, not only among the law enforcement from group members but also industries so that each party can present their concerns, experiences, and visions (Vatis, 2003, p. 5). These activities have had several impacts; including being a model for larger and formal multilateral efforts, and identifying difficulties that individual states and multilateral entities may encounter (Vatis, 2003, p. 5).

In October 1999, the G-8 ministers adopted: Principles on Transborder Access to Stored Computer Data" which has three major sections. The first section focuses on preservation of data stored in computer systems.

> Each State shall ensure its ability to secure rapid preservation of data that is stored in a computer system, in particular data held by third parties such as service providers, and that is subject to short retention practices or is otherwise particularly vulnerable to loss or modification, for the purpose of seeking its access, search, copying, seizure or disclosure, and ensure that preservation is possible even if necessary only to assist another (State Principles On Transborder Access 1999).
>
> The second section focuses on expedited mutual legal assistance:
>
> Upon receiving a formal request for access, search, copying, seizure or disclosure of data, including data that has been preserved, the requested State shall, in accordance with its national law, execute the request as expeditiously as possible (G-8 Countries Combat Organized Crime 1999).

The third section focuses on the transborder access to stored data not requiring legal assistance:

> Notwithstanding anything in these Principles, a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of:
>
> a. accessing publicly available (open source) data, regardless of where the data is geographically located;
> b. accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data (State Principles On Transborder Access 1999).

This particular section has significant importance in terms of jurisdictional issues. It allows a country to penetrate to another member state if the investigation involves jurisdiction via cyberspace as long as the state informs the member being searched of the search after the search occurred; in other words, they are required to provide a post-search notification of the searched state (Putnam and Elliott 2001, p. 65).

The G-8, in another meeting in 2000, published Okinawa Charter on Global Information Society and indicated its commitment to creation of an international cooperation to target cybercrime (G7-G8 Summit in Okinawa 2000). This meeting created another task force-- the Digital Opportunity Taskforce (dot force)-- in order to integrate its efforts into a broader international approach (G7-G8 Summit in Okinawa 2000). To this end, the dot force will convene as soon as possible to explore how best to secure participation of stakeholders. This high-level Taskforce, is in close consultation with other partners in a manner intended to be responsive to the needs of developing countries.

Efforts made by the G-8 states demonstrate the importance of the cooperation at the international level which may lead to creation of criminal deterrence in a sense that the investigation and prosecution of the criminal act should be swift and certain.

The G-8 held a meeting in Paris, France in May 2003 and ended up with three significant decisions with respect to critical infrastructure protection: They determined that they needed unprecedented global cooperation to protect their information infrastructures, including computer network and communication systems. They also need to respond to terrorist and criminal threats against them (Meeting of G8 Ministers of Justice and Home Affairs 2003).

Council of Europe (CoE)

The Council of Europe (CoE) is an intergovernmental organization, which is made up of forty-five European countries (Council of Europe 2003). In addition to 45 countries, states such as the US, Canada, and Japan have observer status in the CoE (Council of Europe 2003).

In 2001, CoE held a Convention on Cybercrime, and non-European countries, such as the US, Canada, and Japan participated in the drafting process. The underlying reasons behind having a convention are described thus by the CoE (International Working Group 2002):

- Considering that the aim of the Council of Europe is to achieve a greater unity between its members;
- Recognising the value of fostering co-operation with the other States parties to this Convention;
- Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international co-operation;

- Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;
- Concerned at the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;
- Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;
- Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

The purpose of this convention was "to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of electronic evidence of a criminal offence" (International Working Group 2002). According to Weber, the Convention on Cybercrime establishes three general principles to international cooperation.

> First, international cooperation will be provided among the states "to the widest extent possible". Second, the obligation to cooperate extends not only to the crimes established by the treaty, but also to the collection of electronic evidence whenever it relates to a criminal offense. Third, the provisions for international cooperation do not supercede preexisting provisions of international agreements on these issues (2003, p. 433).

The CoE has taken a more comprehensive approach by publishing and refining a draft on cybercrime (Sofaer 2001). The Draft includes a detailed description of the concepts, computer system, computer data, and data traffic (Convention on Cybercrime 2001). The Draft also includes several provisions which criminalize some of the activities in cyberspace. Chapter II defines specific crimes against computer systems: Offences against the confidentiality, integrity and availability of computer data and systems are defined under Title 1. These are:

> a) Illegal access is defined as an act "committed intentionally, the access to the whole or any part of a computer system without right,… with the intent of

obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system" (Article 2 Illegal Access).

b) Illegal interception is defined as an act "…committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data (Article 3 – Illegal interception).

c) Data interference defines the act which is "committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

d) System interference is an act "committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data (Article 5 – System interference).

e) Misuse of devices is an act which is the "the production, sale, procurement for use, import, distribution or otherwise making available of a device and password (Article 6 Misuse of devices).

Title 2 defines Computer-related offences, which are

a) Computer-related forgery which is defined as any " input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches (Article 7 – Computer-related forgery.)

b) Computer-related fraud which is defined as the causing of a loss of property to another by any input, alteration, deletion or suppression of computer data, or any interference with the functioning of a computer system (Article 8 – Computer-related fraud).

Title 3 defines content-related offenses which involve child pornography and criminalizes producing, offering, distributing, procuring, and possessing child pornography though and/or in a computer and/or computer system (Article 9 Offences Related to Child Pornography). Title 4 defines offenses related to infringements of copyright and related rights.

The significance of that convention is that once in force, all countries that ratified the Convention on Cybercrime, including those who are non-member observer states, are required to standardize their laws to comply with the provisions of the Convention (Westby 2003). Those countries which are signatory states are required to adopt such domestic laws in order to establish minimum standards (Council of Europe 2001). In Budapest, on November 23, 2001, the CoE opened the treaty for signature by the member states and by non-member states, including the US As of December 2002, there were thirty-two signatories and it had been ratified by Albania and Crotia (Weber, 2003, pp. 429-430).

Of course, there is some criticism towards the Draft of the Convention regarding issue of human rights and information freedom. For some, the Draft was contrary to well-established norms for the protection of the individual; It improperly extends the police authority of national governments; It will undermine the development of network security techniques; and it will reduce government accountability in future law enforcement conduct" (Ever, 2000). Some even said this treaty will "kill the Internet" (Davis, 2003, p. 217). Nevertheless, the convention addresses deterrence as a necessary function and it aims at swift and efficient law enforcement effort toward cybercrime detection, investigation, and prosecution all of which will protect "confidentiality, integrity, and availability of computer systems" (Baron, 2002, p. 268). The treaty of the CoE on cybercrime is significantly important for a number of reasons. "The Council's approach recognizes that accomplishment of this goal is predicated upon finding solutions to the lack of criminal statutes, the lack of procedural powers, and the lack of enforceable mutual assistance provisions that result from the jurisdictional gap in cybercrime regulation" (Weber, 2003, p. 430).

European Union (EU)

European Union (EU) has emerged from three organizations formed in the 1950s by Belgium, West Germany, France, Italy, Luxembourg, and the Nederland: the European Cola and Steel Community (ECSC), the European Atomic Energy Community (Euratom), and the European Economic Community (Sussmann, 1999, p. 479). “The EU is, in fact, unique. Its Member States have set up common institutions to which they delegate some of their sovereignty so that decisions on specific matters of joint interest can be made democratically at the European level” (The European Union at a Glance 2003). Currently there are more than twenty-five member states within the EU. With respect to cyber security and critical infrastructure security, EU has published several documents. The EU also created entities to respond to the challenges of critical information infrastructure security. Among these efforts, in April 1998, the European Commission prepared a study called COMCRIME which focused on security of information infrastructures and combating computer-related crime (Cybercrime European Commission 2004). In January 1999, the European Parliament and the Council adopted an action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. In the Tampere Summit of the European Council held in October 1999, it was concluded that in order to agree on common definitions and sanctions, high-tech crime should be included (Cybercrime European Commission 2004). In 2001, Cybercrime European Commission prepared a document entitled Network and Information Security: Proposal for a European Policy Approach, in which the following four conditions were presented as key conditions in order to be successful in responding to cybercrime and information infrastructure vulnerabilities (Cybercrime European Commission 2001):

- The adoption of adequate substantive and procedural legislative provisions to deal with both domestic and transnational criminal activities.
- The availability of a sufficient number of well-trained and equipped law enforcement personnel.
- The improvement of the co-operation between all the actors concerned, users and consumers, industry and law enforcement.
- The need for ongoing industry and community-led initiatives.

Another significant effort by the EU is the eEurope 2005 Action Plan which was approved by the European Council in June 2002 (Council of Europe 2002). The central component of the eEurope 2005 Action Plan is information infrastructure protection (Westby, 2003). It stresses “the importance of ensuring the appropriate security of networks[5] and the information systems transmitted through them for individuals, business, administrations and other organizations” (Council of Europe 2002).

Another significant decision by the EU with regard to critical information and infrastructure protection is creation of the European Network and Information Security Agency (ENISA). The objectives of the ENISA is to facilitate and intensify European coordination in the area of information security, provide the highest security of the information infrastructure systems for the Members, and to create common understanding of information security among the member states in the EU (Information

[5] Definitions : "network" which refers to transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed and mobile terrestrial networks, networks used for radio and television broadcasting, and cable TV networks; "information system" understood to mean computers and electronic communication networks, as well as electronic data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance; "network and information security" defined as the ability of a network or an information system to resist accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services that may be offered by these networks and systems.

Society 2003). The management board of the Agency will be composed of five representatives appointed by the Council, five by the Commission, two by the European Parliament, as well as four industry and two consumers' representatives (EU News Report 2003). The agency will have a budget of 24 million euro over a five year period and it is intended to help the Commission and the Member States cooperate more efficiently in their responses to information security and network problems such as viruses and unauthorized interception of communications, computer crashes, and information technology (IT) network failures (EU Business 2003).

United Nations (UN)

The United Nations (UN) has increased awareness of information security, in particular, computer related crimes. In 2000, the Tenth United Nations Congress on Crime Prevention and the treatment of Offenders was held in Vienna, Austria. In sum, the meeting emphasized the importance of internationally coordinated efforts toward preventing and responding to threats against information systems and cyber security. In addition, it is emphasized that the exchange of technical and forensic expertise between national law enforcement authorities are crucial for faster and effective investigation of such crimes (Tenth United Nations Congress 2000). Furthermore, in different meetings, the Members of the UN have expressed their concerns about the threat of cybercrime and cyberterrorism, and proposed training programs about cyberterrorism for the national law enforcement agencies (Security Council 4792nd Meeting 2003).

Asia Pacific Economic Cooperation (APEC)

APEC was formed in 1989 in response to the growing interdependence among Asia-Pacific economies, and since then, APEC has become the primary regional vehicle for promoting open trade and practical economic cooperation (TIA Online 2002). Asia Pacific Economic Cooperation (APEC) established the Telecommunication and Information Working Group (APEC-TEL), which provides coordination between the governments, private sectors, and business of the twenty-one APEC members (Westby 2003, p. 103).

The Fifth APEC Ministerial Meeting on Telecommunications and Information Industry was held in May 2002 in China and the Members of the APEC declared the need for economies to promote the development of advanced, secure and reliable information infrastructures and expressed their commitment to improve the multilateral and bilateral cooperation in the APEC region in developing telecommunications regulatory policies, and information and network security (APEC Shanghai Declaration 2002). They also made clear that it is very important to establish a legal basis to address the criminal misuse of information technologies and law enforcement cooperation in combating that misuse (TELMIN 2002).

Organization for Economic Co-operation and Development (OECD)

Organization for Economic Co-operation and Development (OECD) defines cyber security in their Guidelines for the Security of Information Systems as “the protection of the interest of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity” (OECD 2002).

The Guidelines for the Security of Information Systems and Networks addresses some of the fundamental issues regarding cyber security. It is stated that due to increased interconnectivity, information systems and networks have now become more vulnerable to a growing number and a wider variety of threats, which explains one of the fundamental issues in information security (OECD 2002). By stating "… participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks" the OECD put the responsibility on the shoulders of every member in the organization (OECD 2002). The OECD Council adopted nine important principles[6] in July 2002 (Westby 2003, p. 73) to develop "the culture of cyber security" (OECD 2002).

Interpol

The International Criminal Police Organization-"Interpol" was established in 1956 to globally enhance and facilitate cross-border criminal police cooperation (Interpol 2003). Currently, there are 181 countries on over five continents that participate. Interpol is the largest international police organization, which serves as an entity to help member countries with their investigations involving international crimes.

[6] 1. Awareness: Participants should be aware of the need for security of information systems and networks and what they can do to enhance security. 2. Responsibility: All participants are responsible for the security of information systems and networks. 3. Response: Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents. 4. Ethics: Participants should respect the legitimate interests of others. 5. Democracy: The security of information systems and networks should be compatible with essential values of a democratic society. 6. Risk assessment: Participants should conduct risk assessments.7. Security design and implementation: Participants should incorporate security as an essential element of information systems and networks. 8. Security management: Participants should adopt a comprehensive approach to security management. 9. Reassessment: Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

Interpol, among other crimes, focuses on the misuse of information technologies under the name of information technology crime (Interpol 2003). Interpol has created parties of information technology crime in regions around the world. Instead of establishing a new division, Interpol gathered “working parties” or experts from members of national computer crime units (Interpol 2003). Currently there are five major working parties that the Interpol works with: a) European Working Party on Technology Crime, b) American Regional Working Party on Information Technology Crime, c) African Regional Working Party on Information Technology Crime, d) Asia-South Pacific Regional Working Party on Information Technology Crime, and e) Steering Committee for Information Technology Crime (Interpol 2003). Among these working groups, the European Working Party on Technology Crime, formed in 1990, has shown significant achievements, including the compilation of the Computer Crime Manual, now called the Information Technology Crime Investigation Manual (ITCIM), a best practice guide for the experienced investigator, numerous training courses in order to share its expertise with other members, a rapid information exchange system which essentially consists of two elements, and preparing Training video / CD-ROM for international law enforcement (Interpol 2003).

European Police Office (Europol)

The Council Act of July 26, 1995 signed up the Convention on the establishment of a European Police Office[7] (Europol Convention 2003) (Europol), which was established to

[7] This Convention establishes a European Police Office, "Europol", to be located in The Hague, Netherlands. Its task is to improve the effectiveness of the competent authorities in the Member States and cooperation between them in an increasing number of areas preventing and combating terrorism, unlawful drug-trafficking, trafficking in human beings, Crimes involving clandestine immigration networks,

improve police cooperation between the Member States to combat terrorism, illicit drug trafficking, and other serious types of international crime, became fully operational in 1999 (Area of Security 2003). The official inauguration of Europol in 1998… marked a new watershed of EU cooperation in the field of "Justice and Home Affairs"… which reflects a shift in the direction of supranationalism and away from Europe's long-standing intergovernmental approach to international law enforcement" (Occhipinti, 2003, p. 1).

Europol has also the following principal tasks (Europol 2003):

- to facilitate information exchange between Member States;
- to obtain, assemble and analyze information and intelligence;
- to notify the authorities of the Member States without delay of information concerning them and of any relations identified between criminal offenses;
- to assist investigations in the Member States;
- to keep a computerized system of collected information.

In other words, Europol can serve as an effective mechanism in terms of investigating crimes involving information technologies, such as cybercrime and cyberterrorism.

> It is important to emphasize that Europol will not have executive authority, and it is important that Europol should not be viewed as a European equivalent of the Federal Bureau of Investigation in the United States. Nor will Europol take over from, or place any type of restraint on, national counter-terrorist agencies (Marotta, 2001, p. 18).

However, according to Occhipinti, recent developments indicate that the nature of collaboration on policing in the EU has become more supranational and the EU will move even closer to having a supranational form of police cooperation, "including a role for Europol that increasingly resembles that of the US FBI." (2003, p. 238).

illicit trafficking in radioactive and nuclear substances, illicit vehicle trafficking, combating the counterfeiting of the euro, money-laundering associated with international criminal activities.

Privacy

There is always tension between enforcing laws and protecting civil liberties. Responding to crime, in particular, terrorism and cyberterrorism causes the emergence of such debate as to what the power and limit of the government should be. In particular, terrorism makes things more complex because of the fact that one of the purposes of terrorism is to force the government to overreact so that the government, itself, uses some type of force to suppress the terrorist activity. “By overreacting or by failing to pull back after weakening or defeating the terrorists, the state itself may subvert democracy if it employs severe countermeasures” (Warlaw 1994, p. 7). Privacy is one of the issues that is potentially a candidate for a great deal of controversy.

As William Cohen, Secretary of Defense in the Clinton Administration, states,

> … we, as a democratic society, have yet to come to grips with the tension that exists between our constitutional protection of the right to privacy with the demand that we made on the need to protect us. It would be a mistake to place our national security and law enforcement institutions in a position where they would have to compromise our precious hard-won rights or infringe upon our privacy in order to protect us. The worst possible victory granted cyber-attackers would be one that destroyed these values, whereby we would become less open, less tolerant and less free (2000).

There are principles that are applicable in the investigation and prosecution of cyber related criminal activities. These general legal principles include the right to privacy, protection from unwarranted search and seizure, the protection against self-incrimination, and the right to due process (Drozdova, 2001, p. 184).

Privacy has been endangered not only by the intrusion of the government, but criminals and non-criminal entities also contribute to the problem of privacy. While hackers, cyberterrorists, and other types of cyber criminals abuse the Internet and other computer networks, private companies can create consumer and communication profiles with or without the knowledge of individual's by using increasing data transaction through networks. That type of profiling may also result in intrusion of individuals' privacy.

In fact, the problem of privacy represents one of the most controversial aspects of the Internet and enforcing cybercrime laws (Selin 1996, p. 377).

Privacy is one of the critical issues for this study because not only does it reflect the characteristics of the country but also it can be an important determinant in terms of the level of vulnerability. It is true that countries where democratic values and fundamental human rights, in particular, privacy, are ensured and protected by the law, cyber criminals and cyberterrorists may have more opportunities to attack, as opposed to other countries where every single movement by an individual or entity is closely monitored. The next section focuses on the concept of privacy and some of the key sources of debate and discussion emanating from some of the strategies, programs, and applications the governments and international entities have implemented at the national and international level.

Definition

There is no commonly acknowledged definition of what privacy is (Blume, 2000, p. 193). In 1763, in England, William Pitt wrote "the poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter- but the King of England cannot enter" (as cited in Merl, 2001, p. 268-269). Today, the term privacy has been defined in a number of ways.

Westin defines privacy as "the claim of individuals, groups, and institutions to determine for themselves, when, how, and to what extent information about them is communicated to others (1967).

According to Holvast (1993), the concept of privacy has three aspects: a) territorial privacy, which can be defined as protecting the close physical area surrounding a person, b) privacy of the person, which is provided by protecting a person against undue interference, such as physical searches or information violating his moral sense; and c) informational privacy: which is control of whether and how personal data can be gathered, stored, processed, or selectively disseminated (as cited in Fisher-Hubner, 2000, p. 173).

Several versions of privacy definitions also specifically focus on privacy in network systems and communication systems. In communication networks or computer systems privacy is defined as:

- the protection given to information to conceal it from persons having access to the system or network.
- the protection given to unclassified information, such as radio transmissions of law enforcement personnel that requires safeguarding from unauthorized persons,
- the protection given to prevent unauthorized disclosure of the information in the system (Federal Standard 1996).

Privacy Protection Models

Privacy in cyberspace can be protected through different models, three of which are public enforcement, sector-specific regulation, and self-regulation (Drozdova, 2001,

p. 198). Public enforcement involves close scrutiny over the procedures and practices of law enforcement activities that aim at investigating and prosecuting cyber related offenses. Public officials, such as ombudsman, commissioner, or registrar enforce data protection laws through monitoring compliance, investigating any wrong-doing by law enforcement, and the like. Sector-specific regulations, on the other hand, cover specific sectors, such as video rental records or financial privacy. Self regulation is the last alternative model through which private companies establish codes of practice (Drozdova, 2001, p. 198). Drozdova claims that public enforcement provides a higher level of privacy protection than self-regulation; however, in both cases, if the data is transmitted beyond the control of the government (to another country with a less powerful level of privacy protection) and private company (to a company with lower standards of privacy protection) then these models either totally lose their function or they become less powerful (Drozdova, 2001, p. 199).

The US Perspective and Privacy

Even though individual states have enacted several laws and developed new strategies, programs, and policies to respond to new crimes, they are not free from criticism by the public, including civil rights organizations, academicians, and the like. Privacy becomes a major issue of controversy both in the international and national arena, and the US is no exception. In fact, three distinct examples of controversial programs and policies from the US are given in the next section, all of which represent discussion over their legitimacy, justification of their existence, and possible problems emanating from their application.

The first is a program, called Carnivore, which was developed by the FBI in 1999. Carnivore is a tool that provides proactive capability for intelligence gathering, and serves in the interest of national security (Merl, 2001). Carnivore was created to respond to crimes committed through the Internet, including, terrorism, organized crime, and other types of crimes (Accelerated Promotions 2004). Carnivore works like a pocket sniffer. First, it filters a portion of network traffic or it looks for the particular information which may identify the criminal subject (Dunham, 2002, p. 545). Then, if the related information is detected, the packets of communication that belong to the suspected person are separated for further filtering and storage based on the specifics of the warrant (Merl, 2001). Carnivore will store the email address or the entire information packet depending on the search given to law enforcement. Other packets which are unrelated to the specific investigation are neither recorded nor saved by the FBI.

There are two views of the use of Carnivore and privacy concerns. On the one hand, the government considers the system as a necessary tool since it performs a remarkable balancing act in a highly efficient way (Strauss, 2002, p. 237). According to Merl, the heightened capability through instantaneous Internet connections is not the only problem facing the US but the threat to global security in the new century by cyber criminals is also a problem; therefore, it is justifiable to use tools like Carnivore (2001, p. 257). Another rationale for the FBI to design Carnivore is that many Internet Service Providers (ISPs) lack the ability to identify the messages of a specific subscriber while excluding the messages of all other people (Accelerated Promotions 2004).

On the other hand, the opponents of Carnivore present several problematic issues. Electronic Privacy Information Center (EPIC) is one of the entities focusing on privacy issues. According to EPIC, there are three major problems with the use of Carnivore: 1) the likelihood that Carnivore performs broader sweep over Pisa's transmissions. Carnivore on the Internet captures much more information from an individual than does the other tools, such as pen registers and trap and trace devices (Statement of The Electronic Frontier Foundation 2000). The system seems to exacerbate the over-collection of personal information by obtaining more information than it is legally entitled to, which may result in having the potential to turn into mass surveillance systems, thus threatening an open and free society (Statement of The Electronic Frontier Foundation 2000). Even the independent review which was commissioned by the Justice Department also found that the system is capable of "broad sweeps" (Electronic Privacy Information Center – EPIC 2002). 2) The ability of Carnivore to transmit information about non-suspects, as well as suspects violates the Fourth Amendment. The system is criticized because there is the potential for information about non-criminal individuals to be passed through the system (Dunham 2002). 3) The lack of personnel accountability in the FBI causes concerns for over-collection (Electronic Privacy Information Center – EPIC 2000). According to critics, Carnivore does not include appropriate safeguards to prevent misuse and might violate the constitutional rights of individuals (Carnivore 2002).

As a response to the criticism, some claim that Carnivore does not contravene the Fourth Amendment's protection against "unreasonable searches and seizures" because a person does not enjoy a "reasonable expectation of privacy" of their e-mail headers (Strauss, 2002, p. 232). In fact, when the EPIC sued the FBI due to employment of Carnivore, the FBI defended the system by assuring the public that it only captures online information and email authorized for seizure by the court order (Konrad 2000).

The second major source of debate nowadays is the PATRIOT Act (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) of 2001. This Act makes significant changes to more than 15 federal statutes (Schachter, p. 197, 2002). Although the Act is aimed at terrorism and incidents related to terrorism, it covers a wide range of topics including terrorism, money laundering, wiretaps, expanded search warrants, the Foreign intelligence Surveillance Act (FISA), investigation techniques involving different computer technologies, and other computer related offenses. The heart of the matter in this Act is that it grants federal agencies greater power to trace and intercept communications of terrorists, both for law enforcement and intelligence purposes. However, there are critics who consider such authority potentially dangerous in terms of the power and ability it gives to the government.

In terms of privacy, Rotenberg claims the USA. PATRIOT Act "is the most sweeping expansion of government surveillance authority" (2002, p. 1116). Moreover, for some, the Act may go too far because it gives authority to monitor e-mail communications, to share grand jury information with intelligence and immigration officers, to confiscate property, and to impose new book-keeping requirements on financial institutions (Schachter 2002). In terms of investigating cyberterrorism or crime related to the cyber environment, the law permits criminal investigators to retrieve the content of electronic communications in storage, like e-mail, with a search warrant. Furthermore, the communication may be kept in remote storage for more than 180 days without notifying the subscriber (18 USC. 2703).

The significance of the PATRIOT Act regarding authorization of the government to monitor, detect, and investigate suspected activity on the Internet or other network systems is that probable cause, which is one of the corner stones of the Fourth Amendment of the Bill of Rights, is not required. Instead the Act gives law enforcement the authority to obtain Web addresses, session times, and e-mail addresses if the agent certifies that the information is “relevant to an ongoing criminal investigation” (Osher, 2002, p. 527).

In addition to Carnivore and the PATRIOT Act, President's Commission on Critical Infrastructure Protection (PCCIP) was also criticized for a number of reasons. According to EPIC, “almost every solution proposed by the commission represents some new expansion of government authority and some new encroachment into personal liberty” and the propositions by the PCCIP could result in creation of the development of a large-scale monitoring policy for communications networks (EPIC 1998).

In another testimony, Marc Rotenberg, Executive Director of the EPIC, criticized the government for their inability to secure computer systems without significantly damaging the privacy of individuals. In fact, EPIC claims that “the federal government’s recent efforts to promote computer security in the private sector have created more problems than they have solved” (2000). They also claim that privacy safeguards placed by the government are insufficient (Rotenberg 2000).

International Perspective on Privacy

While at the national level privacy is protected through constitutions, legislative instruments, and self-regulations, there is no globally agreed upon level of protection of citizens' rights due to international variance in legal practices, normative standards, and political objectives (Drozdova, 2001, p. 184). Trade-offs between privacy and intrusion by the government or private industry can vary depending on the historical and social background of a country.

In the international arena, privacy is recognized as one of the fundamental human rights by the 1948 Universal Declaration of Human Rights. In this Declaration, it is stated that "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attack upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attack" (Article 12). It also states that "everyone has the right to freedom of opinion and expression; This right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers" (Universal Declaration of Human Rights- Article 19). Drozdova considers these provisions the source of the basic framework for the international law for the right to privacy, which could be extended to cyberspace (Drozdova, 2001, p. 188).

In terms of personal data protection, however, the OECD was the first international organization to issue a policy on protection of personal data. It is called "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," which was adopted in 1980. OECD also published "Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security" in 2002. In this document, the OECD, among other things, emphasizes the value of democracy[8] and the confidentiality of information, which is, thus, a focuses on the value of privacy.

EU Perspective on Privacy

EU can currently be considered as the region in the world where the personal data has reached the highest degree of particularization (Rodota 2003, p. 81). While EU has also embraced both the CoE's and UN's declarations, it also has specifically indicated protection of "personal data and privacy for users of publicly available electronic communication services" in Directive 2002/58/Ec of the European Parliament and of the Council (2002). The EU Directive[9] is aimed at enforcing a relatively high standard of data protection (Hubner, 2000, p. 174). In fact, the protection of personal data has been recognized as a fundamental human right by the EU (Rodota, 2003, p. 81). The system in the EU was set up to:

- Increase the level of personal data protection in the individual member states;

[8] Democracy: The security of information systems and networks should be compatible with essential values of a democratic society. Security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency (Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security).

[9] 9EU Directive on Personal Protection, Article 6: Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Article 7: Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or Article 28 Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

- Confer the power to control and develop the operation of this integrated system of personal data protection on supranational bodies, for instance by updating the existing directives or adopting new directives;
- Create a geographic and political area where personal data may move freely across the borders of member states; and
- Make physical and logical security of data banks a prerequisite for the protection of personal data by providing that member states should take adequate measures to be complied with by any entity processing data (Article 17 of Directive 95/46).

The importance of this Directive is that it provides a formal standard for an international treaty, which envisages multilateral coordination (Rodota, 2003, p. 83). It also emphasizes the vitality of having a similarly high level of coordination between individual member states and other third party nations that are not members of the EU. This is one of the most critical aspects of that Directive because without such a comprehensive approach, which emphasizes broader involvement, it may not be possible to accomplish the full scale of cyber security because of its transnational character.

While the EU has provided a high level of protection for personal data, it also appreciates the fact that there should be tools available to law enforcement agencies of the member states, as well as the Europol. Especially when it comes to terrorism and transnational cybercrime, the EU emphasizes that law enforcement be under scrutiny by an independent authority.

Council of Europe (CoE) Perspective on Privacy

CoE, on the other hand, revealed a similar approach in its Convention for the Protection of Human Rights and Fundamental Freedoms in 1950. It was then stated:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (Article 8, Right to Respect for Private and Family Life).

The CoE has been one of the major players in the arena of international data protection (Blume 2000). The CoE[10] considers privacy one of the fundamental rights of an individual (Council of Europe 1981). While the CoE provides tools to law enforcement agencies, it also creates entities to protect the integrity of privacy in order to ensure privacy protection. Therefore, the CoE requires an independent authority outside of police to monitor the use of data by the police (Blume 2000).

The Draft, written as a result of the CoE Convention on Cybercrime is opened to signatures by the member states. "The treaty addresses the controversy of interception of communications data for the purpose of criminal investigations, and requires signatory states to grant law enforcement authorities the power to collect or record traffic or content data in domestic law" (McAuliffe 2001). However, in the Convention, the issue of privacy is defined in the `illegal interception` section so as to protect "the right to privacy of data communication" (Keyser 2003).

[10] Council of Europe Convention on Cybercrime Article 15 – Conditions and safeguards: 1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure. 3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, a Party shall consider the impact of the powers and procedures in this Section upon the rights, responsibilities and legitimate interests of third parties.

Controversial Applications at the International Level

Although there have been several pieces of legislation, policies, and programs put into practice in different countries, one program has been under the spotlight of the international community, in particular, in Western democracies. The project, called ECHELON, "is the term popularly used for an automated global interception and relay system operated by the intelligence agencies in five nations," including the United States, the United Kingdom, Canada, Australia and New Zealand (What is Project ECHELON 2002).

The US National Security Agency (NSA) created a global spy system, codename ECHELON, which captures and evaluates almost every phone call, email, fax, and telex message sent anywhere in the world, and therefore, the system is considered the greatest surveillance effort ever established (Poole 2002).

ECHELON is controlled by the NSA, and it is operated by the combination of the Government Communications Head Quarters (GCHQ) of England, the Communications Security Establishment (CSE) of Canada, the Australian Defense Security Directorate (DSD), and the General Communications Security Bureau (GCSB) of New Zealand. These organizations are bound together under a 1948 agreement, UKUSA, whose terms and text remain classified even today (Poole 2002).

The ECHELON system captures all satellite, cellular, microwaves, and fiber-optic communications traffic, and process this information through the massive computer capabilities of the NSA, including advanced voice recognition and optical character recognition (OCR) programs. It looks for code words or phrases (known as the

ECHELON “Dictionary”) that will prompt the computers to flag the message for recording and transcribing for future analysis (Sassen 2004).

Among the activities that ECHELON targets are: terrorism, political spying, and commercial espionage (Poole 2002).

The author of this research believes that the following passage is important in its perspective on justification of deployment of such a system.

> …ECHELON must be permitted to function in the most effective manner possible that does not unacceptably compromise the privacy and freedoms that are so important to Americans. It is understandable that this may involve some invasion of the privacy of American persons, but this is a balance that must be maintained. While the prospect of occasionally having innocent e-mail messages screened by a NSA computer is troublesome, the prospect of inhaling sarin gas on the New York City subway system is far more alarming. Given our democratic form of government, this balance must be dictated by our elected officials, namely Congress and the President (Sloan 2001).

This paragraph is a common justification by those who advocate the limitation of privacy for the sake of national security and crime prevention. The question, then, will be what is the limit, if there is one? Or, to what extent are individuals willing to give up their privacy rights, if they are so willing? Nevertheless, at the international level “a global harmonization of privacy legislation is very difficult to achieve due to cultural, political, and historical differences” (Fischer-Hubner, 2000, p. 174).

Summary

Responding to cyberterrorism or cybercrime necessitates careful and vigilant analysis of the vulnerabilities which may possibly exist in the critical information infrastructures of any given country. The possible lack of legal precedent, and the unique political and cultural characteristics of each country complicate the issues. In any case, transnational response to those criminal activities requires all concerned parties work together at all fronts, technically, legally, politically, and culturally. However, such a commitment also requires efforts both at the domestic and international level. As revealed in chapter 2, there are a variety of strategies, policies, and techniques that individual countries, as well as international and supranational entities have instituted. While these efforts are promising and give ample reasons to be optimistic, there is a long way to go.

It is vital to respond to vulnerabilities emerging from reliance on technology and motivation and capabilities of terrorists, organized crime groups, individuals, and other criminal groups to launch cyber attacks against critical information infrastructures without violating the fundamental rights of law-abiding citizens. In other words, there is a delicate balance between responding to a very serious crime and maintaining the integrity of the other people’s fundamental rights, particularly, in the case privacy issues. Concrete and sound cooperation at the domestic (national) and international level will help to maintain that balance, which requires awareness and determination.

CHAPTER 3

RESEARCH DESIGN AND METHODOLOGY

Introduction

The purpose of this chapter is to explain the overall methodology of the research and present the detailed research plan. Specifics discussed include the purpose of the research, research questions, research plan, overall methodology, explanation of research design, construction of the research instrument, and limitations of the research.

Purpose of the Research

The purpose of this study is to identify major factors affecting or constructing the major variables: vulnerability, comprehensive cooperation, and freedom. This study was also aimed at identifying the relationship between major variables of the research. Further, the research developed a scale that involves vulnerability, freedom of society, and comprehensive cooperation. The research also attempted to create a typology of cyberterrorism based on expert opinions.

Problem Statement

The problem of this research has two features: A general problem and a specific problem of the research.

General Problem

The general problem of the research is that vulnerability emerges from increased reliance on technology, lack of legal measures, and lack of cooperation at the national and international level. In sum, lack of global consensus in terms of responding to cyberterrorism and cybercrime is the general problem. Even though the problems with respect to responding to cyber attacks are addressed, the critical concepts, such as vulnerability versus responding to these vulnerabilities, and the effectiveness of these policies, cannot be measured due to the lack of available data on the number of cyber attacks, nor the effectiveness of response policies at the national and/or international level. The general problem of the research is also illustrated in the following figures.

Figure 1. Exploratory illustration of vulnerability-cooperation-freedom model.

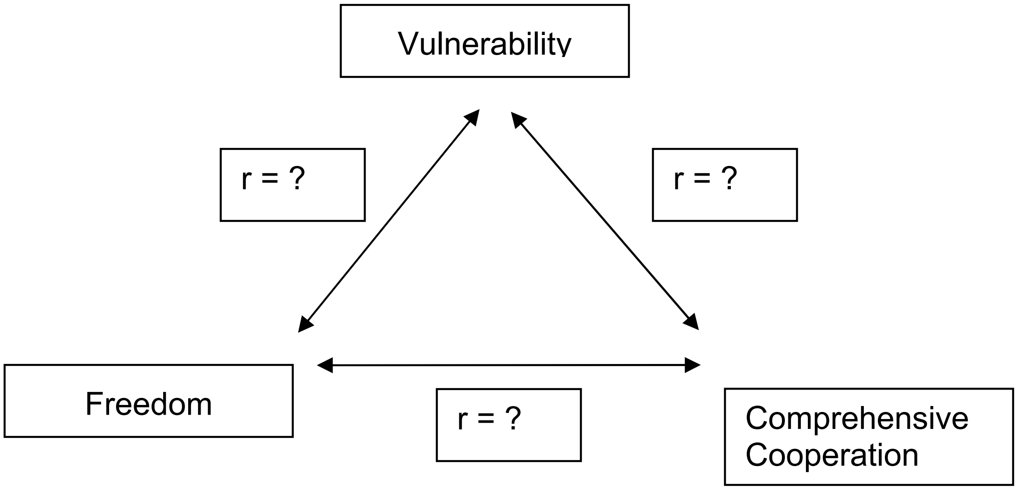
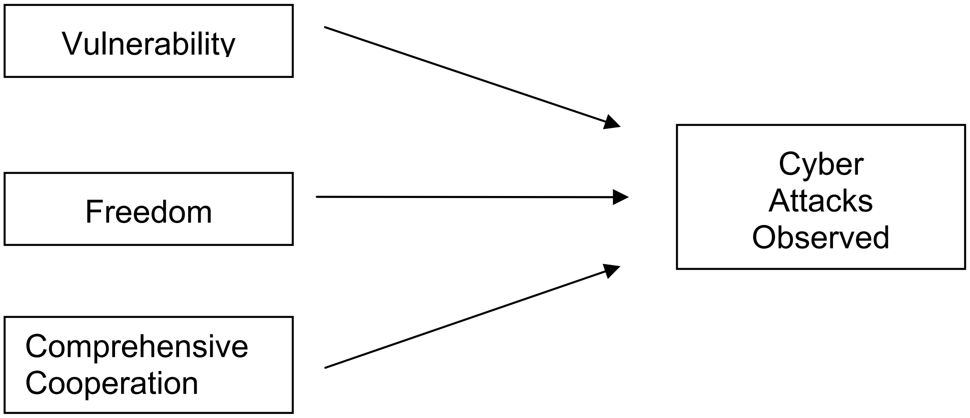


Figure 2. Vulnerability-cooperation-freedom model for future studies.



Specific Problem

The specific problem of the research is that there is no operational measurement of these three important variables: vulnerability, freedom, and law enforcement cooperation. This research will attempt to create operational measurement of these three variables. In particular, the research will attempt to identify the factors constructing vulnerability, comprehensive cooperation, and freedom.

Also, while the literature review revealed different typologies of cyberterrorism, there is a need for comprehensive academic research to identify types of cybercrime techniques which may be used by terrorists to carry out cyber attacks or communication. Due to disagreement as to what cyberterrorism means and what terrorists can do by using the Internet and computer networks, there is confusion about what cyberterrorism constitutes. Therefore this research attempted to clarify the concept of cyberterrorism, as well as to create a typology of cyberterrorism.

Research Questions

The research questions are as follows:

1. What are the factors constructing vulnerability, comprehensive cooperation, and freedom?
2. What is the relationship between vulnerability, comprehensive cooperation, and freedom based on expert opinion? The analysis will be exploratory, and it will analyze the realistic approach versus the liberal approach presented in Chapter 2
3. What is the association between cybercrime techniques and cyberterrorism in terms of using these techniques as cyberterrorism?
4. What are the problems affecting cooperation at the national and international level? The answer to this question will be based on qualitative analysis of the responses from experts.

5. Based on the statistical analysis, what is the rating of vulnerability-comprehensive cooperation-freedom for each country from which the experts are drawn?

6. What are proposed solutions to overcome obstacles of responding to cybercrime and cyberterrorism at the policy level?

Research Plan

The research of this study involves five major components. First, the introductory information about the research and a brief analysis of the problem was presented in the first chapter. Second, the research reviewed the related literature in Chapter Two. The third part of the research involved construction of a scale, which will explore the vulnerability of nations to cyberterrorism. To do so, the research attempted to construct a scale, which was explained in the following section. The fourth component of this research involves analysis of the responses to the survey instrument use to construct the scale. The final component of this research focuses on the conclusive analysis and further recommendations with respect to responding to cyberterrorism and cybercrime.

Methodology

This research involves a modified Delphi method which according to Ludwig "combines quantitative and qualitative methods to explore the future" (as cited in Nelson, 2002, p. 5). Delphi method was originally developed by the RAND Corporation in the 1960s as a forecasting method (Cline 2000). The basic premise of the Delphi method is that it "is based on structural surveys and makes use of the intuitive available information of the participants, who are mainly experts. Therefore, it delivers qualitative as well as quantitative results and has beneath it explorative, predictive even normative elements" (Cuhls, 2003, p. 96).

Fowles (1978) reveals ten fundamental steps to implement the Delphi method:

1. Formation of a team to undertake and monitor a Delphi on a given subject.
2. Selection of one or more panels to participate in the exercise. Customarily, the panelists are experts in the area to be investigated.
3. Development of the first round Delphi questionnaire
4. Testing the questionnaire for proper wording (e.g., ambiguities, vagueness)
5. Transmission of the first questionnaires to the panelists
6. Analysis of the first round responses
7. Preparation of the second round questionnaires (and possible testing)
8. Transmission of the second round questionnaires to the panelists
9. Analysis of the second round responses (Steps 7 to 9 are reiterated as long as desired or necessary to achieve stability in the results.)
10. Preparation of a report by the analysis team to present the conclusions of the exercise (as cited in Illinois Institute of Technology 2004).

Gordon, on the other hand, summarizes these steps into four major steps. The first involves selection of participants; In fact, he considers selection as "the key to a successful Delphi study" (Gordon, 1994, p. 6). The second major step is to formulate the questions, and the third step involves sending questions, evaluating responses and forwarding them to the same or different group of experts for re-evaluation (Gordon, 1994). The final step involves analysis of the responses.

In Delphi method fifteen to twenty participants are acceptable numbers (Ludwig 1997). A response rate of forty to 75% can be anticipated (Gordon, 1994, p. 7).

Gordon also analyzes the strength and weaknesses of the Delphi method. According to him, the Delphi method is a powerful method to "…explore, coolly and objectively, issues that require judgment…" (1994, p. 9). More importantly, the Delphi method is constructive and “… more valuable for analyzing evolving trends than existing conditions” (Nelson, 2002, p. 8).

On the other hand, the method also has weaknesses, which may limit the research results. First, Delphi is a time consuming method (Gordon, 1994). Secondly, the level of reliability in the outcome of the study puts the burden on the quality of the experts selected by the researcher (Makridakis and Wheelright 1978 as cited in Nelson, 2002, p. 9). Nevertheless, the next section discloses detailed explanation of the steps for designing the research instrument.

Research Design

As indicated before, this research uses a modified Delphi method. Delphi method is an appropriate methodology for this study since the survey involves several judgment questions for which expertise is necessary to answer. To construct the survey, the first major step involved identifying the participants of the research. In other words, the experts whom the questionnaire is sent are identified. Since the main focus is responding cyberterrorism and identification of vulnerability, the experts were chosen such that they reflect a variety of expert positions. They are not randomly selected to establish the reliability of the responses. In other words, to ensure the accuracy of the responses, the participants of this research are selected based on their expertise. Experts in this research involve academics who focus on cyberterrorism, terrorism, and cybercrime. In addition to academicians, practitioners from the field who have hands-on experience in terms of terrorism and cybercrime investigations and prosecutions are selected. Moreover, since responding to terrorism, in particular, cyberterrorism involves national security and law enforcement efforts, the experts who are practitioners are chosen from both law enforcement and the national security area. It is also necessary to state that some countries of focus have different systems that combine law enforcement and national security under one agency's jurisdiction.

Pilot Study

After identification of the participants, the next step is to formulate the questions. To do that, the researcher prepared a pilot survey, which included questions that to be distributed to the actual participants of the research. Before delivering the survey to the experts, the researcher selected three experts, including academicians and practitioners who have experience and high-quality background in the areas of terrorism, cyberterrorism, and cybercrime. These experts were given the questions so that they could analyze and give recommendations about the format and content of the questions. The purpose of the pilot study was to have a more comprehensive and powerful survey. Based on the responses, the researcher could modify, change, and reformulate the questions.

Research Instrument

After the questionnaire was prepared based on the pilot study, the questionnaire (Appendix A) was sent to the participants, who were experts from the United States, Canada, and EU countries, such as United Kingdom, and, Germany, and Turkey.

The research instrument of this study is a questionnaire which was distributed to the experts including academicians and practitioners from variety of fields including terrorism, information science, political science, and criminal justice. The scale was constructed to analyze vulnerabilities of the nations to cyberterrorism. The literature review showed that vulnerabilities to cyber attacks against nations' critical infrastructures and other information infrastructures can vary from country to country. Moreover, we have problems emerging from the nature of cyber attacks, which were revealed in the second chapter. Briefly restated, cyber attacks are difficult to detect. Even though they are detected sometimes, target entities or individuals are hesitant to report or publicize them. For those reasons, the number of cyber attacks are difficult to identify, and most of the time the source of these numbers are anecdotal. Nevertheless, the literature shed light on some of the issues and sources creating vulnerabilities, some of which may be exploited by cyberterrorists and cyber criminals.

Scale Constructs

This research involves three major constructs, which are vulnerability, cooperation, and freedom.

The questionnaire involved the total of 28 survey questions; however, 17 items in the survey were used to do factor analysis. The other items in the survey are used for other purposes including creation of a typology of cyberterrorism, to explore the importance of cooperation, and to analyze the role of multilateral organizations with regard to responding to terrorism, in particular, cyberterrorism.

Every question in the questionnaire addresses a small portion of the scale. The scale involves a 1-7 style of the Likert scale, and depending on the content of the question, every item in the questionnaire constructed one of the three major variables vulnerability, comprehensive cooperation, or freedom.

The variables were identified based on the literature review. There are three main variables in this research: vulnerability, freedom of the society, and comprehensive cooperation. All of the three variables have several indicators. In the next section, conceptual definitions of these variables and their indicators are stated.

The first category of the survey involves analysis of the vulnerability variable in terms of the factors creating vulnerability. Vulnerability in this research is defined as any weakness stemming from any weakness of a system security, lack of awareness of potential attacks, lack of legal systems criminalizing any action against critical information infrastructures, presence of terrorist groups which may have motivation and capability of cyber attacks, and lack of cooperation and coordination among law enforcement entities and between the public and private sectors.

The vulnerability construct has several items. The first one is the level of economic development indicated by the GNP per capita and percentage growth in GNP per capita (Poe and Tate, 1994, p. 858). The level of reliance on technology involves the following items: The number of Internet service providers, the number of people who have Internet connection, the level of dependency on telecommunication services whose indicator is the number of telephone lines in use and cellular telephones in a country, the level of dependency on automated systems, including transportation and communication, the total amount of money invested for technology, and the level of public and private sector awareness against the threat of cyber attacks, targeting the critical information infrastructures.

These questions actually explore the level of possible impact of cyber attacks by the terrorists and other criminal groups. It is expected that the greater the expected impact of such attacks, the more vulnerable the country will be. Not only will terrorists have more opportunity to attack, but also they will have high motivation to execute their actions by targeting critical information infrastructures, given the fact that the attack will have a greater impact.

Question # 1: What is your assessment of the vulnerability of the United States to cyber attacks by groups including terrorists and unfriendly nations?

The purpose of asking this question is to explore the initial response of the experts before they answer the next questions, which are expected to determine specific factors that may lead to increased vulnerability.

Question# 2: What is your assessment about the level of motivation of the terrorist group(s) to target the United States?

This question is acquired from the literature, which considers the motivation as one of the fundamental factors leading terrorists executing cyber attacks against target countries. Even if the organizations including terrorists and criminal groups, or individuals have the capability, if they do not have the motivation of using their capabilities, they may not carry out cyber attacks.

Question# 3: What is your assessment about the level of capability of the terrorist group(s) to carry out cyber attacks against the United States?

This question explores the second important concept, which may indicate the probability of execution of cyber attacks by terrorists. Similarly, even if the organizations including terrorists, criminal groups, or individuals have the motivation to carry our cyber attacks, if they do not have the capability, then it will be impossible for them to succeed.

This question will be an essential determining factor as to whether the terrorists will be able to initiate cyber attacks.

Question # 4: What is your assessment about the level of economic development in the United States and its vulnerability to cyber attacks by terrorists and unfriendly nations?

The literature reveals that economically developed countries become more vulnerable to cyber attacks as opposed to developing or under-developed countries. This question explores the responses from the experts on the issue of the relationship between level of economical development and vulnerability of the country to cyber attacks.

Question# 5: What is your assessment about the relationship between the level of industrialization in the United States and its vulnerability to cyber attacks by terrorists and unfriendly nations?

The level of industrialization is also another determining factor. Vulnerability is expected to increase as the level of industrialization increases.

Question# 6: What is your assessment about the relationship between the number of Internet users in the United States and its vulnerability to cyber attacks by terrorists and unfriendly nations?

The number of Internet users is an important indicator as to the level of economic development and access to communication technologies. It is also a critical factor that may determine the level of vulnerability in a given country, considering the fact that the impact of a cyber attack against the computers will be greater, or in other words, the impact of a cyber attack may create massive fear in countries where the number of Internet users is greater than in other countries.

Question# 7: What is your assessment about the relationship between the number of Internet Service Providers in the United States and their vulnerability to cyber attacks?

Similar to the question# 6, the number of Internet Service Providers in a country can be a powerful indicator about the number of Internet users, as well as an indication of the level of public and private sector reliance on communication technologies.

Question# 8: What is your assessment about the relationship between the level of the US dependency on telecommunication services and its vulnerability to cyber attacks terrorists and unfriendly nations?

Reliance on technology is one of the most critical sources of vulnerability according to literature. Dependency on technology is one of the indicators of reliance on technology. Therefore this question will explore the experts' opinion about the accuracy of this proposition. Those countries which rely heavily upon technology are expected to have the greatest vulnerability.

Question# 9: What is your assessment about the relationship between the level of dependency on automated systems in the United States and its vulnerability to cyber attacks by terrorists and unfriendly nations?

Similar to question# 8, reliance on technology is one of the most critical sources of vulnerability, and the level of dependency on automated systems is also one of the indicators of reliance upon technology. This question will explore the essence of the level of dependency on automated systems and its relationship with the vulnerability variable.

Question# 10: What is your assessment about the relationship between the total amount of money spent on technology in the United States and its vulnerability to cyber attacks by terrorists and unfriendly nations?

This question explores the relationship between the total amount of money spent on technology in a given country and its vulnerability. This question assumes that the greater the amount of money spent on technology, the more vulnerable the country will become because eventually the reliance on technology increases if it is not already high.

Question# 11: What is your assessment about the level of public and private awareness against the threat of cyber attacks by the cyberterrorists targeting critical information infrastructure in the United States?

This question involves exploring the level of public and private sector awareness of the importance and necessity of taking measures that will ensure the security of critical information infrastructures. Awareness, or lack thereof, may reduce or increase the vulnerability of the critical information infrastructures to cyber attacks.

Question# 12: Given the factors above, would you change your assessment of the vulnerability of the United States to cyber attacks by cyberterrorists?

This question attempts to compare the experts' responses to Question# 1 and their responses to Question# 12. The difference between the two might reveal the extent of the relationship between the factors determined by the previous questions. The second category of the survey involves questions which will explore the second variable of the research: Freedom. Freedom in this research is defined as a person's protection of privacy from intrusive actions of the government, other individuals, and organizations. The Freedom scale in this research is similar to the Freedom scale in the Freedom House's *Freedom in the World* survey, except this research narrows its focus. In fact, this research focuses only on the issue of privacy. The indicators of this item include laws that lead to intrusive government and law enforcement practices and the presence of laws which criminalize the actions of individuals that may result in interference of one's privacy.

Question# 13: What is your assessment of the level of freedom (civil liberties) in the United States?

This question solicits the experts to answer based on their expertise. Although Freedom House offers an academically reliable source of information regarding the level of freedom in a given country, the researcher will have a chance to make a comparison between the Freedom House *Freedom in the World* Survey and the responses from the experts.

Question# 14: Are you aware of the “Freedom” scale used by Freedom House?

This question explores the knowledge of the experts regarding the existence of the Freedom House database.

Question# 15: What is your assessment about the following statement? “The system of government (SoG) in the United States facilitates freedom”.

Similarly, this question explores the level of facilitation of freedom by the system of government in a country. It will again compare the responses from the experts and the data from Freedom House.

The third, and final, category of the survey involves cooperation, which incorporates law enforcement cooperation and public and private cooperation. Cooperation is defined as any effort on the side of law enforcement agencies to ensure the security of the people and public and private entities from any cyber attack carried out by terrorists and other criminals. Law enforcement cooperation also incorporates the legal measures that a given country takes. Finally, law enforcement cooperation involves multilateral and bilateral agreements with which a country can participate, to establish cooperation with other countries and third parties. These agreements can be bilateral or multilateral. The indicators of this variable are composed of several items. The first involves the legal aspect of the efforts aiming at criminalizing actions and easing the cooperation process, which involves investigating and prosecuting terrorists. MLATs, conventions involving international participation, multilateral and bilateral cooperation among countries, presence of entities which facilitate cooperation at the national and international, and cooperation between the government and the private sector are the indicators of the law enforcement cooperation variable.

Question# 16: Assess the level of cooperation between law enforcement agencies and the private sector in the United States?

The level of cooperation between law enforcement and the private sector is one of the most important aspects of effective response to cyber attacks according to literature. Therefore, this question enables the researcher to explore the experts' responses regarding the level of cooperation.

Question# 17: Is there a clearly designated agency for investigating cyber attacks?

In order to have law enforcement cooperation, it is vital that a country have such an agency or entity which is responsible for investigating and prosecuting cyber attacks.

Question# 18: Do existing multilateral international agreements and efforts adequately defend the United States against cyberterrorism?

International cooperation, in particular, multilateral cooperation represents one of the most important aspects of law enforcement cooperation toward more effective response strategies to cyber attacks. This question explores the existence of such agreements and efforts and their strength in terms of adequately defending the country against cyber attacks.

Question# 19: What is your assessment on the importance of multilateral cooperation to respond to terrorism?

Cooperation may involve bilateral or multilateral efforts. This question explores the importance of multilateral cooperation.

Question# 20: Do existing bilateral agreements adequately defend the United States against cyberterrorism?

In addition to multilateral cooperation, bilateral cooperation is also crucial to adequately respond to cyber attacks. This question explores the existence of such agreements and efforts and their strength in terms of adequately defending the country against cyber attacks.

Question# 21: Do existing international organizations, such as the UN, OECD, G-8, and EU provide an environment through which the United States can effectively respond to terrorism?

According to literature review, there are several international organizations, conventions, and other entities which have made an effort toward creating effective response strategies and techniques. This question attempts to identify the level of importance of the each international organization.

Question# 22: What is your assessment on the importance of bilateral cooperation to respond to terrorism?

This question attempts to determine the importance of bilateral cooperation.

Question# 23: In your assessment, which one is more effective in responding to terrorism?

International cooperation is at the heart of the matter when it comes to responding to terrorism. Nevertheless, in the literature, there are comparisons between multilateral and bilateral cooperation in terms of their effectiveness on responding to terrorism. This question explores the responses from the experts.

Question# 24: In your assessment, which one is more achievable?

This question asks the experts their opinion about the probability of success of the bilateral and multilateral cooperation, and tries to find out which one is more achievable.

Question# 25: What is your assessment about the effectiveness of the existing substantive laws amended to respond to cyberterrorism?

According to the literature, one of the critical obstacles in terms of responding to cyber attacks is jurisdictional problems which give authority to law enforcement to investigate such activities. Existence of substantive laws targeting cyber attacks and attackers can be considered the first step toward an effective response; therefore, the purpose of this question is to explore the existence of substantive laws and their effectiveness.

Question# 26: What is your assessment about the effectiveness of the existing procedural laws (e.g. search and seizure laws, evidentiary standards, etc.) amended to respond to cyberterrorism?

This question also explores the existence of procedural laws that organize investigative activities of law enforcement. Therefore this question will determine whether or not procedural laws are present and if they are effective enough to carry out a decent investigation of cyber attacks and prosecution of responsible parties.

Question# 27: Please assess each of the following international organizations in terms of their effectiveness in responding to cyberterrorism? (1 = *not very effective*; 7 = *very effective*; DK = don't know)

United Nations (UN)	1	2	3	4	5	6	7	DK
European Union (EU)	1	2	3	4	5	6	7	DK
Council of Europe (CoE)	1	2	3	4	5	6	7	DK
Interpol	1	2	3	4	5	6	7	DK
Europol	1	2	3	4	5	6	7	DK
Group of 8 (G-8)	1	2	3	4	5	6	7	DK
Asia Pacific Economic Cooperation (APEC)	1	2	3	4	5	6	7	DK
Organization for Economic Co-operation and Development (OECD)	1	2	3	4	5	6	7	DK

The purpose of this question is to have a perspective on the effectiveness of international organizations in their responses to cyberterrorism.

The fourth category of the survey involves a typology of cyberterrorism.

Question# 28: In your opinion, which of the following techniques are associated with cyberterrorism? (1 = *no association*; 7 = *very strong association*; DK = don't know)

Unauthorized access	1	2	3	4	5	6	7	DK
Illicit tampering with files or data (unauthorized copying, modification, or destruction)	1	2	3	4	5	6	7	DK
Computer-mediated espionage	1	2	3	4	5	6	7	DK
Violations against privacy	1	2	3	4	5	6	7	DK
Virus	1	2	3	4	5	6	7	DK
Trojan horses	1	2	3	4	5	6	7	DK
Worms	1	2	3	4	5	6	7	DK
Denial of service attacks	1	2	3	4	5	6	7	DK
Money laundering	1	2	3	4	5	6	7	DK
Fraud	1	2	3	4	5	6	7	DK
ID theft	1	2	3	4	5	6	7	DK
Forgery	1	2	3	4	5	6	7	DK
Child pornography	1	2	3	4	5	6	7	DK
Communication	1	2	3	4	5	6	7	DK
Propaganda	1	2	3	4	5	6	7	DK
Fund raising	1	2	3	4	5	6	7	DK
Recruitment	1	2	3	4	5	6	7	DK

The purpose of this question is to have a typology which may be validated by the experts.

Analysis

Scale Construction

The second phase of the research involved analysis of the responses by the researcher. Since the research involved a pilot study and distribution of the survey to the actual group the experts, the analysis is composed of two phases. The first phase is the evaluation of the responses from the pilot group, which led to reformulation of the questions. The second phase of the analysis involves the evaluation of the responses from the group of experts. In other words, while the first phase of the analysis determines the content and the quality of the questions in the survey, the second phase of the analysis determines the outcome of the research. the final design of the Vulnerability-Cooperation-Freedom scale depends on the outcome of the second phase of analysis.

The six necessary steps for the construction of a Likert scale are as follows:

1. Compile a list of possible scale items
2. Administer these items to a random sample of respondents (in this research it is a targeted sample)
3. Compute a total score for each respondent
4. Determine the discriminative power of the items
5. Select the scale items
6. Test the scale reliability (Noachian and Noachian, 2000, p. 422)

In his book *Scale Development: Theory and Application*, Robert F. DeVellis presents a good outline and pathway toward developing a scale. There are necessary steps that need to be taken in order to develop and validate a scale. After determining what the research will measure, the second step is to generate an item pool, from which the items in the research instrument will be chosen. Then, the format of the measurement should be determined. In this research, twenty-eight items were created, and a 1-7 Likert scale is used. As explained earlier, these items will be reviewed by the expert panel in terms of their clearness, comprehensiveness, and appropriateness in explaining the constructs for the purpose of this research. In accordance with the recommendations from the panel of experts, the items were rephrased and distributed to the actual sample population, which is a list of experts from four different countries--the US, Canada, United Kingdom, and Turkey. The next step was to evaluate the items. A factor analysis was conducted in order to test the items' reliability, validity, variances, means, and coefficient alpha.

Reliability refers to the extent to which a measuring instrument yields the same results in repeated trials (Noachian and Noachian, 2000). Scale reliability, on the other hand, is defined as "the proportion of variance attributable to the true score of the latent variable" and "a scale is internally consistent to the extent that its items are highly intercorrelated" (DeVellis, 1991, pp. 24- 25). Internal consistency is equated with Cronbach's coefficient alpha, α, which is defined as the proportion of a scale's total variance that is attributable to a common source, presumably the true score of a latent variable underlying the items" (DeVellis, 1991, p. 27).

The coefficient alpha is one of the most important indicators of a scale's quality. There are different approaches to determining the acceptable value of alpha. According to DeVellis (1991, p. 85):

- Below .60 unacceptable
- Between .60 and 65 undesirable
- Between .65 and .70 minimally acceptable
- Between .70 and .80 respectable
- Between .80 and .90 very good.

Validity, on the other hand, is concerned with the question of whether the researcher is measuring what he or she intends to measure. Reliability is a necessary, but not sufficient, condition for validity. Validity is inferred from the way in which a scale is constructed, the ability of a scale to predict specific events, or its relationship to other constructs' measures (DeVellis, 1991, p. 43).

Chapter 4 presents detailed explanation of reliability and validity issues. In addition to SPSS statistical factor analysis, LISREL software package was also used to analyze factors which were identified based on the statistical analysis. The relationships between these indicators, factors, and major constructs (vulnerability, cooperation, freedom) were analyzed as exploratory research.

Scale construction relies on the responses from the experts. As indicated before, a Likert scale with 1-7 rating is used in this research; therefore, the rating will be based on this rating. The rating strategy is taken from the rating system used by the Freedom House[11], a nonprofit organization that aims at promoting democracy and human rights around the world (Freedom House 2002).

Vulnerability ratings. There are 4 types of vulnerability ratings: not vulnerable, somewhat vulnerable, vulnerable, and completely vulnerable. Ratings are as follows:

[11] "Freedom House is a clear voice for democracy and freedom around the world. Founded over sixty years ago by Eleanor Roosevelt, Wendell Willkie, and other Americans concerned with the mounting threats to peace and democracy, Freedom House has been a vigorous proponent of democratic values and a steadfast opponent of dictatorships of the far left and the far right." (Freedom House http://www.freedomhouse.org).

Table 3

Vulnerability Ratings

Score	Rating
1	Not vulnerable
2 – 3	Somewhat vulnerable
4 – 5	Vulnerable
6 – 7	Completely vulnerable

1.0 – 2.5: Not vulnerable.

The designation of not vulnerable, somewhat vulnerable, vulnerable, and completely vulnerable cover a broad range. It is necessary to state that a 1 – 2.5 rating does not represent exactly the same level of vulnerability. In other words, being in the same category does not mean that they have exactly the same characteristics in terms of the variables constructing vulnerability. Therefore, the values of 1 and 2 do not represent the same level of vulnerability; however, in terms of categorization, they will be named as “not vulnerable”. Rating 1 represents the lack of reliance on technology, lack of dependency on automation, lack of economical or industrial development, and a small number of Internet users, or ISPs. More importantly, this rating represents no threat coming from terrorist or unfriendly nations. This fundamental condition may put a country in a category of less vulnerability even though a country may heavily rely on technology, have automation systems, or have significantly more Internet users than other countries. In terms of cyberterrorism, this country may be less vulnerable than other countries having similar characteristics in terms of those factors, but face a considerable threat from terrorist groups or unfriendly nations.

3 – 5: Vulnerable.

This rating represents the conditions that put a country in a vulnerable position in terms of variables constructing vulnerability. Again, the rating 3 represents different conditions than a rating of 5. A country having a rating of 5 is more vulnerable than a country having a rating of 3. Countries in this category are those who rely heavily on technology. They are economically developed, highly industrialized and have a population with a significant number of Internet users and ISPs. The difference between a rating of 3 and a rating of 5 stems from the following conditions:

Countries having a rating of 3 may have high ratings in terms of the variables, economic development, industrialization, the number of Internet users, ISPs, dependency on technology, dependency on automation, and total amount of money spent on technology, but they may not be facing any threat from any terrorist group or unfriendly nation, or the threat level is not the same. On the other hand, countries having a rating of 5 may face serious threats from terrorist groups or unfriendly nations. The level of threat or the risk factor is determined according to two very important variables: motivation and capability. A terrorist group may have high motivation, but may lack the capacity to execute any attack which puts a country in a vulnerable condition, but not a completely vulnerable condition.

5.5 – 7: Completely vulnerable.

The rating completely vulnerable represents the highest vulnerability in a country. The conditions that construct vulnerability (economic development, industrialization, the number of Internet users, ISPs, dependency on technology, dependency on automation, and total amount of money spent on technology, terrorists' motivation, and terrorists' capability) are significantly higher than other countries; in other words, the level of vulnerability is the highest for those countries. In particular, those countries, facing threat from terrorist groups and unfriendly nations which have high motivation and capability are expected to have the highest vulnerability.

Rating of cooperation. There are 4 levels of rating in cooperation: no cooperation, limited cooperation, cooperation, total integration. The ratings are as follows:

Table 4

Cooperation Ratings

Score	Rating
1	No cooperation
2 – 3	Limited cooperation
4 – 5	Cooperation
6 – 7	Total integration

1: No cooperation.

The designation of "no cooperation" is represented by a rating of 1. Those countries having a rating of 1 lack of the following variables: public and private awareness, cooperation between private sector and law enforcement, existence of a clearly designated agency that is in charge of investigating cyber attacks, multilateral cooperation with other countries, bilateral cooperation with another country, and existence of substantive and procedural laws. A rating of 1 corresponds to the condition in which those variables do not exist.

2 – 3: Limited cooperation.

Limited cooperation covers the rating 2 – 3. This rating represents the condition in which a country enjoys limited cooperation. The country having a rating of 2 – 3 may have the channels for cooperation such as laws or even agreements; however, external factors such as foreign policy issues may hinder any constructive effort to cooperate with other countries. Or a country may have the laws but the agency or agencies that are responsible for enforcing laws may not be sophisticated enough to include the private sector in their efforts toward cyber security. Therefore, cooperation at the national or international level may exist, but it may be limited.

4 – 5: Cooperation.

A rating of 4-5 represents greater cooperation than the previous rating. In this rating, a country having a rating of 4-5 not only has the mechanisms to cooperate, but also exercises cooperation at the national and international level. The country with a rating of 4-5 is assumed to have a designated agency responsible for investigation of cyber attacks, or other information infrastructure related offenses. Also, that agency is involved in activities which bring the private and public sector together. Moreover, that country is assumed to have laws related to cybercrime and/or cyberterrorism. However, the level of cooperation can be limited compared to the 6-7 rating which involves total integration due to factors which will be explored by the research.

6 – 7: Total iIntegration.

A rating 6-7 represents total integration in terms of cooperation between public and private sectors, and with a designated agency that is in charge of investigating cybercrime and/or cyberterrorism. Also, a country having a rating indicative of “Total Integration” is assumed to have multilateral and/or bilateral agreements with other countries to effectively respond to cybercrime and cyberterrorism. Of course, that country has the related laws defining cybercrime or cyberterrorism, which gives authority to law enforcement to investigate those crimes.

Rating freedom. For the freedom rating, the Freedom House Database system[12] of rating was used.

Table 5

Freedom House Freedom Rating

Score	Rating
1.0 – 2.5	Free
3 – 5	Partly Free
5.5 – 7	Not Free

The difference between ratings used for vulnerability and cooperation constructs and freedom constructs is necessary to address. The smaller numbers in vulnerability and cooperation indicates the lower level of vulnerability and cooperation; accordingly, the higher the numbers for ratings in these two constructs, the greater the vulnerability and cooperation. On the other hand, lower numbers in freedom rating indicates more freedom.

[12] Assigning of the status of Free, Partly Free, Not Free—Each pair of political rights and civil liberties ratings is averaged to determine an overall status of “Free,” “Partly Free,” or “Not Free.” Those whose ratings average 1-2.5 are considered Free, 3-5.5 Partly Free, and 5.5-7 Not Free (see Table 3). The dividing line between Partly Free and Not Free falls at 5.5. For example, countries that receive a rating of 6 for political rights and 5 for civil liberties, or a 5 for political rights and a 6 for civil liberties, could be either Partly Free or Not Free. The total number of raw points is the definitive factor that determines the final status. Countries and territories with combined raw scores of 0-33 points are Not Free, 34-67 points are Partly Free, and 68-100 are Free. Survey Methodology (Available at http://www.freedomhouse.org/research/freeworld/2003/methodology.htm) However, the research concerns with the civil liberties.

Based on the ratings explained above, the rating for each country will be determined according to the research findings. As explained before, the seventeen indicators of the scale provide an overview as to what the ratings for each country will be.

Limitations of the Research

The research has several limitations. One of the limitations stems from the fact that the literature does not reveal any agreed upon definition of cyberterrorism. This is not specific to cyberterrorism; in fact, it represents one of the unique problems of responding to terrorism, regardless of the type of terrorism. Nevertheless, the researcher of the study reveals his perspective with respect to the imperative points of different definitions of cyberterrorism in the literature. Secondly, as revealed in chapter 2, academic research is problematic in the area of cyberterrorism. The difficulty emerges from not only obstacles to investigating and prosecuting such crimes due to the nature of the crime itself, but also the unwillingness of the victims of these attacks to report their victimization. In particular, big businesses and governmental agencies do not report attacks which may cause economic losses and/or damage to the prestige of the targets. Also, it is very difficult to accurately identify the number of attacks which are stopped. Therefore, most of the time the data regarding the number of cyber attacks against both the government and the private entities are anecdotal. This may affect the reliability of the data.

Furthermore, another limitation of the research comes from the characteristics of the participants in the survey. The specific expertise of the individuals may affect their responses which may make it difficult to establish a common ground. In addition, since the survey involves experts from different countries, responses may vary from country to country. Every country may have different law enforcement structures, as well as legal systems which may lead to variation among the responses. To increase the validity of the research, the researcher’s initial plan was to include experts from countries where there is very limited amount of Internet use, if not total absence. However, the initial research, for instance, in Sudan revealed that law enforcement agencies do not share the same perspectives on the issues of cybercrime and cyberterrorism.

CHAPTER 4

ANALYSIS

Introduction

The purpose of this chapter is to analyze the results of the research. This chapter also sheds light on two of the most important components of research-- reliability and validity. Therefore, issues of coefficient alpha, external validity and content validity are discussed in detail since the data are used for the first time. Further, factor analysis was conducted through correlation matrix as well as analysis of the results in terms of the relationship between factors and major variables (constructs). In this section, factors identified based on the survey results are defined in detail. After the factor analysis of the major variables, overlaps between cybercrime techniques and cyberterrorism were analyzed to come up with a typology of cyberterrorism.

Reliability and Validity of the Research

Reliability and validity are two of the most important components of research. The next section analyzes reliability and validity of this study.

External Validity

External validity defines the extent to which the result of the research is generalizable. In other words, external validity is concerned with the representativeness of the sampling. In general, it is assumed that larger sample size increases external validity in terms of generalizability. The research sample in this survey involves two groups of people. The first group is academicians, and the second group is practitioners. The following tables illustrate the distribution of the respondents and their areas of expertise.

Table 6

Categories of Respondents in General

Academicians
Law Enforcement
Lawyers
Politicians
Consultants
Other government personnel

Table 7

Categories of Respondents according to their Status as Academicians or Practitioners

ACADEMICIANS	PRACTITIONERS
Information Science	Anti-terrorism
Criminal Justice	Computer Crime Investigation[13] IT Department
Law and Technology	Administrators
Political Science	Anti-Smuggling and Organized Crime Unit
Computer Science	Criminal Investigation

As stated before, a "targeted sampling" method was used in this research. Since random sampling is not used and the respondents are limited to those who have expertise in the subject matter, it can be assumed that the sample has representative power. The sample size is critical for generalizability; however, in researches such as this, the quality of the samples is much more important than the quantity. Since the questions require extensive knowledge, those who do not have the necessary level of

[13] Cybercrime unit is also called High-Tech Crime Unit. In some cases it is also called Information Technologies.

knowledge and expertise cannot contribute to this research. In other words, the researcher maintains the quality of the sample over the quantity.

Academicians

The distribution of the respondents in terms of their academic background represents variety of fields, including criminal justice, political science, information science, computer science, and law. The distribution of the respondents actually reflects one of the foundations of this research. That is, as revealed in chapter 3, there are four types of vulnerability aspects: political, technical, legal, and cultural. The academicians in the survey have both the quality of the expertise and the representativeness in these four areas. Academicians from political science contribute to this research by answering the questions from every aspect, but more importantly, from political aspects. While these people are political science majors, they have published many articles and books about terrorism, cyberterrorism, cybercrime, and other issues on international security. Similarly, respondents from criminal justice have extensive knowledge and background on those issues. Since the technical aspect is a critical component of vulnerability, academicians from computer science and information science reflected their opinions and perspectives in their responses. Also, leading academicians in law from different countries contributed to this research by answering the questions. Among these academicians, there are those who are not only the prominent academicians in their fields, but they are also nationally and internationally recognized scholars.

Practitioners

In addition to the academicians, the practitioners are the second major group of respondents in this research. Practitioners are those who are actually working in the area of terrorism, cybercrime, computer security, and/or other security areas. These respondents either work as investigators, law enforcement personnel in different police agencies and federal law enforcement agencies or work as computer and information security experts in different government institutions and private companies. Practitioners in law enforcement come from different areas. The first group of practitioner respondents is police officers. Depending on the country they are from, they work in local or national police agencies. In particular, they work in anti-terrorism departments, IT departments where they work in the capacity of information security experts or investigators, who deal with computer crime and other related criminal activities. There are also law enforcement people who are working in federal agencies. In short, it is obvious that the variety of respondents, in terms of their backgrounds, gives the researcher the ability to include a quality sample with strong representativeness.

When we explore the characteristics of the countries in the study, there are differences between those countries in terms of economic development, industrialization, etc. While the US, Canada, United Kingdom, and Germany share similar characteristics, Turkey does not share those similarities. While these characteristics will be discussed in the next chapter, it is necessary to reveal that those differences actually enable the researcher to have a comparative analysis, which at the end, increases generalizability of the research. Instead of having countries with similar characteristics, it is important to have a country like Turkey, which has unique characteristics in terms of its vulnerability to terrorism.

Geographic considerations in terms of which country these experts are from is another important aspect of the sample population. In this research, there are two major groups of countries. The first group involves industrialized countries. These are the US, Canada, United Kingdom, and other EU countries. The second group includes Turkey. The number of experts in this study was identified based on their availability and accessibility. On the other hand; however, the researcher thinks that these countries provide good comparativeness in terms of their level of economic development, industrialization, and other aspects. Also, the US and Turkey provide a perfect comparative perspective given the characteristics of these two countries in terms of the vulnerability they have and motivation and capability that terrorist organizations that have targeted these two for decades.

There are also issues that should be discussed in terms of external validity. There are factors that may affect external validity which may also affect the outcome of the research. These factors are: 1) Testing effect, 2) Selection bias, and 3) Reactivity or the awareness of being studied, known as the “Hawthorne effect” (Hagan, 2000, p. 78).

The following section analyzes those factors and their impact on the research. This research involves a survey, not an experiment. Therefore, the above factors may not be as effective as they are in experiments. Yet it may be necessary to explain the possible impact of these factors on this research.

First of all, testing effect involves distributing a research instrument. The members of the sample population answered the survey only once, so the testing effect is not an issue in this research. The second factor that affects external validity is selection bias. This research does not involve random selection, which means the sample is biased; however, the content and nature of the research necessitate using targeted sampling instead of random sampling. Therefore, selection bias can be considered irrelevant. The last factor that affects external validity is reactivity or awareness of being studied the “Hawthorne effect.” This factor generally is an issue in researches which involves experimentation.

In this research, it seems that other than reactivity or awareness of being studied, the background and knowledge of respondents affect their responses, but this is the nature of acquiring responses from experts.

Content Validity

Content validity is concerned with the sampling adequacy of the items in the research instrument (DeVellis 1991). Establishment of content validity involves subjective judgment of the investigator and is usually non-empirical in nature (Hagan 2000).

There are different techniques to evaluate the research in terms of its content validity. The first step is to clearly define the concept, which is a construct in this research. The constructs in this research are vulnerability, law enforcement cooperation, and freedom in given country. These concepts are clearly defined in chapter 3.

The second major step toward content validity of a scale is to identify the components of the concept. This relies heavily on the literature review. In order to adequately identify the components of the constructs, the researcher of this study did extensive research while writing the literature review. Since this scale will be the first in the area of cyberterrorism, the researcher carefully identified the critical components for each of the constructs. Since there are other scale categories, which measure other constructs, the components and concepts of the previous studies, especially in the area of political science and criminal justice, helped the researcher to identify them. Extensive literature review revealed those components. Of course, while the literature review helped the researcher to identify these concepts and components, it was imperative that these components and other necessary concepts were reviewed by the experts.

So the third major step toward identifying and verifying the components of the construct of this study was to submit the items of the survey, which includes the components of the construct, to the panel of experts. The panel of experts were composed of three people who have the expertise, not only in the areas of terrorism, cyberterrorism, and security, but also, more importantly, in the area of academic research. In other words, the experts had the knowledge and experience in developing scales and conducting academic research. First, they reviewed the wording of the items. Secondly, the experts were asked to review the appropriateness and comprehensiveness of the items. Finally, they also determined whether or not the items reflect the research concepts. Based on their responses and recommendations, some items were revised. In addition to panel of experts, during the actual distribution of the survey to the targeted sample, the researcher received positive feedback from a number of respondents who found the items and questions in the survey appropriate and comprehensive. This feedback is also considered an indicator of content validity.

Findings

The sample size of this research is 130 experts from a variety of fields. The number of respondents who actually participated in the survey is 102, and the number of responses considered during the statistical analysis is 98, (N=98). The reason for the difference between the participant numbers is that those who participated in the research, but did not take the survey, participated in the research by telephone interview, and answered some of the questions with in-depth analyses. They did not give answers for each question due to their busy schedule.

It is necessary to state that this study involves exploratory research based on the expert opinions. The analysis of findings in this research is composed of two major sections. The first section presents results of the factor analysis. This section also reveals the results of the research in terms of discussion of factors that were identified as a result of this research.

> If a large number of respondents fail to answer a particular item, then that item should be eliminated from a scale. If the missing item is one of a series of measures of the same basic dimension, we could assign to that item the average score for the items answered… Another alternative to substituting the average score from the items answered is to assign an intermediate score to missing responses (Hagan, 2000, p. 308).

Since the survey responses contained missing data, an average score for the items answered was assigned to the missing responses.

Factor Analysis

The evaluation of the items was done according to their reliability, validity, variances, means, and coefficient alpha. The following section explained these concepts, then reveals the results of the study.

Item means is defined as “a mean close to the center of the range of possible scores” (DeVellis, 1991, p. 83).

Cronbach's alpha is an index of reliability associated with the variation accounted for by the true score of the "underlying construct" (Reynaldo and Santos, 1999) The construct is the hypothetical variable that is being measured (Hatcher, 1994).

Item-Scale Correlation

In this research, a list of scale items was created. As explained in chapter three, the research instrument was a survey with 28 questions. Out of 28 questions, 17 items are extracted to construct a scale. Seventeen items are the indicators of factors which will be parts of the three constructs of this research.

Table 8

Item List of Vulnerability-Comprehensive Cooperation-Freedom with Statistics

Item	Mean	Std. Dev.	*n*
MOTIVATION	4.763	1.8689	98
CAPACITY	4.281	1.4643	98
LEVEL OF ECONOMIC DEVELOPMENT	4.488	1.5365	98
INDUSTRIALIZATION	4.318	1.5075	98
NUMBER OF INTERNET USERS	4.416	1.7866	98
NUMBER OF ISPs	4.165	1.6550	98
DEPENDENCY ON TELECOMMUNICATION	5.033	1.5022	98
DEPENDENCY ON AUTOMATION	4.759	1.4140	98
MONEY SPENT ON TECHNOLOGY	4.115	1.5692	98
LEVEL OF AWARENESS	3.761	1.5949	98

(table continues)

Table 8 *(continued).*

Item	Mean	Std. Dev.	*n*
FREEDOM – CIVIL LIBERTIES	2.632	1.5733	98
LEVEL OF COOPERATION	3.299	1.3483	98
DESIGNATED AGENCY	3.791	1.7440	98
MULTILATERAL AGREEMENTS	3.179	1.4154	98
BILATERAL AGREEMENTS	3.373	1.4833	98
SUBSTANTIVE LAWS	3.134	1.3452	98
PROCEDURAL LAWS	3.372	1.3851	98

Computation and other statistical analyses were executed through use of SPSS statistical analysis program.

Item-scale correlation was determined based on the analysis of the “Correlation Matrix” table. For this analysis SPSS statistics software program was used. As shown in the correlation matrix analysis (See APPENDIX B: Correlation Matrix of the Items of a Scale- VCF)), there is no multi-collinearity problem. Items are highly related to each other.

Item mean values and coefficient alpha values are shown in the following table.

Table 9

Item Means and Variance Summary Item Statistics

Mean	Min	Max	Range	Max/ Min	Var	# of Items
3.934	2.632	5.033	2.402	1.913	.466	17

The covariance matrix is calculated and used in the analysis. The reliability of this research, as shown in the table, is an acceptable value.

Table 10

Scale Statistics

Mean	Var	Std. Dev.	# of Items
66.878	139.832	11.8250	17

Table 11

Coefficient Alpha Values for Each Item

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	# of Items
.753	.754	17

In addition to SPSS statistical analysis program, LISREL, a software product, was used to do factor analysis. LISREL uses the correlations or covariance among measured variables such as survey items to estimate or infer the values of factor loadings, variances, and errors of latent (unobserved) variables (LISREL 1998).

Analysis was done according to the three major variables, constructs of the research. The freedom variable was constructed based on the Freedom Data Base. For analysis purposes, freedom is considered a separate factor loading the Freedom scale.

Seventeen items were used to do the factor analysis, for which the SPSS and LISREL programs were used. Analysis shows that seventeen items are loaded to 6 factors (See Appendix C Rotated Component Matrix- VCF).

The factors and the indicators loading to these factors are listed as follows:

Construct I – Vulnerability Construct

Factor 1
Level of economic development
Level of industrialization

Factor 2
The number of Internet users
The number of ISPs

Dependency on Automation
The total amount of money spent on technology
Motivation
Capacity

Construct II – Comprehensive Cooperation:

Factor 3
Designated Agency
Level of cooperation between law enforcement and private sector
Awareness

Factor 4
Bilateral cooperation
Multilateral cooperation

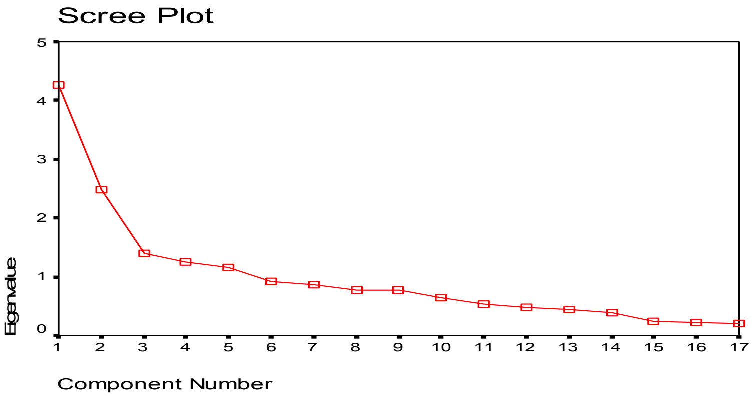
Factor 5
Substantive laws
Procedural laws

Construct III – Freedom

Factor 6
Freedom (Civil liberties)

While the above list reflects the outcome of actual the factor analysis, the author of this research also previously prepared anticipated item groupings which is presented in the following illustration. The examination of the anticipated item grouping showed that in terms of factors under each construct, the factor analysis confirms the theoretical factor structures.

Figure 3. Scree plot vulnerability- comprehensive cooperation- freedom scale.

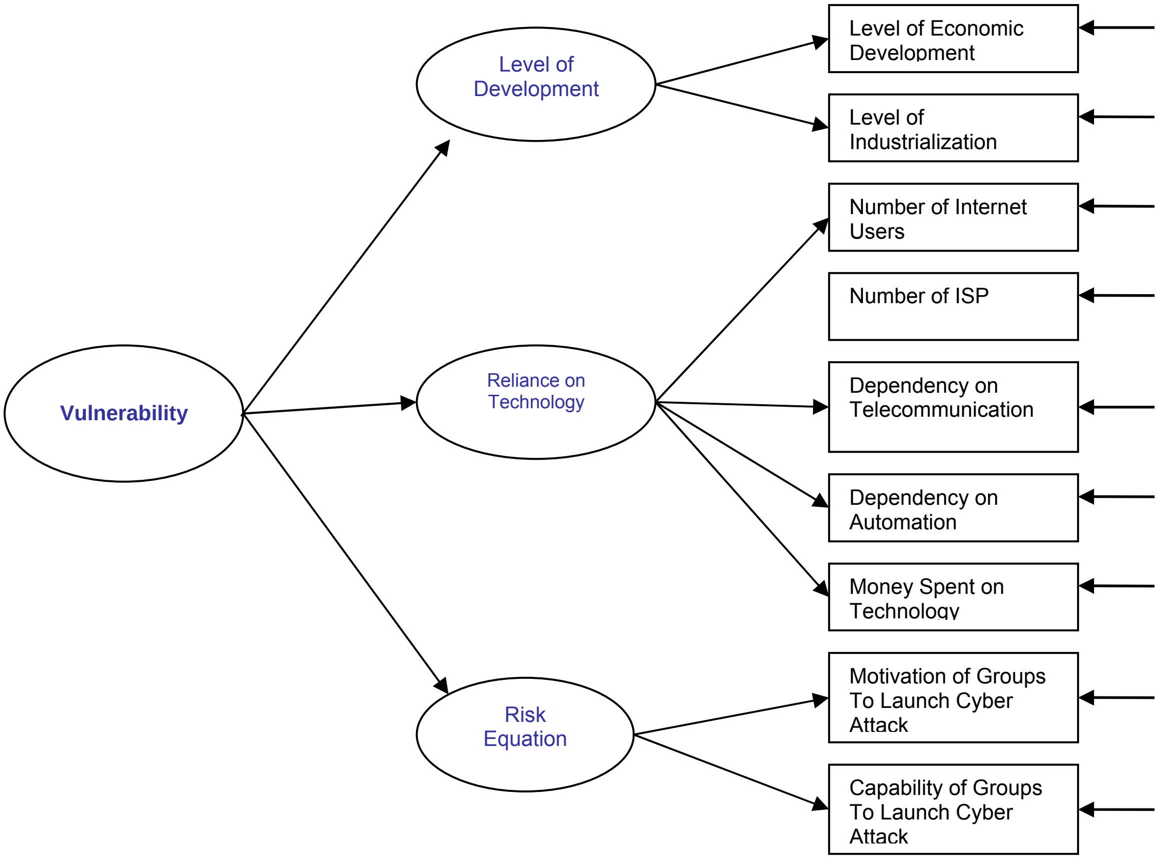


To extract the factor loadings, principal component analysis with rotation method involving Varimax with Kaiser normalization is used. The following section includes the illustration of the factor analysis and the modifications carried out by the researcher along with the explanation.

Construct I – Vulnerabilty

As shown in the Figure 3, nine items out of 17 in the scale load to 3 factors, constructing vulnerability. These three factors are level of development, reliance on technology, and risk equation.

Figure 4. Indicators-factors constructing vulnerability scale.


Vulnerability
Level of Development
Reliance on Technology
Risk Equation
Level of Economic Development
Level of Industrialization
Number of Internet Users
Number of ISP
Dependency on Telecommunication
Dependency on Automation
Money Spent on Technology
Motivation of Groups To Launch Cyber Attack
Capability of Groups To Launch Cyber Attack

Factor 1 – Level of Development

The indicators “level of economic development” and “level of industrialization” load to the “level of development” factor.

This factor includes “level of economic development” and ‘level of industrialization.” While there are a variety of indicators for both economic development and industrialization, in this research, GDP is used for economic development, and level of electricity consumption per kWh is used to determine the level of industrialization.

Factor 2 – Reliance on Technology (initial)

Factor analysis showed that number of Internet users in a given country, the number of ISPs, level of dependency on technology, level of dependency on automation, total amount of money spent on technology, terrorists’ motivation, and capacity to launch cyber attack load to factor 2. However, the qualitative analysis of the expert responses showed that the experts might have been tempted by a target-rich environment, not the motivation results from factors including target richness, and more importantly, political and socio-economic conditions. The qualitative analysis of the expert responses also confirmed that some of the experts answered motivation questions based on the level of reliance on technology the target country has, while the majority of the experts considered issues such as foreign policy decisions, being the super-power in the world, and other political, socio-economic characteristics of the target country as the source of motivation. Also, experts consider motivation and capability as one of the most important factors to determine the level of vulnerability. Therefore, I consider these two items as separate factors, and since they will be under the vulnerability construct, this may be considered as a minor modification. This also enables the researcher to focus on a more comprehensive motivation than target richness. Therefore, factor 2 was separated into two factors; reliance on technology and risk equation. The following section explains these two factors.

Factor 2 – Reliance on Technology (revised)

The indicators, “number of Internet users in a given country,” “the number of ISPs,” “level of dependency on technology,” “level of dependency on automation,” and “total amount of money spent on technology” load to a level of “reliance on technology” factor. “Reliance on technology” refers to the extent to which a country depends on technology; In other words, the factor explains the level of technology on which daily affairs of individuals in a given country, as well as public and private organizations, institutions, and infrastructures rely.

Factor 3 – Risk Equation

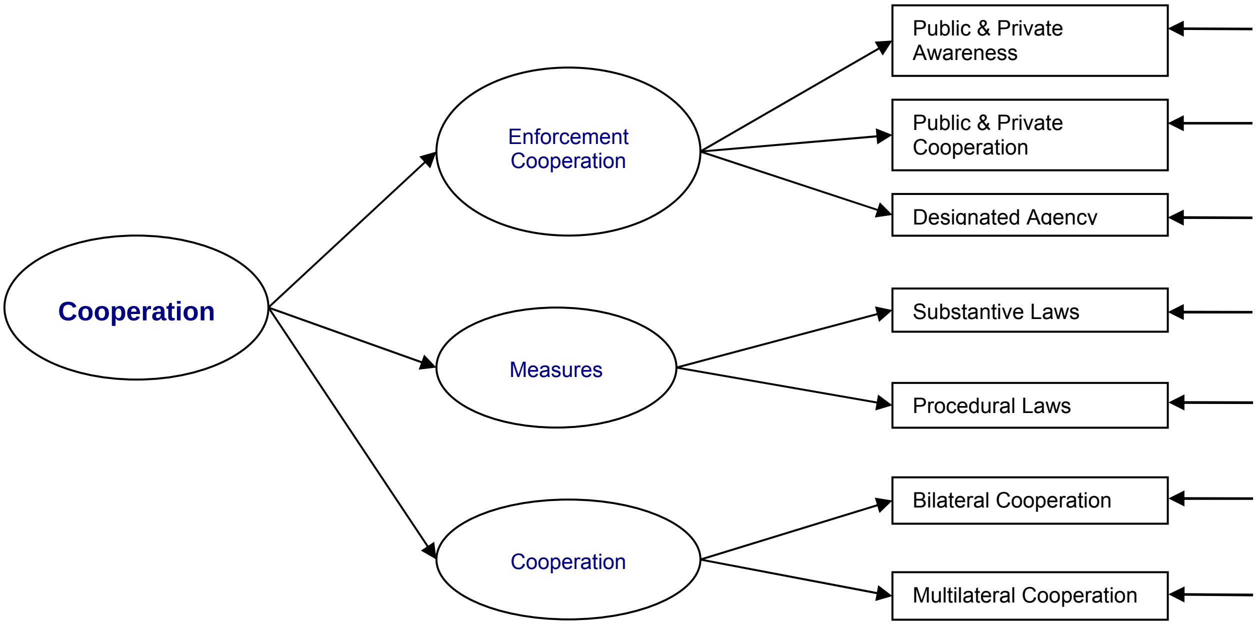
The indicators, motivation of terrorists and unfriendly nations to launch cyber attacks and their level of capability to execute such attacks load to the risk equation factor. The risk equation refers to the extent to which any terrorist organization, unfriendly nations, or individual/groups have the capability and motivation to launch a cyber attack.

As shown in the Illustration 4, the second major variable, cooperation, in the vulnerability-cooperation-freedom scale is constructed by three factors: law enforcement cooperation, legal measures, and international cooperation.

Construct II – Comprehensive Cooperation

The cooperation construct is composed of three factors according to the factor analysis; factor 4, which consists of cooperation between law enforcement agencies and the private sector, level of awareness against the existence of the threat and risk of cyber attacks, and existence of a designated law enforcement agency; factor five, which consists of bilateral agreements, and multilateral agreements; and factor six, which consists of the existence of substantive and procedural laws.

Figure 5. Indicators-factors constructing cooperation scale.



Factor 4 – Law Enforcement Cooperation

The indicators “public and private awareness,” “cooperation between law enforcement agencies and private sector,” and “existence of a designated law enforcement agency” load to the law enforcement cooperation factor.

The law enforcement cooperation factor refers to the degree to which law enforcement agencies in a country engage in activities and programs, through which cooperation between local/federal/or national law enforcement agencies and other public security institutions and the private sector engage in cooperative efforts to respond to and/or to deter a cyber attack or criminal incident related to cyberspace or computers.

Factor 5 – Legal Measures

The indicators of legal measures are existence of “substantive laws” and “procedural laws.”

Legal measures refers to the extent to which a country has substantive and procedural laws amended to criminalize attacks and/or use of computers to commit cybercrime or cyberterrorism, resulting in physical or emotional damage, as well as fear within the society.

Factor 6 – International Cooperation

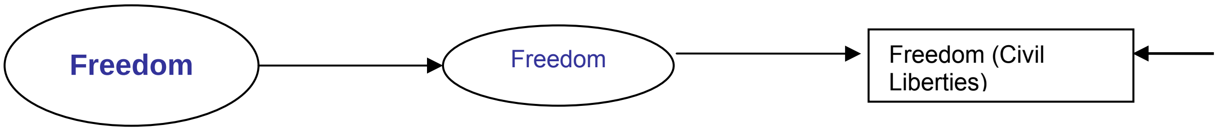
The indicators of international cooperation are “bilateral cooperation” and “multilateral cooperation.”

International Cooperation refers to any bilateral or multilateral agreements made and/or ratified by a country to facilitate cooperation with another country or international/supranational organization to respond to crime involving cybercrime and cyberterrorism.

Construct III – Freedom

Since freedom construct is taken from the Freedom House database, the freedom factor is put here in order to indicate that freedom is one of the factors, constructing the freedom scale. When it is included in the factor analysis, it actually loads as a separate factor; therefore, it will be considered as the seventh factor.

Figure 6. Indicators-factors constructing freedom scale.



Factor 7 – Freedom (Civil liberties)

The freedom factor is defined as the major construct, which consist civil liberties including, but not limited to "the freedom to develop opinions, institutions, and personal autonomy without interference from the state. In particular, civil liberties include freedom of expression and belief, rule of law, personal autonomy and individual rights (Freedom House Inc., 2003).

As stated before, the analysis of the research findings also involves an exploratory analysis of the relationship between three major constructs. To do this the LISREL software program was used. LISREL analysis also revealed the following (See Appendix D: The Vulnerability-Comprehensive Cooperation-Freedom Scale);

- The results of structural equation model (SEM) are presented in Figure 1. All coefficients in the model are standardized. Additionally, the significance level of each path is shown in Figure 1. Our model shows that all of the indicators significantly predict the constructs.

- Level of development (β = .41), Level of technology (β = .60), and Risk equation (β = .40) significantly predicts vulnerability.

- Law enforcement cooperation (β = .40), Legal measures (β = .57), and International cooperation (β = .08) predicts comprehensive cooperation.
- Freedom also significantly predicts the Freedom construct.
- Of more importance, however, are reciprocal paths linking vulnerability, cooperation, and freedom.

Table 12

Reciprocal Path Matrix for Vulnerability, Cooperation, and Freedom

	Vulnerability	Cooperation	Freedom
Vulnerability	1.00		
Cooperation	0.30	1.00	
Freedom	-0.39	-0.48	1.00

- As presented in the correlation matrix, each of these constructs has a moderately strong relationship with each other.
- The table shows that there is a positive relationship between vulnerability and cooperation. In other words, higher vulnerability requires a higher level of cooperation.
- However, freedom has a negative relationship with vulnerability and cooperation.

As the level of freedom increases, the level of vulnerability increases. In other words, countries that are designated as free (based on the research results and the Freedom House database) also have increased levels of vulnerability. Notice that the relationship in this statement seems to explain a positive relationship between vulnerability and freedom. However, as explained in chapter 3, the numerical value for the freedom rating is different than vulnerability and cooperation. For example, in the US, the scale rating for vulnerability is 4 while the scale rating for freedom is 2 in the expert scale, which means higher value increases vulnerability. On the other hand, the lower the value of the rating, the more free a country is. Therefore the relationship between freedom and vulnerability is negative. The relationship between freedom and cooperation is also negative, which means the lower the rating of freedom, the greater likelihood that a country will need cooperation with other countries, as well as domestic cooperation incorporating public and private sectors.

Vulnerability-Comprehensive Cooperation-Freedom Ratings for Countries

The values of the scale variables (vulnerability, comprehensive cooperation, and freedom) of each country are extracted from research results. To determine their values, mean scores for indicators which load to a particular factor are calculated. The average value of the mean scores for the factors determines the mean value for each of the constructs--vulnerability-cooperation-freedom.

Rating for the Developed Countries

Table 13

Mean Scores of 9 Items & Average Mean of Vulnerability for Developed Countries

	Mean	Std. Dev.	N
MOTIVATION	5.453	1.8328	47
CAPABILITY	4.349	1.4720	47
ECONOMIC DEV	4.606	1.7722	47
INDUSTRIALIZATION	4.395	1.7455	47
NUMBER OF INTERNET USERS	4.644	1.8885	47
NUMBER OF ISP	4.588	1.7987	47
DEPENDENCY ON TELECOMMUNICATION	5.512	1.5441	47
DEPENDENCY ON AUTOMATION	5.351	1.4394	47
MONEY SPENT ON TECH	4.326	1.5745	47

Table 14

Mean Scores of 7 Items & Average Mean of Comprehensive Cooperation Variable for Developed Countries

	Mean	Std. Dev.	N
PUBLIC AND PRIVATE AWARENESS	4.049	1.4223	47
PUBLIC AND PRIVATE COOPERATION	3.815	1.1120	47
DESIGNATED AGENCY	4.361	1.6023	47
MULTILATERAL COOPERATION	3.106	1.1687	47
BILATERAL COOPERATION	3.274	1.1637	47
SUBSTANTIVE LAWS	3.457	1.1646	47
PROCEDURAL LAWS	3.758	1.2938	47

	Mean	Min	Max	Range	Max/Min	Var	# of Items
Item Means	3.688	3.106	4.361	1.255	1.404	.195	7

Table 15

Mean Scores of 1 Item & Average Mean of Freedom Variable for Developed Countries

	Mean	Std. Dev	# of Items	N
FREEDOM	2	1.161	1	47

Table 16

Average Rating of Vulnerability-Cooperation-Freedom According to Experts for Developed Countries

Scale Variables	Rating Values
Vulnerability	4.8
Cooperation	3.7
Freedom (Freedom House Data Base)	2

Based on the rating system proposed by this research, developed countries are rated thus:

The vulnerability rating for the developed countries is 4.8, which falls into the rating of vulnerable. The cooperation rating is 3.7, which falls into the rating of limited cooperation, but very close to the rating of cooperation.

The freedom average value is 2, and a rating of 2 falls into the category of “Free” according to the Freedom House database. This result, itself, can be considered a sign of validity of this research because the freedom ratings for the developed countries in this research are “Free” too.

Rating for Turkey.

Based on the expert responses, the ratings for Turkey are as follows.

Table 17

Mean Scores of 9 Items & Average Mean of Vulnerability for Turkey

	Mean	Std. Dev.	N
MOTIVATION	4.128	1.6813	51
CAPABILITY	4.218	1.4689	51
ECONOMIC DEV	4.380	1.2905	51
INDUSTRIALIZATION	4.246	1.2627	51
NUMBER OF INTERNET USERS	4.206	1.6786	51
NUMBER OF ISP	3.774	1.4188	51
DEPENDENCY ON TELECOMMUNICATION	4.592	1.3306	51
DEPENDENCY ON AUTOMATION	4.212	1.1566	51
MONEY SPENT ON TECH	3.920	1.5542	51

Table 18

Mean Scores of 7 Items & Average Mean of Cooperation Variable for Turkey

	Mean	Std. Dev.	N
PUBLIC AND PRIVATE AWARENESS	3.496	1.7100	51
PUBLIC AND PRIVATE COOPERATION	2.824	1.3814	51
DESIGNATED AGENCY	3.266	1.7183	51
MULTILATERAL COOPERATION	3.246	1.6187	51
BILATERAL COOPERATION	3.466	1.7333	51
SUBSTANTIVE LAWS	2.837	1.4403	51
PROCEDURAL LAWS	3.017	1.3833	51

Table 19

Mean Scores of 1Item & Average Mean of Freedom Variable for Turkey

	Mean	Std. Dev.	# of Items	N
FREEDOM	3.2	1.685	1	51

Table 20

Average Rating of Vulnerability-Cooperation-Freedom for Turkey

Scale Variables	Rating Values
Vulnerability	4.186
Cooperation	3.164
Freedom	3.21

Based on the rating system proposed by this research, the ratings for Turkey are as follows:

The vulnerability rating for the developed countries is 4.2, which falls into the rating of Vulnerable.

The cooperation rating is 3.1, which falls into the rating of limited cooperation.

The freedom average value is 3, and a rating of 3 falls into the category of "Partly Free," according to the Freedom House Database. This result, itself, can be considered a sign of validity of this research since the rating for Turkey is also 3.

Rating for United States.

Table 21

Mean Scores of 9 Items & Average Mean of Vulnerability for the US

	Mean	Std. Dev.	N
MOTIVATION	6.349	1.0160	33
CAPABILITY	4.398	1.4042	33
ECONOMIC DEV	4.772	1.7772	33
INDUSTRIALIZATION	4.654	1.6619	33
NUMBER OF INTERNET USERS	4.874	1.8299	33
NUMBER OF ISP	4.803	1.7393	33
DEPENDENCY ON TELECOMMUNICATION	5.577	1.5209	33
DEPENDENCY ON AUTOMATION	5.568	1.3964	33
MONEY SPENT ON TECH	4.519	1.4592	33

Table 22

Mean Scores of 7Items & Average Mean of Cooperation Variable for the US

	Mean	Std. Dev.	N
PUBLIC AND PRIVATE AWARENESS	4.099	1.4774	33
PUBLIC AND PRIVATE COOPERATION	3.788	1.1390	33
DESIGNATED AGENCY	4.247	1.4701	33
MULTILATERAL COOPERATION	2.911	1.0887	33
BILATERAL COOPERATION	3.121	1.0845	33
SUBSTANTIVE LAWS	3.418	1.2162	33
PROCEDURAL LAWS	3.822	1.4157	33

Table 23

Mean Scores of 1Item & Average Mean of Freedom Variable for the US

	Mean	Std. Dev.	# of Items	N
FREEDOM	2.1	1.277	1	33

Table 24

Average Rating of Vulnerability-Cooperation-Freedom for the United States

Scale Variables	Research Value
Vulnerability	5.057
Cooperation	3.630
Freedom	2.152

Based on the rating system proposed by this research, the United States is rated thus: The vulnerability rating for the developed countries is 5.5, which falls into the rating for vulnerable. However, the rating category is higher than other developed countries. The cooperation rating is 3.6, which falls into the rating of limited cooperation, but very close to the rating of cooperation.

The freedom average value is 2, which falls into the category of “Free” according to the Freedom House Database. This result itself can be considered a sign of validity of this research because the freedom ratings for the developed countries in this research are “Free” too. The experts also provided explanations for their responses. The qualitative analyses of these responses along with the discussion of the findings above were analyzed in the fifth chapter.

Analysis of the Overlaps between Cybercrime Techniques and Cyberterrorism

This section involves the analysis of the association between cybercrime techniques and cyberterrorism, which led to the typology of cyberterrorism.

Table 25

Item Means – Variance Summary Item Statistics and Coefficient Alpha Values (Cyberterrorism Typology)

	Mean	Min	Max	Range	Max/Min	Var	# of Items
Item Means	5.052	3.410	5.845	2.435	1.714	.2574	17

The covariance matrix is calculated and used in the analysis.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	# of Items
.9185	.9198	17

Item-scale correlation is determined based on the analysis of “Correlation Matrix” table. For such analysis SPSS statistics software program is used. As shown in the correlation matrix analysis (Appendix E: The Correlation Matrix for Cybercrime and Cyberterrorism Overlaps), there is no multi-collinearity problem.

Also, in terms of the total variance explained, Factor 1 explains 41%, Factor 2 explains 13.4%, and Factor 3 explains 10.4% of the variance. In other words, three factors explain the total variance of 65%.

Table 26

Descriptive Statistics of Overlaps between Cybercrime Techniques and Cyberterrorism

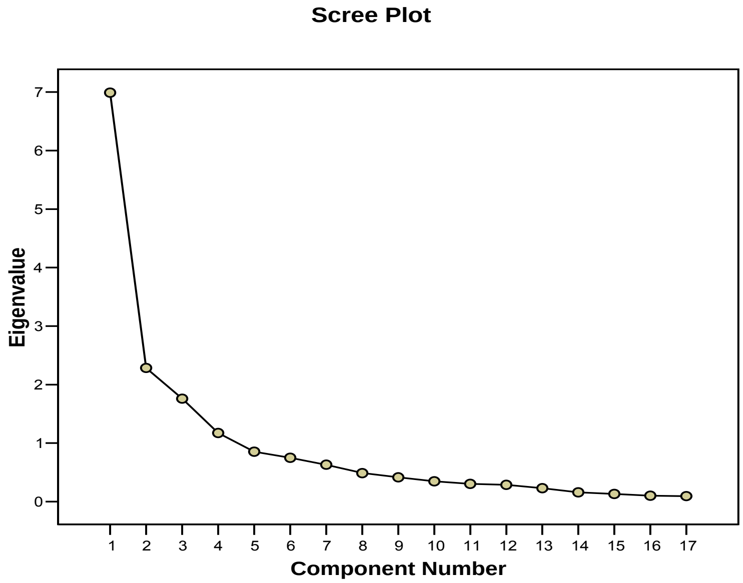
Variable	Mean	Std. Dev.	# of Cases
UNAUTHORIZED ACCESS	5.1977	1.7040	98.0
TAMPERING DATA	5.3258	1.6358	98.0
ESPIONAGE	5.8452	1.3584	98.0

(table continues)

Table 26 *(continued).*

Variable	Mean	Std. Dev.	# of Cases
PRIVACY	4.6136	1.9073	98.0
VIRUS	5.3750	1.6392	98.0
TROJAN	5.3117	1.5078	98.0
WORMS	5.1829	1.6126	98.0
DENIAL OF SERVICE ATTACK	5.0988	1.7207	98.0
MONEY LAUNDERING	5.0465	1.6616	98.0
FRAUD	4.7416	1.8306	98.0
IDTHEFT	5.0989	1.7764	98.0
FORGERY	4.8295	1.7599	98.0
CHLDPORNOGRAPHY	3.4103	1.9073	98.0
COMMUNICATION	5.1573	1.8495	98.0
PROPAGANDA	5.4382	1.7525	98.0
FUND RAISING	5.0909	1.6661	98.0
RECRUITMENT	5.1163	1.7076	98.0

Figure 7. Scree plot of the association between cybercrime techniques and cyberterrorism.



To extract the factor loadings, principal component analysis with rotation method involving Varimax with Kaiser normalization is used. Based on the rotated component matrix analysis of the association between cybercrime techniques and cyberterrorism, there are three major typologies. The loadings are actually confirmatory in nature since they reflect the literature. The exception to the literature is that in the literature, generally, there are more than three groups. As shown in the Appendix F: The Rotated Component Matrix of Overlaps Between Cybercrime Techniques and Cyberterrorism, 17 items list of cybercrime techniques load to 3 different factors. The following section explains each of them in detail.

Typology 1: Disruptive and Destructive Information Attacks

Factor 1: Disruptive and destructive information attacks with communality values of the items.

Unauthorized Access	.600
Tampering Data	.741
Virus	.724
Trojan	.738
Worms	.673
Denial of Service Attack	.636

The indicators--unauthorized access, tampering data, espionage, virus, Trojan horses, worms, denial of service attacks load to disruptive and destructive information attacks. It appears that all of the indicators except for the indicator “espionage” seem relevant to the same category. The indicator, espionage loads to Factor 1 with .548 while it loads to factor 3 with .396. The expectation of the researcher was to see espionage in Factor 2.

Typology 2: Facilitation of Technology to Support the Ideology

Factor 2: Facilitation of technology to support the ideology with communality values of the items.

Money Laundering	.596
Espionage	.771
Fraud	.777
ID Theft	.629
Forgery	.842
Privacy	.671

The indicators--money laundering, fraud, ID theft, forgery, and child pornography, and privacy intrusion load to Factor 2, the facilitation of technology to support the ideology of the terrorist organization. Except for child pornography, which loads to factor 2 with .759, the justification of the other indicators is not problematic. It is not clear that child pornography has ever been used by terrorists. Also, the average mean value of this indicator was the lowest among others. Therefore, the author of the study decided to exclude that indicator from the list of the indicators. The indicator, espionage initially loaded to factor 1. While that is understandable, to avoid any confusion for the future research, the author of this study decided to include espionage within the factor 2. Since espionage can be used to blackmail or to acquire finance from related parties which may have vested interest in the issue of espionage, it will enable researchers to focus on the item espionage along with privacy intrusion and others. The indicators--money laundering, fraud, ID theft, and forgery are required computer and other telecommunication techniques or the awareness of the benefits. The purpose of using these techniques is to either pursue financial resources to support the infrastructure of the organization or to make an ideological statement. As discussed earlier, cyberterrorism can be used as force multiplier. ID theft and privacy intrusion can be used for many purposes. Privacy intrusion means “the acquisition or use of personal data”. ID theft and privacy intrusion can be used to identify the whereabouts of a targeted individual or to intimidate the individual or group, and more importantly, ID theft can be used for other purposes. Personal information can be used to commit other crimes by accessing the Internet with that ID. Also, personal information can be used to intimidate or to blackmail the person.

Typology 3: C-F-R-P (Communication, Fund raising, Recruitment, Propaganda)

Factor 3: C-F-R-P with communality values of the items.

Communication	.734
Propaganda	.805
Fund Raising	.772
Recruitment	.805

The factor actually represents the names of the indicators; in other words, the indicators of the C-F-R-P factor are loaded by the indicators Communication, Fund raising, Recruitment, and Propaganda. The indicator fund raising seems to need an explanation since may be perceived to be similar to Factor 2; however, the indicator loads to Factor 3 with .851 therefore it is considered under Factor 3 instead of Factor 2.

Summary

Based on the survey results, factors constructing 3 major variables of the research--vulnerability-comprehensive cooperation-freedom were identified. The exploratory research findings also revealed that there is a positive relationship between vulnerability and comprehensive cooperation, while the relationship between freedom and vulnerability and freedom and comprehensive cooperation is negative.

Also, the analysis revealed that there are three categories of cyberterrorism based on expert opinions. These three categories are Typology 1: Disruptive and destructive information attacks, Typology 2: Facilitation of technology to support ideology, and Typology 3: C-F-R-P (Communication, Fund raising, Recruitment, Propaganda). The typology analysis has shown there to be overlaps between cybercrime techniques and cyberterrorism.

In sum, the research analysis revealed critical results based on expert opinions. This chapter analyzed and discussed both the qualitative and quantitative findings of this study.

CHAPTER 5

CONCLUSION

Introduction

This chapter reveals the final analysis of the research. It also presents a discussion about the findings of the research. Future research possibilities and what could have been done differently are also discussed. Finally, a conclusion will be presented.

Analysis of the Findings

First, it is necessary to state that the results of the research, and consequently, the analysis of it involve an exploratory research based on expert opinions. In other words, the results are not mathematically conclusive, yet the research analysis reveals invaluable results based on expert opinions.

Analysis of the findings consists of two main sections. The first section focuses on the analysis of statistical results. This section also states the factorial analysis in terms of the validity. Finally, this section involves analysis of the cyberterrorism typology. The second section focuses on the qualitative analysis of the responses from the experts.

The research is based on the expert responses from several countries as well as an in-depth analysis of the literature. Therefore, this section analyzes the research findings in combination with the responses from the experts.

Analysis of Statistical Results

Statistical analysis showed that the research fulfilled the requirements of reliability. The Cronbach's alpha value is .753, which is a reasonably good rating. The reliability and validity issues are explained in detail in the fourth chapter.

As illustrated in Chapter four, I presented anticipated item groupings, in other words, anticipated factors constructing major variables. The initial factor analysis involved 5 factors, excluding freedom. One of the factors loading to the vulnerability construct consists of the number of Internet Users in a given country, the number of ISPs, level of dependency on technology, level of dependency on automation, total amount of money spent on technology, terrorists' motivation, and capacity to launch cyber attack load to Factor 2. The anticipated grouping actually considered motivation and capability as the items loading to a separate factor. In fact, the modified factor analysis reflects this. In sum, factor analytic results based on the statistical analysis are consistent with these anticipated groupings, which could be considered as evidence for factorial validity. The anticipated groupings have been determined based on the in-depth literature review. The qualitative analysis of the expert responses also supported the anticipated groupings. In other words, as the researcher, I explicated the expected factor structure, and the comparison of the statistical factor analysis revealed that the results are confirmatory.

Based on the survey results, seven factors constructing the major variables of the vulnerability-comprehensive cooperation-freedom scale are identified. These factors are presented to the literature as a result of the research. These factors are: level of development, risk equation, reliance on technology, law enforcement cooperation, legal measures, international cooperation, and freedom.

The table shows the problem is that cyber attack can be carried out from a country with limited technical capabilities, and unless that country is willing to engage in some type of agreement, it will be very difficult to present a case to that country. Similarly, lack of legal measures in a country will also hamper the prosecution of an individual or a group on the basis of committing cybercrime or cyberterrorism, since the specific cyber attack is not criminalized in that country.

However, freedom has a negative relationship with vulnerability and comprehensive cooperation. As the level of freedom increases, the level of vulnerability also increases. Also the relationship between freedom and cooperation is negative, which means, the lower the rating of freedom, the greater likelihood that a country will need cooperation with other countries, as well as domestic cooperation incorporating public and private sectors.

The second statistical analysis involved identifying a typology of cyberterrorism by looking at the responses to the question asking about the association of cybercrime techniques and cyberterrorism. In other words, the question is asking whether or not individual cybercrime techniques can be used by terrorists to launch an attack. Responses showed a high level of variance. Three major groups of cyberterrorism typology were identified. These are disruptive and destructive information attacks, facilitation of technology to support the ideological cause, and C-F-R-P, which is communication, fund raising, recruitment, and propaganda.

Qualitative Analysis of the Responses

As revealed before, there are three major variables of this research, which construct the scale. In terms of the relationship between the indicators and factors, expert responses provided invaluable insight. Experts could answer the questions just by rating the questions. In addition, they could provide explanatory answers to the questions. Some of the experts provided in-depth analysis in their answers.

Vulnerability

The research has shown that vulnerability is a very critical concept with respect to cybercrime and cyberterrorism. In terms of how vulnerable the countries in this research are, there are very useful and intriguing responses from the experts. Professor Dorothy Denning, who is a prominent and well-known expert in the area of cyberterrorism and information warfare in the US clarifies the issue of vulnerability and reliance on information technology. She presents a very useful analogy by saying the following:

> one cannot be vulnerable to a cyber attack unless one is using IT, so vulnerability requires some reliance on IT. But one can imagine a company like Amazon that is 100% reliant on the Web for its business vs. a small bookstore that is only 2% reliant on the Web (most of its business coming from local, walk-in customers). We can't conclude that Amazon is more vulnerable because it could put much more care into protecting its Web server than the small bookstore. Perhaps what can be said is that the potential consequences of a cyber attack increase with IT reliance, so cyber security becomes more important (Survey conversation through telephone and email with Dorothy Denning, Ph.D.)

She also emphasized that a country can rely on information technologies, but what is important is the "implementation of security measures and other steps taken to ensure security of the systems. Having said that, high reliance on technology may put a country into a risky position, but proper implementation of security measures can reduce the vulnerability.

The next section reveals the responses of the experts regarding the factors and indicators and their relation with the constructs.

Level of development factor. Level of economic development and industrialization are two indicators of the level of development factor.

- Level of economic development and vulnerability

One expert asserted that there is an inevitable relationship between the level of economic development and vulnerability. He claimed that "high levels of economic development depend upon a complex and huge set of infrastructures which are vulnerable. However, he also indicated that the very complexity of the systems probably mitigates against a major system failure as a result of single point attacks." Another expert presents an explanation about the relationship between level of economic development and vulnerability by saying "Any society that places a high level of reliance on any one technology/way of doing business will be at an increased risk of attack in that particular area. Regarding this, another expert stated that "factors other than economic development play a role in our being the prime target of terrorists and unfriendly nations, but I think economic development is an essential aspect of that phenomenon."

Another expert explains the relationship between being a developed country and vulnerability by stating that, "what makes the US powerful and prosperous also makes the US vulnerable. This statement actually summarizes why some countries are more vulnerable than others. The US is the dominant power in the world; accordingly, the policies of this country create impact in different regions, in particular, in hot areas, such as the Middle East. Therefore, foreign policy decisions may have a direct impact on the vulnerability of the US in addition to its reliance on information technologies.

Furthermore, another expert explains the relationships among being economically developed and technology being used by that country and vulnerability. According to him, “being an economically developed country requires using stronger concentration on integrated, sometimes cross-border solutions which will lead to a stronger use of available networks (i.e. Internet) and hence, to a higher vulnerability to cyber attacks in general.”

Conversely, another expert claimed that most of the other infrastructures are either pretty safe / decentralized or have a real-world fallback option which decreases the risk of cyber attacks.

- Level of industrialization and vulnerability

One of the experts posited that when it comes to level of industrialization and vulnerability, the relationship between the level of industrialization and vulnerability is less related than the relationship between the level of economic development and vulnerability “because industrial sites are generally stand-alone in terms of their electronic systems.

There are interconnections but these tend to be more about moving data that is less time-sensitive than that in the economic world”. Similarly, another expert stated that “If “industrialization” refers to the manufacturing industry, there are only few relations to cyberspace, and they mostly have fallback options." These responses provide an understanding as to what kind of explanatory power industrialization has in terms of explaining vulnerability. While industrialization may not be a sole source of vulnerability, a high level of industrialization today is another indication of an economically developed country. Therefore, while industrialization may not explain vulnerability as comprehensively as the level of economic development does, it can be an indicator.

This explanation by the expert can also be used as an assertion against the idea that factories and other industrial entities are under the threat of cyberterrorism.

Reliance on technology. The indicators, "number of Internet Users in a given country," "the number of ISPs," "level of dependency on technology," "level of dependency on automation," and "amount of money spent on technology" load to a level of reliance on technology factor.

- Number of Internet users and vulnerability

The relationship between the number of Internet users and vulnerability stems from the fact that cyber attack, whether it is carried out by ordinary criminals or terrorists, aims at harming individuals. Moreover, another expert affirms that "a high number of internet users globally mean a high number of potential victims, respectively attackers."

Another expert from the US asserted that "there is a clear relationship between the number of Internet users and our vulnerability to cyber attacks, if only because the increased number." However, in some cases, a lower number of Internet users may not mean that the country will be equally less vulnerable. According to one expert from

Turkey, while the PC users in Turkey is 4 % of the general population, since the reliance on computer technology by the public and government institutions is well above the average population, the level of vulnerability could be higher than expected. This actually explains why the level of vulnerability for Turkey is higher than expected. Even though the level of reliance in Turkey is lower than developed countries, the vulnerability level is similar. The above explanation about the difference between public institutions and the private sector clarifies why Turkey has a higher score in the vulnerability rating.

- The number of ISPs and vulnerability

The relationship between the number of ISPs and vulnerability is not as significant as the relationship between the number of Internet users and vulnerability, according to some experts. They stated that the fewer number of attacks could be enough to take out key nodes if the number of ISPs is smaller. In other words, a high number of ISPs may increase the complexity which decreases vulnerability.

- Dependency on telecommunication and vulnerability

When explaining the relationship between dependency on telecommunication and vulnerability, an expert from the US stated that there is “a clear relationship between our dependency on telecommunication services and our vulnerability to cyber attacks. If nothing else, the fact that we depend on telecommunication services makes them an attractive target for terrorist and other antagonistic groups.”

While dependency on telecommunication is a major source of vulnerability for the US, an expert from Turkey claims that Turkey’s infrastructure is vulnerable to cyber attacks, but since dependency is quite low, this makes Turkey more secure than it is. Accordingly, another expert states that Turkey has not developed e-government applications which is an indication of the level of development in terms of information technologies. So there is a dilemma here. In one case the vulnerability stems from higher reliance on telecommunication, in another case vulnerability may exist but can be lower due to lower dependency. In other words, security measures in Turkey are not adequate; rather they have not been targeted yet, since it may be because the expected outcome is lower from such an attack.

- Dependency on automated systems and vulnerability

One expert claims that most infrastructures rely on automated systems are either closed or highly decentralized; therefore, they are not vulnerable. Another expert, on the other hand, claims that a high level of dependency increases the vulnerability. Conversely he says, when countries such as Turkey have low levels of dependency, it actually decreases vulnerability to cyber attacks.

In other words, the implementation is the critical cornerstone with respect to vulnerability. Higher reliance on automation can be a source of vulnerability if the system is more centralized and open to the main system, and if it is decentralized with a closed system of application, vulnerability is expected to be lower, according an expert.

- Total amount of money spent on technology and vulnerability

When one expert explains how technology is related to vulnerability, she stated that “technology becomes an integral part of our society and of our infrastructure; because it is an integral part of our society and our infrastructure, it becomes an attractive target.” According to one expert, technology is a major factor especially when it comes to information infrastructure protection, but even more important right now, is the proper education and awareness of network administrators and, generally, the people in charge of information security. Therefore, while total amount of money spent on technology may increase vulnerability, awareness of possible risks and education can play a vital role in responding to those vulnerabilities.

According to one expert, money spent on technology may not mean that it is spent for appropriate things.

Risk equation factor. As discussed in chapter four, the risk equation factor is composed of capability and motivation of the terrorists or other groups intending to launch cyber attack.

- Motivation:

In terms of motivation, according to some experts, most of the terrorists prefer traditional methods, including bombing, assassination, kidnapping, etc. The experts claimed that terrorists may not get what they intend from cyber attacks since it may not play to the emotions.

Another issue which deserves a separate analysis is the variation of vulnerability in terms of motivation among countries. While some countries, like the US, could be a major target for terrorists, other countries, which may be developed, may not be vulnerable to cyber attacks by terrorists. It is simply a matter of facing threat from any terrorist organizations. For instance, “Switzerland faces no home made terrorism, nor does it offer a target of interest for terrorist attacks” an expert from that country asserted. “The US represents unique characteristics in terms of vulnerability. According to one expert, US assets still relatively unprotected, also present a large and attractive target. And the US’s current international political decisions and interests are “very much at the front of people's minds" according to an expert. This means vulnerability to terrorist attack is affected by the US's foreign policy decisions. There are sources of motivation for terrorists to carry out cyber attacks if they are capable to do so. The infrastructures of the US are vulnerable to cyber attacks according to an expert. Yet she agrees with the idea that the US is currently vulnerable to cyber attacks which may not be similar to the magnitude of a 9-11 real-world attack. "But that may not be the point. Smaller, less dramatic attacks could serve to undermine confidence in systems," which could be a major source of motivation. That kind of attack does not require sophisticated technical expertise. As discussed before, cyberterrorism as "force multiplier" is more plausible than a cyberterrorist attack resulting in similar devastation to 9-11.

Turkey, on the other hand, has a low level of vulnerability compared to other countries given the fact that Turkey's critical infrastructure does not depend on information technologies, according to an expert from Turkey. Moreover, the public in Turkey is not fully aware of the level of e-government. The expert also looks at the issue of vulnerability to international terrorism. According to him, unlike the US, Turkey is not at the center of global terror attacks. The domestic and foreign policies of Turkey do not impact the globe. Therefore, according to the expert, Turkey is not a primary cyberterrorism target for terrorists. On the other hand, terrorist organizations, such as Turkish Hizballah, and PKK are using the Internet mostly for propaganda. According to another expert, these terrorist organizations may have the motivation, but lack of capability keeps them from launching cyber attacks.

- Capability

In terms of the relationship between vulnerability and capability, one of the experts clarified that capability is the extent to which such groups have the capacity to launch attacks of this type; and vulnerability is the extent to which we are vulnerable to such attacks. She believes that there are groups that are capable of launching cyber attacks on US systems in that they have the expertise and technology to do so. Furthermore, she asserted that there are groups, currently that could launch attacks on our systems that would cause at least some disruption and damage.

Capability, which is another indicator in the risk equation factor, faces a definition problem according to one expert. He pointed out that “It all depends on what you define as ‘cyberterrorism’; if you mean destroying the economy, grounding air traffic, etc then the answer is (2). Otherwise it could be higher, if you take into consideration perception management, propaganda etc. This explanation actually is very critical, given the discussion as to what cyberterrorism means and what kind of destruction cyberterrorism can cause, given the current capabilities of terrorists. Another expert clarifies this issue saying that “For most nations, high economic development equals high reliance on internet and other technologies so vulnerability will be higher, but it also will be dependent on the potential attacker’s level of development.” That means high level of reliance on technology may put nations at risk of being a target of a cyber attack, but the extent to which the attack will lead to destruction or intended impact will be determined by the capability of the attackers.

In terms of comparing countries, there is also difference. According to an expert from the US, who is studying networking between different terrorist organizations, terrorists are taking time to develop their own hackers instead of hiring outsiders to do the job, since it could be too risky. While according to an expert from Turkey, terrorist groups active in Turkey or abroad targeting Turkish interest are not capable of launching cyber attacks. According to the same expert, cyber attacks require a high level of expertise, and the members of the terrorist organizations in Turkey do not have that level of expertise. Even though terrorist organizations in Turkey are using computer technology to communicate and store their information- as in the Turkish Hizballah- the sophistication of their expertise is not enough to launch cyber attacks yet.

Law enforcement cooperation factor. Law enforcement cooperation consists of three indicators: Public and private awareness, level of cooperation between law enforcement agencies and private sector, and a clearly designated agency.

- Public and private awareness and law enforcement cooperation

An expert stated that "without public awareness, training and law enforcement support, law alone is not sufficient enough for fighting against cyber terror, which means a country may have the appropriate laws to criminalize cyber attacks. Awareness, training, and law enforcement support play a critical role.

An expert from the US claimed "there is very little, if any, awareness of the potential for such attacks among the general public, and if the general public, considered both as individuals and as the constituents of our corporate and other agencies, is not aware of the potential for such attacks, they are not likely to make serious efforts to prevent them."

One expert from United Kingdom asserted, "a lack of awareness in public and government, and a failure to recognize that as the methods of countering cyber attack improve, so, too, do the weapons deployed against us" is a major source of vulnerability to cyberterrorism. So, awareness on the part of the public and private sector, in fact, could help to increase the level of cooperation among the law enforcement, as well as the private sector. At the end, awareness of the risk will help to reduce vulnerability.

- Level of cooperation between law enforcement agencies and private sector

In terms of cooperation between law enforcement and private sector, the US can be considered a leading country. An expert from the US stated that The US Secret Service's Electronic Crime Task Forces and the FBI's Infragard program are both doing an excellent job of getting law enforcement and private sector personnel to interact and share information on an informal level, but this is not an easy task." To explain the difficulty, the expert added, "it is a particularly difficult task in the area of cybercrime and cyberterrorism because commercial entities are usually reluctant to share information about successful attacks with law enforcement for fear of negative publicity." This is one of the most critical issues in terms of investigating cybercrime or cyberterrorism because targets mostly involve commercial companies, and they do not want to be publicized in a way which may imply that their system is vulnerable. Furthermore, the expert reveals how the law enforcement entities try to establish and strengthen cooperation with the private sector: The ECTF's and Infragards are working to develop a climate of trust, in which private sector entities can pass information along without fearing it will become public, but this is a slow process and we need to develop a different model, one in which they communicate prospectively, the expert stated.

According to one expert, United Kingdom "is essentially a law-abiding society and, consequently, while we do not have complete integration, law enforcement agencies command a degree of respect and trust and, consequently, co-operation."

- Clearly designated agency

In terms of an agency responsible for responding to cybercrime or cyberterrorism, there are differences between countries. For example, within the US according to one expert, in each jurisdiction at least one authority is designated, but sometimes overlaps may result in confusion. Moreover, another expert gave a perspective in terms of how the interaction between agencies occurs. She stated that "the FBI and Secret Service each investigate cyber attacks, and both are concerned about cyberterrorism. But both being federal agencies, they are small in terms of personnel and therefore cannot deal with all cyber attacks, not even in terms of vetting them and seeing that they are investigated by other agencies." In addition, she said "another complicating factor is that both the FBI and Secret Service work with the Department of Justice, which is responsible for prosecuting cybercrime and cyberterrorism. The Department of Justice cannot begin to handle all the cyber attacks that occur and, indeed, should not. The default model in the US is prosecution at the state and local level, and that is where most law enforcement officers work (there are over 17,000 state and local law enforcement agencies in the US). And there is absolutely no agency that is responsible for coordinating investigations of cyber attacks."

In United Kingdom, the following institutions are responsible for investigating cyberterrorism; the Defense Communication Services Agency, SIS, MI5 and others who share responsibility and report directly to the Joint Intelligence Committee.

Turkey is a good example in terms of how the Turkish National Police (TNP), the national law enforcement agency, adapted itself to the new trends in cyberspace. An expert informs that even though Turkey does not have the legal measures with respect to cyberterrorism or cybercrime, TNP has already established units within the departments and in major cities.

International cooperation. The International cooperation factor is composed of two indicators: multilateral agreements and bilateral agreements.

- Existing multilateral agreements

Almost every country in this study was involved in a different form of multilateral cooperation. However, there are issues need to be addressed. According to one expert, the issue of multilateral cooperation is a “slightly mixed bag”, which means while organizations, such as Europol and Interpol can work together without any problems, when the issues of critical national infrastructure are concerned, it becomes a major issue of sovereignty. This may be overcome through a better coordination and exchange of intelligence, the expert said.

Also in terms of multilateral agreements, even though a country, such as the US, is a party to several multilateral agreements, foreign policy issues, for example, Iraqi Freedom, and other “go-alone” policies have destabilized international support to the US one expert stated.

The experts were asked about the importance of multilateral cooperation, since one of the major constructs in this research is cooperation. One expert stated, “Without it we cannot achieve anything.” However, another expert affirms that multilateral cooperation can be important and achievable “but only useful if good local work is done on which cooperation can build.” Furthermore, another leading expert stated that multilateral cooperation is “critical. By its very nature, cyberterrorism tends to be transnational. Therefore, to be effective in responding to a terrorist attack and in working to prevent such an attack, we must be able to call upon the assistance of other countries.”

- Existing bilateral agreements

While existing multilateral agreements are important cornerstones to effectively respond to terrorism, “the time scales for emerging threats is much shorter than that of new bilateral agreements – yes, they are good but are probably relatively ineffectual at any one time,” one expert claims. Furthermore, another expert claimed that existing bilateral agreements seem inadequate to deal with problems worldwide.

As a response to the question whether or not existing international organizations such as the UN, OECD, G-8, and EU, one expert stated that “they need to work out how to cut across institutional stovepipes and provide comprehensive and global response to threats.”

Similarly, another expert stated that it “really depends on the processes that both parties are willing to commit to in order to bring about an effective response. In recent times, I would say that these organizations have not always been in full agreement (to put it mildly).” This is unfortunately observed at the UN and in other international organizations when it comes to the issue of military operations and terrorism. Nations brought their own concerns to the table instead of trying to bring solutions.

Like multilateral agreements, bilateral agreements play a very critical role in responding to overwhelming problems in our world. As one expert cited from John

Donne: “No man is an island”, and added, “global terrorism is global, individual countries are not; therefore we need global alliances.”

In terms of effectiveness of bilateral and multilateral cooperation, there are opposing opinions. For instance, one expert claimed that “trust, loyalty and co-operation can be developed in a partnership of two.” Cooperation may increase exponentially as the members within a partnership increase. Therefore, bilateral cooperation is more achievable.

While most of the experts in the research considered multilateral cooperation effective, in terms of achieving either one, experts agree that bilateral agreement is more achievable than multilateral agreements.

According to James Lewis, who is a Research Fellow and the Director of Technology and Public Policy at the Center for Strategic and International Studies in Washington, D.C., multilateral cooperation is possible, but harder to achieve, since organizations like the UN are composed of diverse members in terms of political, economic, cultural, or even legal issues.

Cooperation is a must to respond to terrorism, cyberterrorism, or cybercrime; however, there are problems that need to be addressed, according to Professor Lewis. These problems are:

1. Lack of adequate computer laws
2. Lack of practices and patterns of cooperation
3. National sensitivity over cooperation issues, especially if it involves sovereignty.

As a solution to these problems, Professor Lewis proposed informal cooperation among different law enforcement agencies worldwide to overcome the bureaucracy and other obstacles.

Legal measures. The legal measures factor is composed of two indicators: substantive and procedural laws.

- Effectiveness of the existing substantive laws

There is variation among countries having substantive laws. While some countries extensively amended laws regarding cybercrime and cyberterrorism, some either do not have comprehensive laws, or they use cybercrime laws to prosecute terrorism-related cyber criminal activities. In some countries, such as Switzerland, laws against cyberterrorism are, in fact, the laws against criminal acts in general, which focus on data destruction and similar acts. While in countries such as the US, specific laws exist to cover cyberterrorism. One expert stated, “in the United States, the substantive laws at the federal level do a very good job of dealing with cyberterrorism.” Further she explains how the system works:

> Now, if a cyberterrorist attack causes death, injury and/or property damage, we can, as I noted earlier, prosecute that under traditional substantive law, for the most part. Using computer technology to shut down a power grid and thereby causing death is homicide; the computer is simply a tool for committing murder. The same is true for non-traditional crimes like hacking and virus dissemination; most states – as well as the federal system – do a good job of criminalizing these activities.

In United Kingdom, on the other hand, “laws have led to greater restrictions on certain behaviors while not really addressing the problem at hand. Many decisions made under new laws now being challenged so no real progress made” one expert claimed.

On the other hand, in Turkey, there is not a law criminalizing cyber attacks, yet nor does Turkey have any law which regulates the ISPs in terms of keeping records of accesses, emails, or other Internet related activities which may weaken law enforcement organizations.

- Effectiveness of the existing procedural laws

In terms of procedural laws, similar to the substantive laws, there is a variation from one country to another. While in Switzerland, national laws provide a good base for the fight against cybercrime perpetrated by either terrorists or ordinary criminals, in the US depending on the characteristics of the criminal act, laws may define cyberterrorism.

Freedom. All the countries in this research except for Turkey are rated as Free countries. Experts in the Free Countries agreed that governments are facilitating civil liberties in their countries. Turkey is rated as Partly Free based on the Freedom House Database ratings. However, new legislation and attempts toward implementing those laws are expected to facilitate more freedom in Turkey.

Discussion

The discussion section analyzes three critical issues. First of all, the definition of cyberterrorism is discussed based on the literature review and survey results. Secondly, the factors constructing the Vulnerability-Comprehensive Cooperation-Freedom are discussed briefly in terms of the findings. Finally, realistic approach versus liberal approach is analyzed based on the responses from the experts.

First, it is necessary to shed light on the issue of doing research in the area of cybercrime and cyberterrorism. The research and the literature in the area of cyberterrorism involve three groups of experts. The first group of experts claims that cyberterrorism is real and poses a real threat to our society. On the other hand, the second group of experts insists that cyberterrorism is just a myth. The third group, however, asserts that cyberterrorism is real, but the level of threat in terms of capabilities of terrorists to launch an attack which will result in similar impact in terms of physical destruction and fear as the traditional terrorist attacks has not been witnessed yet.

The author of this research thinks that looking at the extremes is not helpful. The fact is terrorists are looking for many ways to inflict pain, fear, and damage to the targeted society. It is correct that the impact of cyberterrorism will not be the same as traditional terrorist tactics, at least for now. But before September 11th, 2001 no one except for “late-experts” could imagine that terrorists would hijack an airplane, actually four, in the US and use them as weapons. To deny cyberterrorism or to conceive it as an absolute weapon is extreme thinking; the middle road is to look at the possible impact, to try to identify vulnerabilities through which cyber attacks can be launched. It has been stated many times on different occasions that terrorists are looking for any necessary means to attack their targets. That is a hard reality and we should concede that we have vulnerabilities, and accordingly we need to take necessary steps to ensure that they are well identified so that necessary precautionary measures are taken.

In terms of academic research, there are issues to be addressed. During the research, including literature review and survey, three patterns of academic and practical conceptions and perceptions of cyberterrorism arose. As revealed before, there is a diverse group of people from a variety of academic backgrounds and from different fields of practice. The responses and writings from these individuals vary depending on their personal backgrounds. Secondly, those whose backgrounds are computer science, information security, or other information related fields naturally focus on the issue of whether terrorists can or cannot have access to network systems and consequently execute their attacks and cause physical damage. Some experts perceive this is possible, and some do not. Those, who are academicians and/or practitioners in the area of terrorism, perceive that cyber attacks are possible. They also emphasize the importance of how terrorists use technology to establish networks.

Another important point that needs to be addressed is that cyberterrorism involves disruptive and/or destructive information attacks. Also, depending on the country, crimes such as money laundering, fraud, or other ordinary crimes can be investigated under terrorism on the basis of supporting terrorist activity. In other words, what makes action terrorism or ordinary crime, such as money laundering is the political motivation toward supporting a terrorist organization or ideology. If we look at the difference between organized crime and terrorism, generally speaking, the most profound difference is the political motivation with a strong ideological basis.

Considering those facts, it is necessary to make a distinction between cybercrime and cyberterrorism. It is important to define- these two concepts in terms of their differences. What is the difference between an ordinary hacker and a person who is committing cybercrime with the intention of supporting a terrorist organization?

To avoid confusion, the author of this research suggests that defining concepts is the first critical step. The definition process should neither exclude activities, which are supposed to be defined as cyberterrorism, nor do they include those that are not supposed to be included. The author of this research considers three important points when he attempts to define cyberterrorism. First of all, the literature shows us that cyberterrorism is a real threat. Second, while we define terrorism, the focal point is a politically motivated violent act which may result in injury, death, or great fear in the public; we should not necessarily look for death or injury when it comes to defining cyberterrorism. In other words, cyberterrorism can be used as “force multiplier,” which may involve disruptive or destructive information attacks, which may not result in physical injury but fear and loss of confidence in the government, especially if such an attack is executed following or prior to a devastating terrorist attack. Finally and most importantly, the definition of cyberterrorism should include a technological aspect which makes cyberterrorism fundamentally different from traditional terrorism.

Another aspect of cyberterrorism is the C-F-R-P factor identified as a result of the survey. The use of communication, fund raising, recruitment, and propaganda by terrorist organizations may or may not be defined as cyberterrorism depending on the country. As discussed before, it depends on the legal measures of a country defining those actions. Nevertheless, the CFRP factor is very important in terms of responding to terrorism as a whole. Response strategies and policies targeting terrorism should include approaches focusing on the CFRP factor. Given the reality that terrorists use IT technologies to establish networks with other terrorist organizations, monitoring activities occurring on the Internet and other telecommunication networks become critical. Monitoring CFRP will provide significant information with regard to future plans of attack.

However, such an attempt may endanger the fundamental rights of individuals, including privacy and other civil liberties. Therefore, law enforcement and other criminal justice entities should avoid any intrusive actions. Of course, the executive branch and legislative bodies of any country have the responsibility to regulate the authority and boundaries of law enforcement.

There is a variation among countries in terms of if and how terrorist organizations use technologies in their activities. Not every terrorist organization uses the Internet to communicate. However, it is accurate to state that international terrorist groups use the Internet to communicate with their members and possibly other groups with similar ideological backgrounds.

In terms of factor analysis, the research has shown that vulnerability, comprehensive cooperation, and freedom have been constructed by seven factors. The relationship between vulnerability and comprehensive cooperation is positive while freedom has a negative relationship with both vulnerability and law enforcement cooperation. As discussed previously, the research shows that a country with a high level of vulnerability is expected to seek more cooperation at the domestic and international level.

Three factors in the research determined the vulnerability construct. The research has shown that there is a relationship between level of development and vulnerability. Also, developed countries are expected to be highly dependent on technology, which according to most of the experts makes countries more vulnerable than those which do not have a similar level of reliance on technology. Another equally important factor is the Risk Equation. In fact, for most of the countries, the Risk Equation can be a primary determinant in terms of whether or not the country is vulnerable. While the Risk Equation Factor does not determine vulnerability directly, it actually explains the risk of being attacked. In other words, a country, for example, Switzerland, can be developed, and may depend greatly on technology. Another country, like the US may be at higher risk than others, since the Risk Equation for the US is more profound than other countries. Of course, it is important to state, again, that having motivation does not necessarily mean that terrorists are capable of executing such an attack. Therefore, capability also plays a very critical role in determining vulnerability.

The research shows that there could be a variation of vulnerability among countries that may have the same level of development in terms of reliance on technology and other things that make those countries more vulnerable. For instance, while the characteristics of the US, in terms of the indicators of vulnerability, put the US at a high level of vulnerability, the measures the US has taken to ensure the safety of its critical information infrastructures decreases that risk. As Professor Denning stated, reliance on technology may be a source of vulnerability, but implementation of security measures may decrease the risk of being a target of an unfortunately successful attack. Conversely, a country, such as Turkey which has different characteristics in terms of reliance on technology may be at a higher risk than it normally should be due to lack of awareness and legal measures.

The variation also can be explained by variation in the motivation of terrorists against individual countries. While level of development and level of reliance on technology factors put a country in a vulnerable position, the experts agreed that the motivation to launch a cyber attack is not solely related to these factors, rather motivation results from foreign policy issues of a country, as well. As one expert explained, for instance, US foreign policy decisions put this country into a more vulnerable position than other countries with similar levels of development or reliance on technology. Countries, such as Switzerland, that have conditions which may put them into the vulnerable category are also exposed to other important components; motivation and capability of terrorists do not exist. On the contrary, some countries, such as Turkey may not be within the category of vulnerable countries, yet motivation of terrorists to launch cyber attacks by different groups can exist. However, their capabilities to execute such an attack seem implausible for the immediate future.

Moreover, the variations of vulnerability, cooperation, or freedom among countries represent another source of vulnerability. In other words, variation, itself is a source of vulnerability. As the research revealed, cyberterrorism or cybercrime is transnational in nature which means response to these crimes requires commitment from several countries. However, since not every country is equally vulnerable they may not consider participating in cooperative efforts in the areas of cybercrime or cyberterrorism. This may, in turn, weaken the comprehensive response.

The second major construct of the V-C-F scale is comprehensive cooperation. I called it comprehensive cooperation, because naming this construct as law enforcement cooperation or just as cooperation might have narrowed the perspective of this research. Comprehensive cooperation includes both domestic and international cooperation, law enforcement cooperation, and legal measures, all of which play very critical role in responding to cyberterrorism or cybercrime. For example, as the experts stated, with lack of awareness, training, and law enforcement support, laws amended to respond to threats coming from cyberspace could be meaningless. Laws, alone, cannot reduce vulnerability. Individuals need to be aware of the risk. Moreover, unless the law enforcement and private sector establish a common understanding and cooperation, law enforcement efforts may not lead to the expected outcome.

The international cooperation factor is as complex as the domestic level of cooperation if not more so. As the experts stated, it is a mixed bag, including ambitious propositions, concerns, disputes, and the like. The fact is vulnerabilities exist even with variations. It could be naïve to say that some developed countries are immune from cyber attacks. Yet, when it comes to international affairs, there is an issue of sovereignty and national security. In particular, foreign policy issues involve national interests of every country. Sometimes countries may push their own agendas, even sometimes by disregarding others' concerns. In such an environment, it is very difficult to establish a general consensus as to what should be done to effectively respond to cyber threats, and in general, other threats coming from terrorists.

This discussion brings us to the analysis of the two different approaches in terms of international cooperation. As discussed in chapter two, different approaches are presented. They are Devost's realistic approach versus the liberal approach. To summarize, the realist perspective holds that the international political system is anarchic and it is based upon distrust of other nations; therefore, international cooperation is not an effective means of deterrence in terms of international and transnational terrorism. The realistic approach tries to deal with cybercrime, cyberterrorism, or any other threat by focusing on the individual efforts of the targeted country. On the other hand, liberal approach, does not perceive the international political system to be as anarchic as do the realists. This perspective holds that countering cyberterrorism should be based more on cooperative efforts than on offensive and defensive efforts. The liberal approach pursues the objectives of increasing the level of interdependency, and promoting international cooperation. However, opponents of this approach claim that not every country is under a similar level of vulnerability, therefore, it is very difficult to accomplish international cooperation, if not impossible. This study shows that yes, there is variation among countries; however, to effectively respond to cybercrime or cyberterrorism even traditional terrorism, countries that are under high risk should work with other countries to create an environment in which they can propose and implement new counterterrorism strategies. Since the possible consequences of a cyber attack in a country can be seen in another country, other countries which may not be under similar threats should step up to the plate to help other countries. In sum, this research supports neither the realistic nor the liberal approaches. According to the experts, the ideal strategy to effectively respond to cybercrime and cyberterrorism would be for countries to take necessary measures individually as if there is another country which may be worked with. At the same time, that country should pursue ways to enlist cooperation with other countries, as if they cannot achieve real safety without such cooperation. It is a fact that not every country is vulnerable to cyber attacks, yet it is also a fact that those that are vulnerable need to work with countries that have less vulnerability, given the nature and consequences of cyber attacks.

Also, with respect to countries such as Turkey, although the expert scale value shows a high level of cooperation, in terms of legal measure, as some of the experts revealed in their responses, Turkey has weaknesses in terms of legal measures that define cyberterrorism and cybercrime. While these crimes are prosecuted as terrorism-related incidents, there should be specific regulations and amendments to define criminality and punishment. While there is an effective communication and coordination between anti-terrorism units across the country, Turkey should reconsider some of its laws regarding cybercrime and accordingly, cyberterrorism.

If countries are taken as a group, like developed countries, results may be different. The research showed that motivation and capability are very important in determining whether that country is vulnerable to cyber attacks. For instance, while the mean values of the indicators which construct the vulnerability variable are very close to each other, only the value of motivation is significantly higher than any of the other mean values of the items. That high level of motivation accordingly increases the risk for the US.

Importance of the Research

The importance of this research can be summarized as follows:

- This research can be considered the first in the area of cyberterrorism and cybercrime.
- This research clarifies the critical concepts of vulnerability and cooperation.
- Furthermore, this research also attempts to create a scale which can be used for different purposes.
- The scale can be used as a standard for the evaluation of the level of vulnerability, cooperation, and freedom to establish a consensus.
- This research identifies necessary steps to establish cooperation at the domestic and international level.
- This research generated invaluable data from experts in cyberterrorism and cybercrime.

First of all, this research can be considered the first in the area of cybercrime and cyberterrorism. While there are a number of studies analyzing vulnerability from more of a technical perspective, the area of research does not have many studies focusing on the technical, legal, and political aspects of vulnerability, cooperation, and freedom all together.

Also, the research clarifies the critical concepts, such as vulnerability and cooperation. In addition, the research attempts to propose a definition of cyberterrorism. Moreover, determining the factors constructing major variables, vulnerability, comprehensive cooperation, and freedom contribute to the field by explaining individual factors. Finally, clarification involves the major construct as well as the indicators loading to the factors.

Furthermore, this research also attempts to create a scale which can be used for different purposes. For research purposes, having such a scale will help researchers to use the scale for their studies focusing on vulnerability, cooperation, and freedom. These types of scales are commonly used in the area of political science, economics, telecommunication, and the like. Scales, such as the Freedom Scale, explained in detail in previous chapters are used not only by academicians but also by governments to monitor political rights and civil rights trends around the world. Therefore the scale created as a result of this research can be improved and made use of by governments to gauge and evaluate their level of vulnerability and level of cooperation.

The scale, as a start, can be used as a standard for evaluation of the level of vulnerability, level of cooperation and freedom so that a consensus or a common understanding may be established, thereby facilitating knowledge of the phenomenon.

In terms of its results, the research also presents invaluable data for academicians and professionals from law enforcement, security institutions, and government officials who are carrying out responsibilities in the area of global and national security. One of the most critical findings of this research is as the vulnerability increases, the necessity for cooperation increases. It shows that developed countries that rely heavily on technology and are exposed to threats from terrorists, unfriendly nations, or other criminal groups should seek to establish more comprehensive cooperation. Comprehensive cooperation should include cooperation at the domestic and international levels. Since the source of vulnerability to cyber attacks can emerge from domestic and international sources the focus should be on both. At this point, the author of this research would like to introduce the concept of the perceptional definition of cooperation. The perceptional definition of cooperation maintains that a country's decision to involve itself in cooperative efforts for the purpose of responding to global security issues will depend on how the country perceives cooperation in responding to global security issues.

Aside from statistical analysis, literature review and content analysis of the expert opinions reveal invaluable information for the identification of the necessary steps to establish cooperation at the domestic and international levels. The research successfully identified four types of vulnerabilities: political, technical, cultural, and legal. These classifications summarize the difficulties to establish cooperation, and the sources of vulnerabilities.

Policy Implications

This study strongly emphasizes the importance of cooperation in response to the threats coming from cyberspace. In particular, considering the matrix of vulnerability-comprehensive cooperation-freedom, countries with high level of vulnerabilities need to involve in cooperative efforts not only with those countries that are highly vulnerable, but also with other countries with lower level of vulnerability. Given the fact that a cyber attack can be launched from anywhere, the source of such an attack does not necessarily have to be a country with a high level of technological development. This brings us to the issue of having vested interest in expanding an alliance to include many countries with a variety of different backgrounds.

In terms of a theoretical discussion, any country concerned about cyberterrorism should embrace the double approach. That is, while taking every necessary step to ensure the safety of their critical infrastructures, they should also make every effort to achieve an inclusive partnership/alliance with other countries.

To achieve such an overwhelming task, different venues should be sought after, including formal and informal cooperation. Cooperation may involve both formal and informal relationships, and the effectiveness of both may vary depending on the case in question. While the desired relationship should be formal cooperation, it has drawbacks, most notably, bureaucratic procedures takes a long time which could be crucial for law enforcement and other national security agencies. Particularly, investigating cyberterrorism does not provide the luxury of spending time for going through bureaucracy. On the other hand, while informal mechanisms are efficient in terms of time, in some countries, informal cooperation may not be approved by their governments. Therefore, in responding to cyberterrorism or cybercrime, both informal and formal cooperation should be put into practice while efforts are being made to lessen the bureaucratic procedures which can be achieved by bilateral agreements.

Awareness is another cornerstone toward achieving real-concrete cooperation. Developing awareness at the domestic and international level toward cyberterrorism and cybercrime will help concerned parties to work with other countries. Recognizing existing or potential risks will motivate countries to start to take necessary measures to respond to cyberterrorism and cybercrime, to include legal, technical, and political procedures.

Another important issue with respect to policy implications is the legal discrepancies and/or lack of legal measures targeting cyberterrorism and cybercrime. While countries amend new laws or update the existing ones to compensate the gap stemming from new trends to respond to cyberterrorism, they also should try to establish a consensus as to what cyberterrorism constitutes and what the general procedures should be in terms of handling investigations and prosecution of cyberterrorism related incidents. Conventions, such as the Council of Europe Convention on Cybercrime –even though there are some questions about the article in the Convention Treaty- is an ambitious attempt toward achieving such a consensus.

In terms of facilitation of cooperation at the national and international levels a number of entities can play important roles. In particular, institutions, such as CERT and FIRST can be instrumental in carrying out informal and formal bilateral and multilateral cooperation. In the area of cyberterrorism and cybercrime such an activity at the informal level among private or public institutions can lead to formal cooperation since informal processes can guide the development of a culture of cooperation. Moreover, entities, such as G-8 and OECD can lead other non-member countries toward developing a certain level of awareness. While these entities do not have operational branches, they can set the standards for future applications and strategies for themselves and be examples for other countries. On the other hand, institutions, such as the UN and the Council of Europe can be more active organizations since they constitute more member states. Also the members can be obliged to fulfill the requests from these multilateral entities, which can be vital to achieve consensus.

Also, developed countries can offer technical and legal assistance to other countries; in other words, developed countries can expand the response policies by supporting other countries. One way to accomplish a sound cooperation is to identify regions and focus those areas. Countries such as Turkey can be a center in the Middle East, including the former Soviet Union Republics. Turkey can work with experts from the US and other European countries to train law enforcement in the region in the area of terrorism and cybercrime. Given the fact that Turkey has a long history of struggle against terrorism and organized crime, the experience can be utilized toward advancing regional countries' abilities and understanding toward how to handle terrorism, in particular, cyberterrorism and cybercrime.

Other critical and rather sensitive issues are national sovereignty and jurisdiction. National sovereignty is a political issue that may be an obstacle since countries have every right to claim their sovereignty when it comes to investigating cyberterrorism. Respectively, the issue of jurisdiction becomes a legal issue when investigating cyberterrorism and cybercrime, both of which are transnational in nature. To overcome these two critical issues existing applications from other areas can be considered. Aviation is one of those areas that involve internationally recognized and implemented regulations worldwide. Agreement over such an area can be a model for cyberterrorism and cybercrime initiatives. Another application is the “European Arrest Warrant” which can give a clue as to how the international community will overcome issues of jurisdiction. Of course the author of this study does not imply that we need to have such a system; however, the European Arrest Warrant can be taken as an example.

In terms of overlaps between cybercrime techniques and cyberterrorism, the study suggests that cybercrime techniques are readily available tools for terrorists to exploit. More importantly, technology provides ample opportunity for terrorists to expand their operations and establish new networks with other terrorist organizations. More importantly, cyberspace gives terrorists new tools to recruit new members and to support their activities financially. The C-F-R-P factor is very critical in terms of responding not only to cyberterrorism, but also to traditional terrorism. The C-F-R-P factor can, in fact, be monitored by law enforcement and can be used to identify possible recruitment techniques, possible new recruits, and finance sources. Also, it can provide invaluable information in terms of communication. It is true that not every terrorist organization uses the Internet for communication; nevertheless, communication on the Internet can provide leads for further investigations.

Recommendations

The recommendations involves two sections. The first section focuses on the recommendations related to the findings, and the second section focuses on areas for future research.

According to the results of the study, the following recommendations should be considered;

There is a positive relationship between vulnerability and comprehensive cooperation; in other words, higher vulnerability requires a higher level of cooperation. Therefore, developed countries, in particular, those that are under threat of cybercrime and cyberterrorism or traditional terrorism should seek more cooperation with other countries.

Secondly, this study also showed that there is a negative relationship between freedom and vulnerability, which means, countries with vulnerabilities to cyber attacks should deter any attack, while they also maintain the level of freedom in their societies. In this case, cooperation will help to achieve that goal.

Third, results also showed that there is a strong association between cybercrime techniques and cyberterrorism which means, according to the experts, that cybercrime techniques can be used either for actual attack or as force multiplier which may not involve physical damage or death, but panic and fear. Therefore, denying cyberterrorism cannot decrease risk. Conversely, considering cyberterrorism as an ultimate weapon for terrorists is an extreme viewpoint. The expert responses and literature revealed that yes, there is a risk, but the level of risk is directly related with the level of motivation and capability of the terrorists. Nevertheless, the resultant typology of the cyberterrorism study shows that it is obvious that cybercrime results in financial loss and sometimes panic within a small community, in particular those using the internet and other types of computer networks. In a sense, efforts targeting cybercrime also lead to responding to the risk coming from cyberterrorism.

Fourth, cooperation is very critical in terms of responding to cyberterrorism and cybercrime. Cooperation at the national level includes law enforcement and private sector. Sometimes overlaps in terms of the responsibilities and authorities between different law enforcement agencies may cause confusion. To avoid such an event, law enforcement should establish a coordination center that will not be a supervisory unit, but a unit which will facilitate coordination and collaboration between layers of bureaucracy. This is particularly important in countries like the US, where there are numerous law enforcement agencies with a number of laws giving authority to them. Also, implementations, such as the US's Secret Service Electronic Crime Task Force, should be expanded across the world. The most important aspect of such programs is that they create a sense of trust between law enforcement agencies and the private sector. Of course, the purpose of these programs should be to share the concerns and support each other. Finally, increasing awareness of vulnerabilities to cyberterrorism and cybercrime can be facilitated by training of law enforcement and the public. At the National level, documents, such as the National Strategy to Secure Cyberspace, published by the US indicated the importance of national and international levels of cooperation to respond to threats coming from cyberspace. It also emphasizes the importance of cooperation and collaboration between the public and private sector to adequately respond to cyber threats. It is true that a document, alone, may not be effective, but it may describe the path to be followed.

Fifth, the international cooperation factor represents one of the major aspects of this research. While there are numerous issues regarding how to achieve a sound international cooperation, the first step toward it involves believing in establishing international cooperation. In other words, countries should spend time and energy establishing a general consensus as to what they should do to achieve real cooperation. Based on the research results, while multilateral cooperation is desirable, bilateral agreements are considered as more achievable than multilateral agreements. Therefore, countries should focus on establishing more bilateral agreements with other countries; they also should explore new venues to set up multilateral cooperation. To achieve a real cooperation at the international level, countries should practice real coordination and exchange of intelligence. Formal bilateral and multilateral agreements and organizations achieve some level of cooperation, but bureaucracy and other obstacles may slow down the procedures which are very critical in investigating cybercrime. To solve that problem, countries should look for ways to practice informal cooperation at least among the law enforcement agencies.

Moreover, legal measures play a very critical role in responding to cybercrime and cyberterrorism. The laws and conventions, such as the Council of Europe Convention on Cybercrime are useful tools to facilitate cooperation. In order to respond to transnational crime, such as cybercrime and terrorism, having a common definition of the crime is vital. Recognizing the importance of defining a crime according to its unique characteristics will not only ease the investigation procedures, but also enable cooperation with other countries. Therefore, countries should reattempt to come up with internationally accepted definitions of terrorism, cybercrime, and cyberterrorism.

Finally, we need to find out new strategies and tactics to respond to the overwhelming problems we face today. Global nature of the issues such as cybercrime and terrorism requires global responses. It is necessary to look for a radical approach. Globalization of crime, in fact, asks for globalization of law enforcement. This statement may sound overambitious; however, given the extent and complexity of cybercrime and terrorism, it may be underestimating the seriousness of these problems if we claim otherwise.

Future Research

In general, future research should involve the following:

- Future research should involve validation of the scale using a re-test method.
- Future research should focus on applying the scale to countries based on their characteristics, considering the indicators.
- The scale can be utilized as a tool to evaluate the ratings of the countries based on their individual characteristics.
- There is a need to improve the scale in terms of data that can be used in determining the ratings.
- There is a need to focus on how informal cooperation processes can be successful without violating the regulations of the concerned countries.

The validation of the scale developed as a result of this study can be carried out by sending the questions with the results obtained based on the study to the same experts in order to gauge the validity of the scale.

Research in the area of cybercrime and cyberterrorism mostly involves vulnerability assessment, and in some cases comparative study focusing on legal measures of different countries. This research focused on clarification of the typology of cyberterrorism and development of a scale. If there is enough data in terms of cyberterrorism and cybercrime incidents, the relationship between three major variables can be made more efficiently instead of solely relying on expert opinion. Also, if we had been able to gather data from those countries that have very limited or no reliance on technology, the comparative aspect of the research would have been more powerful. Moreover, although the author of this research spent a tremendous amount of time and energy trying to increase the diversity of the respondents, the secrecy and sensitivity of the information requested by the survey questions prevented some experts the ability to fully participate in the research. Were this not the case, greater diversity among the expert panel would have been more powerful.

This research managed to develop a scale which is composed of vulnerability-cooperation-freedom. Future research, first of all, should focus on applying the scale to the countries based on their characteristics considering the indicators.

The scale can be utilized as a tool to evaluate the ratings of the countries based on their individual characteristics. Like the Freedom House Database, the scale can be used to determine the ratings of the countries in terms of how vulnerable they are to cyber attacks, the level of cooperation they are involved in, and what more they can do to secure their safety without limiting civil and political liberties.

Also, this research is the first attempt to develop a scale; therefore, there is a need to improve the scale in terms of data that can be used in determining the rating. In other words, we need to do more validation testing with other countries.

In addition, there is a need to do research in the area of comprehensive cooperation**.** Future research should include analysis of specific topics, such as jurisdictional problems in terms of investigating those crimes. There is enough research in the literature in terms of jurisdictional problems, and a few people have studied how we can deal with those problems. In terms of how law enforcement cooperation should be put into practice still begs for more attention. The research in this area should focus on how international and supranational bodies, such as Interpol, Europol, and other regional training centers facilitate cooperation. The problems facing cooperative efforts can be analyzed by looking at the principles of those entities and how they implement them.

In addition to formal cooperation, there is a need to focus on how informal cooperation processes can succeed without violating the regulations of the concerned countries. It is obvious, based on the research that there is an imminent necessity to work together to respond to cybercrime and cyberterrorism. However, since international cooperation procedures are regulated by bilateral and multilateral agreements, it is important to figure out a way to avoid any confusion and violations of these agreements.

Future research should also focus on how terrorists establish networks with other terrorist organizations, and how they use technologies. While there is literature analyzing networking, the CFRP factor deserves more analysis in terms of how terrorists use the Internet to facilitate fund raising and recruitment.

Conclusion

Responding to transnational crime, including cybercrime and cyberterrorism is an overwhelming task. The global nature of cybercrime and cyberterrorism requires global responses. Creating a scale is an attempt toward establishing a kind of standard as to what are the factors affecting three major constructs of this research. There are seven factors constructing the 3 major variables. Also, exploring a typology of cyberterrorism can help concerned parties to analyze what kind of cybercrime techniques can be used by terrorists and those who are supporting terrorist activities.

In addition, this study clarifies important concepts, including vulnerability, cooperation, freedom, and cyberterrorism. The study, more importantly, proposed recommendations as to how the Vulnerability-Comprehensive Cooperation-Freedom scale or “Ozeren Scale” can be used by academicians and other related entities at the public and private level.

There are limitations from which this study suffers. The number of respondents is significant. Having a higher number of respondents could have resulted in more powerful research in terms of generalizability. On the other hand, the quality of the respondents actually provided a high level of expertise and input to the research.

In conclusion, this research has shown that whether it is cyberterrorism, cybercrime, or traditional terrorism, it does not make a significant difference when it comes to international cooperation. In fact, the most developed and powerful countries in the world are the ones that rely on more cooperation, according to the results of this study. Regardless of how sophisticated their systems of response to terrorism, the most vulnerable countries are the same countries that need more cooperation from other countries. The research clearly shows that law enforcement cooperation is an ultimate necessity for the most vulnerable countries. John Donne said once, “No man is an island,” and there is no guarantee that some countries or entities are immune from the global problems we face today. Therefore realizing that fact will hopefully lead the international community to work together to come up with a consensus as to what we can do to respond to cybercrime and cyberterrorism.

APPENDIX A

THE VULNERABILITY-FREEDOM-LAW ENFORCEMENT SCALE

QUESTIONNAIRE

Country of origin ____________________

Would you please put `X` by the number of your choice depending on your answer.

“**DK**” = “**don’t know**”

1. What is your assessment of the vulnerability of your country to cyber attacks by the groups, including terrorists and unfriendly nations?

Not vulnerable			Vulnerable			Completely vulnerable	DK
1	2	3	4	5	6	7	

Participant’s own explanation:

2. What is your assessment about the level of motivation of the terrorist group(s) to target your country?

No motivation			Motivated			Very high motivation	DK
1	2	3	4	5	6	7	

Participant’s own explanation:

3. What is your assessment about the level of capability of the terrorist group(s) to carry out cyber attacks against your country?

No capability			Capable			Very capable	DK
1	2	3	4	5	6	7	

Participant’s own explanation:

4. What is your assessment about the relationship between the level of economic development in your country and its vulnerability to cyber attacks by terrorists and unfriendly nations?

No relation			Related			Completely related	DK
1	2	3	4	5	6	7	

Participant's own explanation:

5. What is your assessment about the relationship between the level of industrialization in your country and its vulnerability to cyber attacks by terrorists and unfriendly nations?

No relation			Related			Completely related	DK
1	2	3	4	5	6	7	

Participant's own explanation:

6. What is your assessment about the relationship between the number of Internet users in your country and its vulnerability to cyber attacks by terrorists and unfriendly nations?

No relation			Related			Completely related	DK
1	2	3	4	5	6	7	

Participant's own explanation:

7. What is your assessment about the relationship between the number of Internet service providers in your country and their vulnerability to cyber attacks?

No relation			Related			Completely related	DK
1	2	3	4	5	6	7	

Participant's own explanation

8. What is your assessment about the relationship between the level of your country's dependency on telecommunication services and its vulnerability to cyber attacks by terrorists and unfriendly nations?

No relation			Related			Completely related	DK
1	2	3	4	5	6	7	

Participant's own explanation

9. What is your assessment about the relationship between the level of dependency on automated systems in your country and its vulnerability to cyber attacks by terrorists and unfriendly nations?

No relation			Related			Completely related	DK
1	2	3	4	5	6	7	

Participant's own explanation

10. What is your assessment about the relationship between the total amount of money spent on technology in your country and its vulnerability to cyber attacks by terrorists and unfriendly nations?

No relation			Related			Completely related	DK
1	2	3	4	5	6	7	

Participant's own explanation

11. What is your assessment about the level of public and private awareness against the threat of cyber attacks by the cyberterrorists targeting critical information infrastructure in your country?

No awareness at all						Highly coordinated efforts	DK
1	2	3	4	5	6	7	

Participant's own explanation

12. Given the factors above, would you change your assessment of the vulnerability of your country to cyber attacks by cyberterrorists?

Not vulnerable			Vulnerable			Completely vulnerable	DK
1	2	3	4	5	6	7	

Participant's own explanation:

II. Freedom in the Society

13. What is your assessment of the level of freedom (civil liberties) in your country?

Free			Partly free			Not free	DK
1	2	3	4	5	6	7	

14. Are you aware of the “Freedom” scale used by Freedom House?

Yes	No
1	0

15. What is your assessment about the following statement: “The system of government (SoG) in your country facilitates freedom”.

Strongly disagree			SoG does not affect freedom			Strongly agree	DK
1	2	3	4	5	6	7	

Participant’s own explanation:

III. Law Enforcement Cooperation

16. Assess the level of cooperation between law enforcement agencies and private sector in your country.

No cooperation			Cooperate			Total integration	DK
1	2	3	4	5	6	7	

Participant’s own explanation:

17. Is there a clearly designated agency for investigating cyber attacks?

No authority			At least 1 authority			Clearly identified authority	DK
1	2	3	4	5	6	7	

Participant's own explanation:

18. Do existing multilateral international agreements and efforts adequately defend your country against cyberterrorism?

No agreement						Adequately defend	DK
1	2	3	4	5	6	7	

Participant's own explanation:

19. What is your assessment on the importance of multilateral cooperation to respond to terrorism?

Not important						Very important	DK
1	2	3	4	5	6	7	

Participant's own explanation:

20. Do existing bilateral agreements adequately defend your country against cyberterrorism?

No agreement						Adequately defend	DK
1	2	3	4	5	6	7	

Participant's own explanation:

21. Do existing international organizations, such as the UN, OECD, G-8, and EU provide an environment through which your country can effectively respond to terrorism?

No agreement						Adequately defend	DK
1	2	3	4	5	6	7	

Participant's own explanation:

22. What is your assessment on the importance of bilateral cooperation to respond to terrorism?

Not important						Very important	DK
1	2	3	4	5	6	7	

Participant's own explanation:

23. In your assessment, which one is more effective on responding to terrorism?

Multilateral	Bilateral
1	2

24. In your assessment, which one is more achievable?

Multilateral	Bilateral
1	2

25. What is your assessment about the effectiveness of the existing substantive laws amended to respond to cyberterrorism?

No substantive law						Very effective laws	DK
1	2	3	4	5	6	7	

Participant's own explanation:

26. What is your assessment about the effectiveness of the existing procedural laws (e.g. search and seizure laws, evidentiary standards, etc.) amended to respond to cyberterrorism?

No procedural law						Very effective laws	DK
1	2	3	4	5	6	7	

Participant's own explanation:

27. Please assess each of the following international organizations in terms of their effectiveness in responding to cyberterrorism? (1 = not very effective; 7 = very effective)

United Nations (UN)	1	2	3	4	5	6	7	DK
European Union (EU)	1	2	3	4	5	6	7	DK
Council of Europe (CoE)	1	2	3	4	5	6	7	DK
Interpol	1	2	3	4	5	6	7	DK
Europol	1	2	3	4	5	6	7	DK
Group of 8 (G-8)	1	2	3	4	5	6	7	DK
Asia Pacific Economic Cooperation (APEC)	1	2	3	4	5	6	7	DK
Organization for Economic Co-operation and Development (OECD)	1	2	3	4	5	6	7	DK

28. In your opinion, which of the following techniques are associated with CYBERTERRORISM? (1 = no association; 7 = strongly associated)

Unauthorized access	1	2	3	4	5	6	7	DK
Illicit tampering with files or data (unauthorized copying, modification, or destruction)	1	2	3	4	5	6	7	DK
Computer-mediated espionage	1	2	3	4	5	6	7	DK
Violations against privacy	1	2	3	4	5	6	7	DK
Virus	1	2	3	4	5	6	7	DK
Trojan horses	1	2	3	4	5	6	7	DK
Worms	1	2	3	4	5	6	7	DK
Denial of service attacks	1	2	3	4	5	6	7	DK

Money laundering	1	2	3	4	5	6	7	DK
Fraud	1	2	3	4	5	6	7	DK
ID theft	1	2	3	4	5	6	7	DK
Forgery	1	2	3	4	5	6	7	DK
Child pornography	1	2	3	4	5	6	7	DK
Communication	1	2	3	4	5	6	7	DK
Propaganda	1	2	3	4	5	6	7	DK
Fund raising	1	2	3	4	5	6	7	DK
Recruitment	1	2	3	4	5	6	7	DK

Thank you very much for participating.

APPENDIX B

THE CORRELATION MATRIX OF THE ITEMS OF A SCALE- VCF

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	**ECONOMY**	1																
2	**INDUSTRY**	0.59	1															
3	**INTUSER**	0.38	0.4	1														
4	**ISP**	0.32	0.39	0.59	1													
5	**TELECOMM**	0.33	0.29	0.45	0.56	1												
6	**AUTOMATE**	0.34	0.36	0.46	0.57	0.74	1											
7	**MONEY**	0.2	0.35	0.26	0.31	0.4	0.45	1										
8	**CAPACITY**	0.11	0.09	0.32	0.31	0.32	0.28	0.41	1									
9	**MOTIVATI**	0.17	0.15	0.32	0.31	0.34	0.42	0.23	0.3	1								
10	**AWARE**	0.06	0.12	0.11	0.2	0.19	0.24	0.27	0.16	0.1	1							
11	**COOP**	0.07	0.01	0.13	0.06	0.07	0.22	-0.04	-0.03	0.15	0.32	1						
12	**AGENCY**	-0.01	-0.03	-0.09	0.01	0.12	0.26	-0.02	0.02	0.04	0.27	0.44	1					
13	**SUBSLAW**	0.1	0.01	0.05	0.1	0.14	0.17	0.11	0.01	0.05	0.18	0.26	0.31	1				
14	**PROCLAW**	0.03	0.04	0.02	0.17	0.12	0.11	0.07	0.07	0.06	0.06	0.33	0.13	0.53	1			
15	**BILATE**	-0.09	-0.06	-0.02	-0.02	0.22	0.18	0.1	0.13	0.13	0.07	0.03	-0.03	0.08	0.04	1		
16	**MULTI**	0.12	0.07	0.08	0.04	0.13	0.14	0.03	-0.06	0.07	0.18	0.27	0.16	0.28	0.17	-0.01	1	
17	**FREEDOM**	-0.07	-0.05	-0.12	-0.25	-0.31	-0.41	-0.13	-0.04	-0.36	-0.17	-0.37	-0.32	-0.23	-0.27	-0.11	0.05	1

APPENDIX C

THE ROTATED COMPONENT MATRIX- VCF

	Component				
	1	2	3	4	5
MOTIVE)	.551	.104	.226	-.155	.008
SMEAN(CAPACITY)	.742	-.143	-.218	.040	.025
SMEAN(ECONOMIC)	.107	.845	.017	.138	-.042
SMEAN(INDUSTRY)	.180	.822	-.049	.106	-.042
SMEAN(INT_USER)	.524	.537	.028	-.114	.069
SMEAN(ISP)	.625	.467	.042	-.151	.174
SMEAN(TELECOMM)	.691	.327	.143	.011	.098
SMEAN(AUTOMATE)	.690	.354	.337	.023	.054
SMEAN(MONEY)	.668	.103	-.171	.349	-.026
SMEAN(AWARE)	.358	-.077	.396	.439	-.112
SMEAN(FREEDOM)	.013	-.098	-.696	.068	-.082
SMEAN(COOP)	.028	.029	.711	.122	.265
SMEAN(AGENCY)	.074	-.140	.690	.260	.052
SMEAN(MULT1)	-.048	.171	.125	.630	.285
SMEAN(BILATERA)	-.054	.044	.079	.821	.050
SMEAN(SUBSLAW)	.088	-.051	.218	.266	.755
SMEAN(PROCLAW)	.069	.006	.107	-.002	.885

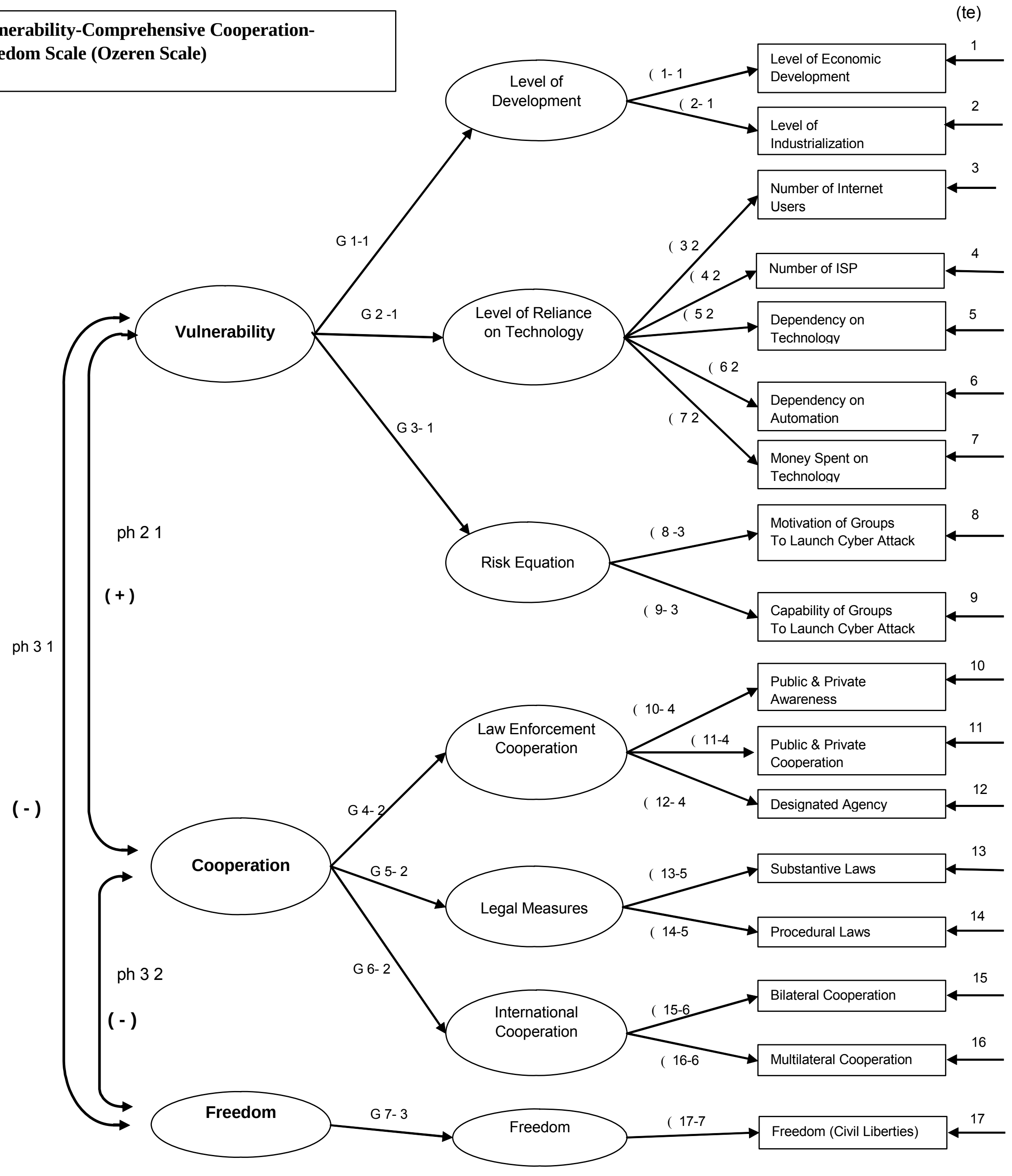
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.a Rotation converged in 10 iterations.

APPENDIX D

THE VULNERABILITY-COMPREHENSIVE COOPERATION-FREEDOM SCALE

(OZEREN SCALE)

Vulnerability-Comprehensive Cooperation-Freedom Scale (Ozeren Scale)



G - Gamma
(ΞLambda

APPENDIX E

THE CORRELATION MATRIX FOR CYBERCRIME AND CYBERTERRORISM OVERLAPS

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	Unauthorized Access	1.00																
2	Tampering Data	0.68	1.00															
3	Espionage	0.51	0.55	1.00														
4	Privacy	0.40	0.39	0.43	1.00													
5	Virus	0.57	0.66	0.48	0.42	1.00												
6	Trojan	0.58	0.67	0.44	0.37	0.81	1.00											
7	Worms	0.50	0.66	0.39	0.42	0.73	0.85	1.00										
8	Denial of Service Attack	0.46	0.53	0.37	0.30	0.60	0.61	0.63	1.00									
9	Money Laundering	0.37	0.37	0.42	0.42	0.39	0.30	0.36	0.42	1.00								
10	Fraud	0.28	0.22	0.31	0.51	0.37	0.34	0.36	0.37	0.66	1.00							
11	ID Theft	0.50	0.42	0.36	0.46	0.48	0.45	0.45	0.48	0.56	0.65	1.00						
12	Forgery	0.39	0.25	0.34	0.29	0.38	0.33	0.31	0.44	0.57	0.68	0.69	1.00					
13	Child Pornography	0.28	0.32	0.28	0.50	0.35	0.33	0.31	0.31	0.40	0.57	0.48	0.47	1.00				
14	Communication	0.34	0.32	0.39	0.35	0.33	0.22	0.19	0.33	0.44	0.50	0.33	0.39	0.45	1.00			
15	Propaganda	0.21	0.10	0.36	0.25	0.21	0.12	0.15	0.18	0.50	0.39	0.28	0.31	0.24	0.70	1.00		
16	Fund Raising	0.40	0.18	0.29	0.19	0.20	0.17	0.22	0.26	0.55	0.39	0.41	0.36	0.20	0.53	0.71	1.00	
17	Recruitment	0.35	0.20	0.44	0.13	0.33	0.19	0.20	0.27	0.48	0.31	0.33	0.36	0.09	0.51	0.66	0.74	1.00

The covariance matrix is calculated and used in the analysis.

APPENDIX F

THE ROTATED COMPONENT MATRIX OF OVERLAPS BETWEEN CYBERCRIME TECHNIQUES AND CYBERTERRORISM

Rotated Component Matrix[a]

	Component		
	1	2	3
Unauthorized Access	.706	.171	.281
Tampering Data	.843	.135	.092
Espionange	.548	.171	.396
Privacy	.363	.575	.073
Virus	.827	.245	.130
Trojan	.882	.209	.006
Worms	.838	.230	.025
Denial of Service Attack	.662	.302	.145
Money Laundering	.234	.585	.495
Fraud	.131	.849	.267
ID Theft	.373	.692	.213
Forgery	.195	.725	.267
Child Pornography	.190	.759	.036
Communication	.155	.372	.657
Propaganda	.019	.206	.858
Fund Raising	.113	.180	.851
Recruitment	.197	.037	.869

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

[a] Rotation converged in 5 iterations.

REFERENCES

About NISCC. (2001). What is NISCC's remit?. Retrieved March 01, 2004 from http://www.niscc.gov.uk/aboutniscc/index.htm.

About NISCC. (2001). EARG. Retrieved March 02, 2004 from http://www.niscc.gov.uk/aboutniscc/index.htm.

Accelerated Promotions. (2004). Anti terrorism technology: Carnivore surveillance system. Retrieved March14, 2004 from http://accelerated-promotions.com/consumer-electronics/usa-patriot-act-carnivore.htm.

Akdeniz, Y., Taylor, N., & Walker, C. (2001). BigBrother.gov.uk: State surveillance in the age of information and rights. *Criminal Law Review, 1*, 73-90.

Andreano, F. P. (1999). The evolution of federal computer crime policy: The ad hoc approach to an ever-changing problem. *American Journal of Criminal Law, 27*(81), 82-103.

APEC Shanghai Declaration. (2002). The Fifth APEC ministerial meeting on telecommunications and information industry. Retrieved February 13, 2004 from http://www.apecsec.org.sg/apec/ministerial_statements/sectoral_ministerial/telecommunications/2002.html

Aras, B., & Bacik, G. (2002). The mystery of Turkish Hizballah. *Middle East Policy, 9* (2), 147-160.

Area of Security. (2003). Europol Convention: European Police Office. Retrieved March 13, 2004 from http://europa.eu.int/scadplus/leg/en/lvb/l14005b.htm

Article 17 of Directive 95/46. (1999). Security of processing. Retrieved October 22, 2004 from http://europa.eu.int/ISPO/legal/en/dataprot/directiv/chap2.html#HD_NM_37

Bakewell, E. J., Koldaro, M., & Tija, J. M. (2001). Computer crime. *The American Criminal Law Review, 38,* (3), 481-524.

Ballard, J. D., Hornik, J. G., & McKenzie, D. (2002). Technological facilitation of terrorism: Definitional, legal and policy issues. *American Behavioral Scientist, 45*, (6), 989-1016

Barkham, J. (2001). Cyberwar, cybercrime, and cyberterrorism: A bibliographic essay. *American Society of International Law*. Retrieved March 10, 2004 from http://www.asil.org/barkham.pdf

Barkley, J. (1994). Security in open systems. *NIST Special Publication 800, 7.*

Baron, R. M. F. (2002). A critique of the international cybercrime treaty. *The Catholic University of America, 10*, 263.

Bendrath, R. (2002). Cyber-Violence: The future of violence? Presentation at a Conference Derogation, exclusion, violence- analyses on the dangers to a humane republic. University Belfield, Institute for Multi-Disciplinary Violence and Conflict Research.

Berinato, S. (2002). The truth about cyberterrorism. *CIO Magazine.* Retrieved on April 13, 2004 from http://www.cio.com/archive/031502/truth.html

Blume, P. (2000). Data protection of law offenders. In D. Thomas & B. D. Loader (Eds). *Cybercrime: Law enforcement, security, and surveillance in the information age* (pp. 193-218). New York: Routledge

Borland, J. (1998). Analyzing the threat of cyberterrorism. *TechWeb*. Retrieved Spetember 13, 2002 from http://www.techWeb.com/ wire/story/TWB19980923S0016

Brenner, S. W. (2001). Defining cybercrime: A review of State and federal law. In R. D. Clifford (Ed). *Cybercrime: The investigation, prosecution, and defense of a computer-related crime* (pp. 11-68). Durham, NC: Carolina Academic Press.

Brenner, S. W., & Goodman, M. D. (2002). In defense of cyberterrorism: An argument for anticipating cyber-attacks. *University of Illinois Journal of Law, Technology & Policy, 1,* (57).

Carter, D. (1995). Computer crime categories. *FBI Law Enforcement Bulletin, 64,* (7), 21.

Carter, D., & Bannister, A. J. (2000). Computer crime: A forecast of emerging trends. Paper presented at the Academy of Criminal Justice Sciences Annual Meeting, New Louisiana.

CCIPS. (1998). Press release: Juvenile computer hacker cuts off FAA tower. Retrieved March 12, 2003 from http://www.cybercrime.gov/juvenilepld.htm

CERT. (2002). Computer emergency response team. Retrieved April 12, 2002 from http://www.cert.org/

CERT/CC. (2003). Introduction to the CERT® coordination center. Retrieved on February 02, 2003 from http://www.cert.org/faq/cert_faq.html#A1

CHIP. (2002). CHIP computer hacking and intellectual property fact sheet. Retrieved March 03, 2004 from http://www.cybercrime.gov/chipfact.htm

Cilluffo, F. J. (2000). Cyber-Attack: The national protection plan and its privacy implications. *Journal of Homeland Security*. Retrieved from http://www.homelandsecurity.org/journal/articles/displayArticle.asp?article=12

Cilluffo, F. J., & Pattak, P. B. (2000). Bad guys and good stuff: When and where will the cyber threats converge? *DePaul Business Law Journal, (12),* 131- 169.

Cline, A. (2000). Prioritization process using Delphi technique. *Carolla White Paper.* Retrieved April 10, 2004 from http://www.carolla.com/wp-delph.htm

CNN. (1996). Hacked CIA Web site still down. Retrieved January 15, 2004 from http://www.cnn.com

Cohen, W. (2000). The need for Homeland defense. Retrieved November 22, 2004 from http://www.homelandsecurity.org/showQuotes.asp?AuthorID=14

Collin, B. C. (1997). Cyberterrorism from virtual darkness: New weapons in a timeless battle. Retrieved from http://www.counterterrorism.org

Communication System. (2000). The electronic intrusion threat to national security and emergency preparedness (NS/EP) internet communications an awareness document. Retrieved from http://www.ncs.gov/library/reports/electronic_intrusion_threat2000_final2.pdf

Comrey, A. L. (1988). A *first course in factor analysis*. New York: Academic Press

Computer Fraud and Abuse Act. US CODE: Title 18,1030.

Conway, M. (2002). Reality bytes: Cyberterrorism and terrorist 'Use' of the Internet. *First Monday,7,* (11). Retrieved April 04, 2004 from http://firstmonday.org/issues/issue7_11/conway/index.html

Convention for the Protection of Human Rights and Fundamental Freedoms. (1950). *Right to respect for private and family life.* Retrieved March 16, 2004 from http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

Convention on Cybercrime. (2001). Retrieved December 05, 2004 from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Cooper, H. H. A. 2001. Terrorism: The problem of definition revisited. *American Behavioral Scientist 44,* 881-893.

Council of Europe. (1981). *Convention for the protection of Individuals with regard to automatic processing of personal data.* Retrieved February 15, 2004 from http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

Council of Europe. (2001). Convention on cybercrime. Retrieved February 15, 2004 from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Council of Europe. (2002). Council resolution on the implementation of the eEurope 2005 action plan. Retrieved March 12, 2004 from http://europa.eu.int/information_society/eeurope/2005/index_en.htm

Council of Europe. (2003). What is what? Retrieved December 10, 2004 from http://www.coe.int/T/E/Com/About_Coe/whatswhat.asp

Council of Europe. (2003). The Council of Europe's Member States. Retrieved December 15, 2004 from http://www.coe.int/T/E/Com/About_Coe/Member_states/default.asp

Crime & Policing. (2000). The Regulation of Investigatory Powers Act (RIPA). Retrieved March 20, 2004 from http://www.homeoffice.gov.uk/crimpol/crimreduc/regulation/

Critical Foundations: Protecting America's Infrastructures (1997). The report of the President's Commission on Critical Infrastructure Protection*.* Retrieved January 19, 2004 from http:// www.pccip.gov

Cue´llar, M. F. (2001). Past as prologue: International aviation security treaties as precedents for international cooperation against cyberterrorism and cybercrimes. In A. D. Sofaer, & S. E. Goodman (Eds.), T*he transnational dimension of cybercrime and terrorism* (pp. 91-124)*.* Stanford, CA: Hoover Institution Press Publication.

Cuhls, K. (2003). Delphi method: Principles, process, examples, case studies. A Paper presented at training course Technology foresight for practitioners. 6-10 October 2003, Prague, Czech Republic.Retrieved April 11, 2004 from http://www.unido.org/file-storage/download/?file%5fid=16959

Cybercrime European Commission (2001). Network and information security: Proposal for a European policy approach. Retrieved March 14, 2004 from http://europa.eu.int/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf

Cybercrime European Commission. (2004). Anti cybercrime legislative proposals on Council table. Retrieved March 14, 2004 from http://europa.eu.int/comm/justice_home/fsj/crime/cybercrime/wai/fsj_crime_cybercrime_en.htm

Cybercrime European Commission. (2004). What steps is the EU taking to combat cyber-crime? Retrieved March 14, 2004 http://europa.eu.int/comm/justice_home/fsj/crime/cybercrime/wai/fsj_crime_cybercrime_en.htm

Dallas News. (2003). *Secret Service creating team to fight cybercrime.* Retrieved February 03, 2004 from http://www.crime-research.org/eng/news/2003/06/Mess1706.html

Davis, E. S. (2003). A world wide problem on the World Wide Web. International responses to transnational identity. *Washington University Journal of Law & Policy.*

Definitions Information Society. (2003). Establishment of a European network and information security agency. Retrieved March 12, 2004 from http://europa.eu.int/scadplus/leg/en/lvb/l24153.htm

Denning, D. E. (1997). Encryption and evolving technologies as tools of organized crime and terrorism. National Strategy and Information Center

Denning, D. E., & William E. B. (1997). *Encryption and evolving technologies as tools of organized crime and terrorism,* Washington, D.C.: US Working Group on Organized Crime (WGOC), National Strategy Information Center.

Denning, D. E. (2000). Cyberterrorism. *Global Dialogue.* Retrieved from http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc

Denning, D. E. & Baugh, W. E. Jr. (2000). *Hiding crimes in cyberspace. Cybercrime: Law enforcement, security, and surveillance in the information age.* NY: New York, Routedge Taylor & Francis Group.

Department of Defense. (2004). DOD dictionary of military terms. Retrieved March 09, 2005 from http://www.dtic.mil/doctrine/jel/doddict/

DeVellis, R. F. (1991). S*cale development: Theory and applications*. Newbury Park, CA: Sage Publications.

Devost, M. G. (1995). National security in the information age. Master thesis. University of Vermont.

Devost, M. G., Houghton, B. K., Pollard, N. A. (1996). Information terrorism: Can you trust your toaster?. Retrieved September 13, 2002 from htttp://www.terrorism.com

Ditzion, R., Geddes, E., & Rhodes, M. (2003). Computer crimes. *American Criminal Law Review, 40*, 285-336.

Doyle, C. (2002). The USA PATRIOT Act: A legal analysis. *Congress Research Service.*

Drozdova, E.(1999). Emerging international consensus on cybercrimes: results of global cyber law survey of fifty countries in Africa, the Americas, Asia, Europe, the Middle East, and Oceania. Paper presented at the conference on international cooperation to combat cybercrime and terrorism, December 6-7, 1999, Hoover Institution, Stanford University.

Drozdova, E. A. (2001). Civil liberties and security in cyberspace. In A. D. Sofaer, & S. E. Goodman (Eds.), T*he transnational dimension of cybercrime and terrorism* (pp. 183-220). Stanford, CA: Hoover Institution Press Publication.

Dunham, G. S. (2002). Carnivore, The FBI’ S e-mail surveillance system: Devouring criminals, not privacy. *Federal Communication Law Journal 54.*

18 USC. 2703. *Requirements for Governmental Access.*

Electronic Privacy Information Center – EPIC. (2002). FBI's CARNIVORE system disrupted anti-terror investigation Internal memo calls over-collection of data part of "pattern" showing "inability of the FBI to manage" foreign intelligence wiretaps. Retrieved March 15, 2004 from http://www.epic.org/privacy/carnivore/5_02_release.html.

Enders, W. and Sander, T. (1993). The effectiveness of antiterrorism policies: A Vector-Autoregression-Interventon analysis. *American Political Science Review 87*, 829-844.

Enos, L. (2001). Cybercrime fighters lobby Congress for support. Retrieved February 25, 2004 from http://www.ecommercetimes.com/perl/story/11231.html

Entrust. (2003). Entrust applauds DHS establishment of National cyber security division. Retrieved February 28, 2004 from http://www.entrust.com/news/files/06_06_03.htm

EPIC. (1998). Critical infrastructure protection and the endangerment of civil liberties an assessment of the President's Commission on Critical Infrastructure Protection (PCCIP). Retrieved March 15, 2004 from http://www.epic.org/security/infowar/epic-cip.html

Evers, J. (2000). The Netherlands adopts cybercrime pact. Retrieved December 20, 2004 from http://www.theexperiment.org/articles.php?news_id=980

EU Business. (2003). European network and info security agency set for January launch. Retrieved March 04, 2004 from http://www.eubusiness.com/topics/Rd/EUNews.2003-11-21.2957

EU News Report. (2003). new European agency for network and information security. Retrieved March 01, 2004 from http://www.iwar.org.uk/news-archive/2003/10-08-6.htm

EUROPA. (2002). Europol Convention: European Police Office. Retrieved March 07, 2004 from http://europa.eu.int/scadplus/leg/en/lvb/l14005b.htm

European Union at a glance. (2003). Retrieved March 10, 2004 from http://europa.eu.int/abc/index_en.htm

Europol. (2003). Fact Sheet on Europol. Retrieved October 11, 2003 from http://www.europol.eu.int/index.asp?page=facts

Federal Standard. (1996). Telecommunications: Glossary of telecommunication terms. Retrieved January 15, 2004 from http://www.its.bldrdoc.gov/fs-1037/dir-028/_4148.htm

FBI National Computer Crime Squad (1999). Retrieved from http://www.fbi.gov

FIRST. (2002). The forum of incident response and security teams: A description. Retrieved on March 05, 2004 from http://www.first.org/about/first-description.html

Fisher-Hubner, S. (2000). Privacy and security at risk in the global information society. In D. Thomas & B. D. Loader (Eds), *Cybercrime: Law enforcement, security, and surveillance in the information age* (173-192). New York: Routledge

Fogleman, R. R.& Widnall, S. E. (2002). Cornerstones of Information Warfare. Retrieved October 16, 2002 from http://www.af.mil/lib/corner.html

Ford, J. (2002). Selected definitions of vulnerability from the literature. Retrieved March 10, 2004 from http://www.uoguelph.ca/~jford01/Vulnerability/Vuln_defintions.pdf

Freedom House. (2003). Freedom in the World 2003: Survey methodology. Retrieved April 13, 2004 from http://www.freedomhouse.org/research/freeworld/2003/methodology.htm

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. Great Britain: Pearson Education Limited.

G7-G8 Summit in Okinawa. (2000). Okinawa Charter on Global Information Society. Retrieved March 10, 2004 from http://europa.eu.int/comm/external_relations/g7_g8/intro/global_info_society.htm

G-8 Countries Combat Organized Crime. (1999). Retrieved March 14, 2004 from http://canada.justice.gc.ca/en/news/nr/1999/g8pr.html

G8 Path Information Center. (1999). G-8 countries combat organized crime. Retrieved March 04, 2004 from http://www.library.utoronto.ca/g7/adhoc/justice99.htm

Galley, P. (1996) Computer terrorism: What are the risks? *Science, Technology and Society Swiss Federal Institute of Technology.* Retrieved October 19, 2002 from http://www.home.ch/~spaw1165/infosec/sts_en/iw.html

Glave, J. (1998). Pentagon hacker exposed by justice department. Retrieved from http://www.wired.com/news/technology/0,1282,11030,00.html

Glossary of Vulnerability Testing Terminology (2003). Retrieved March 10, 2004 from http://www.ee.oulu.fi/research/ouspg/sage/glossary

Goodman, S. E. (2001). International cooperation to protect civil aviation against cybercrime and cyberterrorism. In A. D. Sofaer, & S. E. Goodman (Eds), T*he* *transnational dimension of cybercrime and terrorism* (pp. 69-72). Stanford, CA: Hoover Institution Press Publication.

Grabosky, P. N., & Smith, R. G. (1998). C*rime in the digital age*. Riverwood, Australia: Ligare Pty Ltd.

Gordon, t. J. (1994). Delphi method. *AC/UNU Millennium Project Futures Research Methodology Futures Research Methodology*. Retrieved October 11, 2004 http://www.futurovenezuela.org/_curso/5-delphi.pdf

Group of 8. (2003). Retrieved December 04, 2003 from http://www.privacyinternational.org/issues/cybercrime/

Hancock, B. (2003). G8 thinks about cybercrime: It is about time too. *Computer & Security, 19,* (5), 405-407

Hatcher, L. (1994). *A step-by-step approach to using the SAS(R) system for factor analysis and structural equation modeling*. Cary, NC: SAS Institute.

High Tech Computer Crime Task Force. (2002). Retrieved on 03/06/2004 from http://www.cyber-response.org/home.html

Hoffman, B. (2004). Defining terrorism. In R. D. Howard, & R. L. Sawyer (Eds.), *Terrorism and counterterrorism: Understanding the new security environment, readings and interpretations* (Chp. 1), New York: McGraw-Hill Companies, Inc.

Homeland Security Press Release. (2003). *Ridge creates new division to combat cyber threats.* Retrieved March 08, 2004 from http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0173.xml

Icove, D. & Seger, K. (1995). *Computer crime: A crimefighter' s handbook*. Sebastopol, CA: O'Reilly & Associates, Inc.

Illinois Institute of Technology (2004). *The* Delphi Method. Retrieved April 12, 2004 from http://www.iit.edu/~it/delphi.html

Information Society. (2003). Establishment of a European network and information security agency. Retrieved March 12, 2004 from http://europa.eu.int/scadplus/leg/en/lvb/l24153.htm

International Working Group. (2002). Common position on data protection aspects in the draft convention on cyber-crime of the Council of Europe. Retrieved December 15, 2004 from http://www.datenschutz-berlin.de/doc/int/iwgdpt/cy_en.htm

Internet Systems Consortium. (2004). Internet domain host count. Retrieved March 28, 2004 from http://www.isc.org/

Interpol. (2003). *Interpol an overview*. Retrieved March 14, 2004 from http://www.interpol.int/Public/Icpo/FactSheets/FS200101.asp

Interpol. (2003). Interpol's contribution to combating information technology crime. Retrieved March 14, 2004 from http://www.interpol.int/Public/TechnologyCrime/default.asp

Interpol. (2003). *Regional working parties.* Retrieved March 14, 2004 from http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#europa

Iuris, A. P. (1997). Information terrorism. In A. Humphreys (Ed), T*errorism a global survey: A special report for Jane's intelligence*. *Review and Jane's sentinel*, Alexandria, VA.: Jane's Information Group.

Jacobson, H. & Green, R. (2002). Computer crimes. *American Criminal Law Review, 39*, (273).

Kelly, J. (2000). US Acquires reputed terrorism guide. *USA Today*.

Keyser, M. (2003). The Council of Europe Convention on cybercrime.

Transnational Law & Policy 12, (2), 287-325.

Konrad, R. (2000). New *documents shed more light on FBI's "Carnivore".* Retrieved March 14, 2004 from http://news.com.com/2100-1023-248762.html?legacy=cnet

Kovacich, G. L. & Boni, W. C. (2000). H*igh-technology crime investigator's handbook:Wworking in the global information environment*. Woburn, MA: Butterworth- Heinemann.

Laqueur, W. (1977). *Terrorism*. London, United Kingdom: Weidenfeld and

Nicolson.

Lawson, S. M. (2002). Information warfare: An analysis of the threat of cyberterrorism towards the US critical infrastructure. *SANS Institute*. Retrieved March 22, 2004 from http://www.sans.org/rr/papers/index.php?id=821

Lewis, A. J. (2002). *Assessing the risks of cyberterrorism, cyber war and other cyber threats.* Center for Strategic and International Studies, Washington, D.C. Retrieved April 17, 2003 from http://www.csis.org/tech/0211_lewis.pdf

Lewis, A. J. (2003). Introduction. In J. A. Lewis (Ed.), *Cyber security: Turning national solutions into international cooperation* (pp. xi-xxiii). Washington D.C.: The CSIS Press:

LISREL, (1998). Retrieved January 19, 2005 from http://www.utexas.edu/cc/stat/software/lisrel/

Ludwig, B. (1997). Predicting the future: Have you considered using the Delphi Methodology? *Journal of Extension*. Retrieved April 11, 2004 from http://www.joe.org/joe/1997october/tt2.html

Lukasik, S. J. (2001). Current and future technical capabilities. In A. D. Sofaer, & S. E. Goodman (Eds), *the transnational dimension of cybercrime and terrorism* (pp. 125-184). Stanford, CA: Hoover Institution Press Publication.

Mark, R. (2003). Now open: National cyber security division. Retrieved February 27, 2004 from http://www.internetnews.com/bus-news/article.php/2218761

Marotta, E. (2001). Europol's Role in anti-terrorism policing. In M. Taylor & J. Horgan (Eds.), *The future of terrorism* (pp. 14-18). London, England: Frank Cass & Co. Ltd.

McDonald, B. L. (2004). Counterfeit Access Device and Computer Fraud Abuse Act of 1984. Retrieved February 10, 2004 from http://www.wrf.com/publications/ppt/privacy/cases/cntrfit_accs.asp

McAuliffe, W, (2001). Council of Europe approves cybercrime treaty. Retrieved March 25, 2004 from http://www.wildernesscoast.org/bib/treaty-by-date.html

Merl, S. R. (2001). The Internet communication standards for the 21st century: International terrorism must force the US to adopt "Carnivore" and new electronic surveillance standards. *Brooklyn Journal of International Law, 27.*

Meeting of G8 Ministers of Justice and Home Affairs. (2003). Public statement by the ministry of the interior, internal security and local freedoms. Retrieved January o5, 2005 from http://www.g8.fr/evian/english/navigation/news/meeting_of_the_justice_and_home_affairs_ministers_of_the_g8_in_paris__on_5_may_2003.html

Miastkowski, S. (2000). Renamed love letter worm still spreads. Retrieved

February 10, 2004 from http://www.pcworld.com/news/article/0,aid,16582,00.asp

Monge, P. & Fulk, J. (1999). Communication technology for global network organizations. In G. Desanctis and J. Fulk (Eds)., *Shaping organizational form: communication, connection,and community*, Thousand Oaks, CA: Sage Publications.

MS-ISAC. (2003). Establishment of the Multi-State ISAC. Retrieved February 25, 2004 from https://disasterhelp.gov/portal/jhtml/general/about_msisac.jhtml;jsessionid=E4YPI11QZ5BA5QFIAAICFEY

Nachmias, D., & Nachmias, C. F. (2000). *Research methods in social sciences*. New York: Worth Publishers.

National Communications Systems. (2000). Electronic intrusion threats to national security and emergency preparedness (NS/EP) Internet Communications. Retrieved September 23, 2004 http://www.ncs.gov/ncs/Reports/electronic_intrusion_threat2000_final2.pdf

National Cyber Security Leadership Act. (2003). Retrieved March 25, 2004 from http://www.theorator.com/bills108/s187.html

National Institute of Justice, (US Department of Justice). (1989). C*omputer crime: Criminal justice resource manual*.

National Strategy to Secure Cyberspace*.* (2003). Retrieved from http://www.dhs.gov/interWeb/assetlibrary/National_Cyberspace_Strategy.pdf

NCFTA. (2004). Retrieved March 08, 2004 from http://www.ncfta.net/about_ncfta.html

Nelson, A. M. (2002). Using a modified Delphi methodology to develop a competency model for vet practitioners. *A paper presented in Partial Fulfillment of the Requirements of RM502E- Advanced Study in Research Methods,* December 24, 2002. Retrieved April 11, 2004 from http://home.earthlink.net/~amkefossen/AJN/publications/RM502EPaper.pdf

Nicholson, L. J., T. F. Shebar, & M. R. Weinberg. (2000). Computer crimes. *American Criminal Law Review, 37,* (207): 207-259.

NIPC. (2001). *History.* Retrieved from http://www.nipc.gov/about/about3.htm

Nitzberg, S. (2002). Conflict and the Computer: Information warfare and related ethical issues. Shrewsbury, NJ: Tele Information Protection Solutions.

Nosworthy, J. D. (2000). Implementing information security in the 21st century- Do you have the balancing factors? *Computer & Security, 19*, 337-347.

Occhipinti, J. D. (2003). *the politics of EU police cooperation: Toward a European FBI?*. London, England: Lynne Rienner Publishers.

OECD. (2002). *Guidelines for the Security of Information Systems and networks: Towards a culture of security*. Retrieved March 13, 2004 from http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf

Osher, S. A. (2002). Privacy, computers and the PATRIOT Act: The Fourth Amendment isn’t dead, but no one will ensure it. *Florida Law Review,* 954.

Parker, D. B. (1999). Sharing infrastructures: Cybercrime intelligence. Paper presented at a conference on cybercrime and terrorism*,* Stanford, CA.

PCCIP. (1997). President’s Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America’s Infrastructures, Washington, D.C. Retrieved February 14, 2003 from http://www.pccip.gov/report_index.html

Persico, B. A. (1999). Under siege: The jurisdictional and interagency problems of protecting the national information infrastructure. *Common Law Conspectus, 7*, 153-171.

Poe, S., & Tate C.N. (1994). Repression of human rights to personal integrity in the 1980s: A global analysis. *American Political Science Review, 88*, 853-872.

Pollitt, M. M. (1997). A Cyberterrorism: Fact or fancy? Proceedings of the 20th national information systems security conference.

Poole, P. S. (2000). ECHELON: America's secret global surveillance network. Retrieved February 23, 2004 from http://fly.hiwaay.net/~pspoole/echelon.html

Principles on transborder access. (1999). Retrieved March 04, 2004 from http://canada.justice.gc.ca/en/news/nr/1999/data.html

Putnam, T. L. & Elliott, D. D. (2001). International response to cybercrime. In A. D. Sofaer, & S. E. Goodman, (Eds). *The transnational dimension of cybercrime and terrorism* (pp. 35-68). Stanford, CA: Hoover Institution Press Publication.

Reynaldo, J. & Santos, A. (1999). Cronbach's Alpha: A tool for assessing the reliability of scales. *Journal of Extension, 37,* (2). Retrieved February 09, 2005 from http://www.joe.org/joe/1999april/tt3.html

Rotenberg, M. (2000). Cyber attack: The national protection plan and its privacy implications. Retrieved March 13, 2004 from http://www.epic.org/security/cip/EPIC_testimony_0200.pdf

Rotenberg, M. (2002). Modern studies in privacy law: Foreword: Privacy and secrecy after September 11. *Minnesota Law Review, 86,* 1115.

Rodota, S. (2003). Europe and cyber security. In James A. Lewis (Eds), *Security: Turning national solutions into international cooperation* (pp. 79-89). Washington D.C.: The CSIS Press.

Sassen, S. (2004). Echelon, Big brother is watching you?. Retrieved February 15, 2004 from http://www.hardwareanalysis.com/action/printarticle/1280/

Schemmel, T. J. (2003). Justice in a changed world: wwwstopcybercrime.com: How the USA PATRIOT Act combats cybercrime. *William Mitchell Law Review, 29*, 921-949.

Schwartau, W. (1996). C*haos on the electronic superhighway: Information warfare*. New York, NY: Thunder’s Mouth Press.

searchSecurity.com. (2002). Carnivore. Retrieved March 13, 2004 from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci508347,00.html

Security Council 4792nd Meeting. (2003). Fight against terrorism would be long with no short cuts, Counter-terrorism Committee Chairman Tells Security Council. Retrieved February 07, 2004 from http://www.un.org/News/Press/docs/2003/sc7823.doc.htm

Selin, S. (1996). Governing cyberspace: The need for an international solution. *Gonzaga Law Review, 32,* 365-388.

Shannon, C.E., & Weaver, W. (1949). *The mathematical theory of communication.* Urbana: University of Illinois Press.

Slambrouck, P. Van (1998). Cyber threat how serious? *The Christian Science Monitor.*

Sloan, L. D. (2001). Echelon and the legal restraints on signals intelligence: A need for reevaluation. *Duke Law Journal.*

Soo Hoo, K., Goodman, S., & Greenberg, L. (1997). Information technology and the terrorist threat. *Survival, 39,* (3), 135–155.

Sofaer, A. D. & Goodman, S. E. (2001). Cybercrime and security: The transnational dimension. In A. D. Sofaer, & S. E. Goodman, (Eds). *The transnational dimension of cybercrime and terrorism* (pp. 1-34). Stanford, CA: Hoover Institution Press Publication

Speeches and testimony. (1998). Testimony by director of Central Intelligence George J. Tenet before the Senate Committee on Government Affairs. Retrieved March 10, 2004 from http://www.cia.gov/cia/public_affairs/speeches/1998/dci_testimony_062498.html

Statement of the electronic frontier foundation. (2000). Before the subcommittee on the constitution of the Committee on the Judiciary United States House of Representatives The fourth amendment and carnivore. Retrieved March 14, 2004 from http://www.eff.org/Privacy/Surveillance/Carnivore/20000728_eff_house_carnivore.html

Statistics on Cyber-terrorism. (2000). Retrieved October 02, 2002 from http://www-cs.etsu.edu/gotterbarn/stdntppr/stats.htm

Stephenson, P. (2000*). Investigating computer-related crimes*. New York: CRC Press LLC

Stern, J. (2000). Pakistan’s jihad culture. *Foreign Affairs*, 115–126.

Strauss, A. Y. (2002). A constitutional crisis in the digital age: Why the FBI' s "Carnivore" does not defy the fourth amendment. *Yeshiva University Cardozo Arts & Entertainment Law Journal, 20,* 231- 258.

Sussmann, M. A. (1999). The critical challenges from international high-tech and computer-related crime at the millennium. *Duke Journal of Comparative & International Law(9).*

Taylor, R. W., & Loper, D. K. (2003). Computer crime. In C. R. Swanson, N. C. Chamelin, & L. Territo (Eds), *Criminal Investigation* (8th ed). New York: McGraw-Hill Companies, Inc.

Taylor, R. W., Caeti, T. J., Loper, K., Fritsch, E. J., & Liederbach, J. (2006). *Digital crime and digital terrorism.* Upper Saddle River, NJ: Prentice Hall.

TELMIN. (2002). Statement on the security of information and communications infrastructures. Retrieved February 15, 2004 from http://www.tiaonline.org/policy/regional/asia/telmin5_statement.pdf

Tenet, G.J. (1998). Testimony before the Senate Committee on Government Affairs. Retrieved March 10, 2004 from http://www.cia.gov/cia/public_affairs/speeches/1998/dci_testimony_062498.html

Tenth United Nations Congress. (2000). Crimes related to computer networks. Retrieved February 05, 2004 from http://www.uncjin.org/Documents/congr10/10e.pdf

Thomas, T. L. (2003). Al Qaeda and the Internet: The danger of cyberplanning parameter. *Parameters XXXIII, 1,* 112-123.

Thomas, D., & Loader, B. D. (2000). Introduction. In D. Thomas & B. D. Loader (Eds), C*ybercrime: Law enforcement, security, and surveillance in the information age* (pp. 1-14). New York: Routledge

TIA Online. (2002). APEC Telecommunications working group. Retrieved on February 19, 2004 from http://www.tiaonline.org/policy/regional/asia/apec_tel.cfm

2002/58/Ec Of The European parliament and of the council (2002). Retrieved March 15, 2004 from http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

United Nations Universal Declaration of Human Rights. Article 12. Retrieved http://www.unhchr.ch/udhr/lang/eng.htm

Universal Declaration of Human Rights, art 19

US Department of Justice. (2003). Frequently asked questions and answers Council of Europe convention on cybercrime. Retrieved March 15, 2004 from http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm#QA1

US Secret Service. (2002). Retrieved February 03, 2004 from http://www.ustreas.gov/usss/mission.shtml

US State Department. (1999). Patterns of global terrorism. Retrieved from

http://www.state.gov/

Varma, D. J. (1999, September 21). Sub-continent in Web war. I. T. Retrieved September 18, 2002 from htttp://it.mycarrer.com.au/comuniations/19990921/A12383-1999sep20.html

Vatis, M. A. (1998). Cybercrime, transnational crime, and intellectual property theft. Before the Congressional Joint Economic Committee Washington, D.C. Retrieved March 24, 2004 from http://www.fbi.gov/congress/congress98/vatis.htm

Vatis, M. A. (2000). The NIPC's international response to cyber attacks and computer crime. Before the House Committee on Government Affairs Subcommittee on government management, information, *and technology* Washington, D.C. Retrieved March 24, 2004 from http://www.fbi.gov/congress/congress00/vatis072600.htm

Vatis, M. (2003). International cyber-security cooperation: Informal bilateral models. In James A. Lewis (Eds), Security: *Turning national solutions into international cooperation* (pp. 1-12). Washington D.C.: The CSIS Press:

Verton, D. (2003). B*lack ice: The invisible threat of cyber-terrorism*. Emeryville, CA: The McGraw-Hill.

Warlaw, G. (1994). The democratic framework. In Charters (ed.) T*he deadly sin of terrorism: Its effect on democracy in six countries* (pp.5-12). CT: Greenwood Publishing Group, Inc.

Weimann, G. (2004). How modern terrorism uses the Internet. Retrieved March 25, 2004 from http://www.usip.org/pubs/specialreports/sr116.pdf

Weber, A. M. (2003). Annual review of law and technology: VIII. Foreign & International law: A cyberlaw cybercrime: The Council of Europe's convention on cybercrime. *Berkeley Technology Law Journal, 18,* 425.

Weles, E. (n. d). Draft Council of Europe Cybercrime convention upset civil rights bodies. Computer Fraud and Security.

Westby, J. R. (2003). International strategy for cyberspace security. *American Bar Association.*

Westin, A. (1967). *Privacy and freedom*. New York.

Wiederin, S. Hoefelmeyer, R. & Phillips, T. (2002). The cyber-world isn't always malicious. Retrieved October 14, 2002 from http://www.orldcom.com

Wiles, J. (2002). Cybercrime-alerts - Secret Service electronic crimes task force We need you. Retrieved January 03, 2004 from http://www.mail-archive.com/cybercrime-alerts@topica.com/msg00627.html

Wilson, C. (2003). Computer attack and cyberterrorism: Vulnerabilities and policy issues for Congress. *Congressional Research Service ˜The Library of Congress.* Retrieved June 10, 2004 from http://www.fas.org/irp/crs/RL32114.pdf

What is Project ECHELON. (2002). Answers to frequently asked questions (FAQ) about Echelon. Retrieved March 04, 2004 from http://archive.aclu.org/echelonwatch/faq.html

Whiteman, H. H. (2001). Cyberterrorism and civil aviation. In A. D. Sofaer, & S. E. Goodman, (Eds). *The transnational dimension of cybercrime and terrorism* (pp. 73-90). Stanford, CA: Hoover Institution Press Publication.

White House. (1998). Combating terrorism: Presidential decision directive 62. Retrieved February 28, 2004 from http://fas.org/irp/offdocs/pdd-62.htm

WordReference.com Dictionary. (2000). Definition of vulnerability. Retrieved from March 10, 2004 from http://www.wordreference.com

Zanini, M. & Edwards, S. J. A. (2001). The Networking of terror in the information age. In J. Arquilla & D. Ronfelt (Eds), *Networks and netwars,* (pp.29-60). Santa Monica, CA: RAND Corporation.