



NOTRE DAME UNIVERSITY

Faculty of Political Science, Public Administration &
Diplomacy

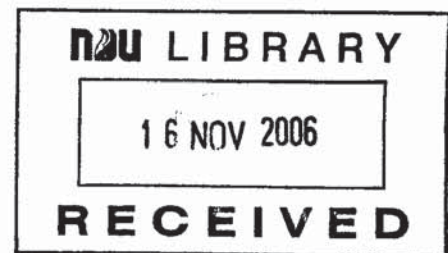
Spring 2006

M.A. Thesis

CYBERTERRORISM: FUTURE TRENDS AND IMPACT

By

Imad Youssef



CYBERTERRORISM: FUTURE TRENDS AND IMPACT

By

Imad M. Youssef
ID# 990737

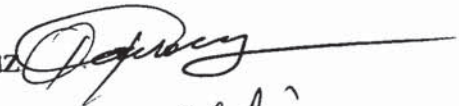
Submitted to the Faculty of Political Science, Public Administration
and Diplomacy

In Partial Fulfillment of the Requirements for the Degree of Master of
Arts in International Affairs and Diplomacy

Notre Dame University, Louaize - Lebanon
2006

Approved by: **Thesis Advisor**

Dr. Akl Kairouz



First Reader

Dr. George Labaky



Second Reader

Dr. Eugene Sensenig-Dabbous



Table of Contents

EXECUTIVE SUMMARY.....	1
CHAPTER 1: INTRODUCTION.....	3
Background.....	3
Problem Statement.....	6
Methodology.....	8
Data.....	10
Limitations.....	10
CHAPTER 2: TERRORISM AND CYBERSPACE.....	12
Information Warfare.....	12
Command and Control Warfare.....	15
Infrastructure Warfare.....	18
Cyberspace.....	18
Origins of Terror.....	19
Defining Terrorism.....	20
Motivations of Terrorism.....	22
Terrorists and Cyberspace.....	24
CHAPTER 3: CYBERTERRORISM.....	26
Definition of Cyberterrorism.....	26
Expert Opinions.....	28
Security Experts “Camps”.....	30
Differentiating between Cyberterrorism and Hacktivism.....	34
Cyberterrorism Attractiveness.....	34
Vulnerability.....	35
Anonymity.....	38
Availability and Low Cost.....	39
Safety and Expertise.....	39
Variety of Targets.....	40
Female Participation.....	38
CHAPTER 4: CYBERTERRORISM THREAT.....	41
Motivations.....	41
Actors.....	42
Targets.....	45
Understanding the Threat.....	47
Possible Impact.....	49
Assessing the Threat.....	49

CHAPTER 5: METHODS OF ATTACK.....	51
Risk Factors.....	51
Types of Cyberterrorism.....	51
Possible Cyberterrorism Scenarios.....	52
Computer Attack Methods.....	56
Physical Attack.....	57
Electronic Attack.....	57
Cyberattack.....	58
Cyberterrorist Tools.....	59
CHAPTER 6: CONCLUSIONS AND RECOMMENDATIONS.....	64
Shifting Definition of Terrorism.....	67
Impact of Cyberterrorism on the Future.....	68
Demassification.....	68
New State Sponsors.....	68
Targeted Message.....	69
Rise of Disruption.....	70
New Tools for Attacker and Defender.....	71
Combating the Threat.....	72
State's Response to the Problem.....	74
Government Response to the Problem.....	74
Commercial Response to the Problem.....	77
Government / Commercial Response.....	78
International Response to the Problem.....	80
Privacy and Personal Freedom.....	82
International Agencies.....	83
Difficulties in Implementing Security Measures.....	84
Recommended Strategies to Counter Cyberterrorism.....	85
Futuristic Perspective.....	88
BIBLIOGRAPHY.....	90

EXECUTIVE SUMMARY

As the world enters the information age, countries has undertaken extensive study of the "Revolution in Military Affairs" and information warfare. This thesis examines the implications of information warfare tactics and techniques for terrorism. It explores the possibility that computers may revolutionize terrorism.

Two concepts are often embodied in academic definitions of terrorism: violence and terror. By adding information warfare techniques, the definition of terrorism could be expanded to include "cyberviolence," the destruction or manipulation of computer information. The "violence" done to this information, which is becoming increasingly important for security and economic prosperity, should be considered terrorism. Although terrorists might turn from destruction to the creation of mass disruption, the addition of information warfare tactics to the terrorist's arsenal does not imply a less destructive future. Should terrorists choose to target critical computer systems they could create destruction and disruption simultaneously.

While there have been many studies in the separate areas of terrorism, cyberterrorism, and cyber warfare, it is hoped that by putting them together we can establish the significance of the cyberterrorism threat. We have verified firstly that cyberterrorists are likely to have similar motivations with terrorists in desiring violence and destruction to meet their political or other causes. While there have been no clear acts of cyberterrorism to date, this could be the result of lack of ability to carry out the attacks in cyberspace and not the feasibility. However, this situation is not expected to remain as is, given the advantages offered by cyberterrorism against forces and societies that rely heavily on information technology. Moreover, many terrorist and state sponsored groups are seeing the asymmetrical benefits of information warfare as a means of redressing the conventional military imbalance of the U.S. vis-à-vis the rest of the world.

This thesis reaches several conclusions regarding information age terrorism. First, the definition of terrorism must change to include cyberviolence and disruption. Second, the terrorist threat is likely to become more "demassified," with smaller numbers of individuals able to create disruption via virtual worldwide organizations. Third, the pattern of state sponsorship is likely to change. While old state sponsors will continue to exist, terrorists may turn to poorer states or choose to fund themselves via information warfare crime. Fourth, information warfare techniques may afford terrorists the ability to target their message more effectively. Fifth, the nature of offense and defense in cyberspace does not mirror that of "conventional" offense and defense in the physical world.

In light of these conclusions, the best method to counter information age terrorism is a joint government/industry program of defensive measures that will increase the effort required for computer disruption while simultaneously diminishing the potential returns offered by this new form of terrorism. At the same time, a strategy that is based on some form of international cooperation is recommended to counter cyberterrorism.

Finally, the lack of actual examples of cyberterrorism (although a blessing) makes it hard to pinpoint specific methods, tools or desired outcomes for policy recommendations.

There is much literature available on the methods, motivations and psychology of terrorists, but little is available in comparison for cyberterrorists. What is available tends to be confined to arguments on the nature of the threat, rather than the threat itself. Thus more work will need to be done on studying the vulnerability of critical information systems, their potential exposure to cyberterrorists and the damage they could do if they gained access.

However, just as the events of 9/11 caught the world by surprise, so could a major cyberassault. Therefore we can neither deny its threat nor dare to ignore it.

CHAPTER 1

INTRODUCTION

1. Background

“We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable - to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb.”¹

This statement applies to all developed and developing countries although impact and consequences may vary from one society into another.

Ours is an age of computers, of automated information systems. We are able to access, distribute, and store incredibly large quantities of information in very little time. It is said that information is power. However, our dependence on automated information systems goes much deeper than power-wielding. Virtually all of the infrastructure and the institutions on which we depend, the government, military, communications systems, transportation, utilities, financial systems, emergency medical services, and more, depend on automation. In the financial world, for example, very few transactions actually involve the physical transfer of money; what we transfer is information about money. As we have harnessed automation and created systems to facilitate and quicken our private, corporate, and governmental transactions, those systems have become increasingly vulnerable. We now face the danger of having our information infrastructures destroyed, altered, or incapacitated. Too often those vulnerabilities go unnoticed until disruption or catastrophe occurs.

¹ National Research Council, System Security Study committee, *Computers at Risk; Safe Computing in the Information Age* (Washington D.C.: National Academy Press, 1991), 7.

Attacks on our information systems may come from a wide range of potential aggressors, from other nations to teenage hackers. One of the greatest threats comes from cyberterrorism.

Cyberterrorism is the convergence of cyberspace (the computer-based world of information) and terrorism (premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents).

The combination of two of the great fears of the late twentieth century are combined in the term “cyberterrorism”. The fear of random, violent victimization segues well with the distrust and outright fear of computer technology. Both capitalize on the fear of the unknown, and people distrust things that they are unable to control.

Terrorism, with its roots in the periphery of mainstream society, is feared. It is perceived as being random, incomprehensible and uncontrollable. Groups with obscure names and origins impact catastrophically on the innocent. It is, in fact, designed to terrorize and be feared. That is its real power.

Modern technology in itself is feared from two perspectives. First, it is by definition arcane. It is complex, abstract and indirect in its impact on individuals. Because computers do things that used to be done by humans, there is a natural fear related to a loss of human control over the machine. Some people believe that, in the future, technology has the ability to become the master, and humanity the servant.

The popular press in general has further fueled the fires by “hying” the concept of convergence. According to the press, one is lead to believe that all of the functions controlled by individual computers will converge into a singular system. Further support for this scenario is developed by the increase in “connectivity”. Many people conclude that the entire world will soon be controlled by a single computer system.

Ironically, these same people subjectively understand that since computers are products of, and operated by human beings, they are not reliable in either the mechanical or the logical sense. Certainly, there can be no doubt as to the immense benefits humanity draws from computer technology. With any technology, be it telephones or automobiles, there are risks, most of which can be managed. It is precisely the "unmanageable" risks that are feared. This thesis will address the risks and possibilities in combining terrorism and computers.

As the world enters the 21st century, the information revolution will continue to propel the world into the "third wave" of development². The shift from an industrial economy and society to one focused on information and its transfer will characterize the third wave. Alvin Toffler claims in his book *The Third Wave and War and Anti-War* that the way a state wages war is similar to how it makes wealth. This comparison might be applied to terrorism and revolutionary violence.

Lewis Gann in his book *Guerrillas in History*, provides an overview of substate violence across history³. Occasionally, substate groups possess weapons superior to those of the state. Substate actors, unless being supplied by a superior power, normally possess weapons that are inferior to those of the target state itself. They often use weapons stolen from, or discarded by the governments. As the technology, complexity, and lethality of weapons systems increased during the twentieth century, these weapons were even more tightly controlled by the state, widening the gap between state and substate "firepower." However, as the world shifts into the information age, this disparity in weapons decreases, with individuals and substate groups now able to control information manipulation tools that were once restricted to the state.

² Alvin Toffler. *The Third Wave*. New York: William Morrow and Co., 1980.

³ Lewis Gann, *Guerrillas in History* (Stanford CA: Hoover Institution Press, 1971)

As the world shifts into the "third wave," where information and its control are rapidly becoming the most important worries and preoccupation for the advancing societies of the first world, will humanity see a corresponding shift by terrorists and revolutionaries to using "information warfare" weapons and techniques to press their case?

While terrorists and revolutionaries have "kept pace with the advance of technology, consistently exploiting new and lesser defended targets, (embassies, airplane hijackings, hostage taking, airplane bombing) they have done so through evolution, not innovation. Bruce Hoffman contends, "... innovation does occur mostly in the methods used to conceal and detonate explosive device, not in the tactics or in the use of non-conventional weapons (i.e., chemical, biological, or nuclear)"⁴.

This thesis explores the implications of information age terrorism. There has already been a shift toward "information warfare" across other parts of the "conflict spectrum" with these techniques being used by criminals, agents of espionage, revolutionaries, and armies engaged in warfare. A corresponding shift in terrorist tactics has yet to occur. While some argue that it is merely a matter of time before we are faced with a major information warfare attack, there are several reasons why terrorists may not actively pursue these techniques.

2. Problem Statement

The world has entered a new millennium with a number of the negative phenomena, having taken steady growth of criminality and terrorism. Speaking about integration and globalization of world processes, it is necessary to recognize that terrorism has been so far successful. Terrorism breaks the frontiers and gets transnational and organized nature. Terror crimes, alongside traditional crimes, have adopted a new quality. New kinds of

⁴ Bruce Hoffman, *Responding to Terrorism Across the Technological Spectrum* (Santa Monica: Rand corporation, 1994), p.6.

terrorism - information and computer (cyber) terrorism have appeared. Terrorist groupings have mastered cyberspace, using practically boundless opportunities of mass media.

With the help of the Internet, the terrorists can destroy an infrastructure of corporate, regional or national computer network by means of a conclusion out of operation control systems or subsystems. They can get the non-authorized access to the confidential information and propagandize extremist ideas justifying terrorist activity through «strike for freedom and independence». Cyberterrorism is one of the most dangerous kinds of terrorism now, and its consequences can be really catastrophic.

This onset of the information-dependent third wave provides opportunities for spectacular gains and serious losses for individuals, corporations, and states. It is within this world that the cyberterrorist will operate. In the same manner that terrorists have exploited widely accepted technology such as dynamite and the airplane (for bombing and hijacking), they may exploit the tools of the "information age" to bring their case before the citizens of the world. Consequently, the world must prepare itself to counter this threat in an age where the old AT&T slogan, "reach out and touch someone" takes on a sinister new meaning. To defend against a threat, one must understand its critical elements. Cyberterrorism, like "conventional" terrorism, will strive to change the mind of its intended audience. It will be perpetrated by groups to have an effect on population as it utilizes different means to this end. A cyberterrorist will strive, not to disrupt physical reality directly (as an exploding bomb would) but rather to disrupt the normal functioning of computers and other information systems. As a result, this cyberspace disruption would cause a disruption in the physical world, as the violence that is normally associated with terrorism may shift into "cyberspace" where bits and bytes, not people, are victims. To

understand the potential shift in terrorism, this thesis splits information age terrorism into two categories: conventional terrorism, and cyberterrorism.

Analysis will focus on the costs and benefits of information warfare techniques for terrorism and the changes that they may force in the definition of terrorism. Despite the inevitable warnings that "the sky is falling," the utility of information warfare attacks may actually be lowest in the "terrorist" portion of the conflict continuum. This does not, however, obviate the need to address the threat. The information warfare threat is real and might cause serious damage in the future. While it may not fit conventional definitions of terrorism, security expert Neal Pollard correctly states that, "to ignore computer abuse as a political crime, simply for the sake of academic purity, is impractical, dangerous esoteric snobbery."⁵ As we will see in this examination of the "brave new world" into which we are headed, there are reasons both for and against terrorism shifting toward information warfare (IW) tactics in the third wave.

3. Methodology

Much of the current hype about cyberterrorism is built on fear of the unknown.

The purpose of this thesis is to move beyond simple speculation to more structured analysis of the threat and appropriate responses. We do have sufficient reasons to believe that cyberterrorism will become a more significant national security concern in the near future. The means and the motives are available but employing digital attacks to achieve specific terrorist objectives still faces multiple obstacles. But it is just a matter of time, if we didn't take any additional preventive actions to protect our systems, cyberterrorists will be successful in removing these obstacles and just as the events of 9/11 caught the world by surprise, so could a major cyberassault.

⁵ Neal Pollard, "Computer Terrorism and the Information Infrastructure," in *InfowarCon '95 Conference Proceedings: Held in Arlington VA 7-8 September 1995*, Carlisle PA: National Computer Security Association, 1995, p. 6.

In order to fully appreciate this new growing threat, it is necessary to discuss several aspects of cyberterrorism. First, it is critical to discuss exactly what cyberterrorists are capable of accomplishing. Second, it is necessary to determine which groups are likely to utilize cyberterrorism to accomplish their goals. Third, it is important to discuss the reasons that these groups would resort to cyberterrorism. Fourth, it is central to determine who bears the responsibility of defending against cyberterrorism. Fifth, it is imperative to discuss what governments and private corporations can do to counter cyberterrorism and protect themselves. Finally, it is important to discuss the difficulties that corporations might face in attempting to counter cyberterrorism.

Therefore, in order to understand and assess the reality of the threat, we have used the following outline in this thesis.

The next chapter discusses terrorism as the root of cyberterrorism. The difficulty in defining terrorism has created different ideas of what cyberterrorism could be. We explore the makeup and motivations for terrorism to see how they subsequently lend themselves to cyberterrorism. Chapter 3 discusses the definitions of cyberterrorism and explores the advantages for terrorists employing cyberterrorism. Different perceptions are considered in an attempt to find principles of the threat posed by cyberterrorism inside chapter 4. In doing so we discuss the motivations, actors and targets of cyberterrorism. Chapter 5 examines several possible hypothetical situations posed by experts in the field of cyberterrorism, and highlights the different weapons that cyberterrorists might use in their attack. Finally, chapter 6 concludes by summarizing the key issues and conclusions drawn in this thesis, discusses various measures and responses that must be adopted to combat the threat of cyberterrorism, and postulates areas for future work.

4. Data

While the world has yet to suffer an acknowledged cyberterrorist attack, several computer crimes and incidents reveal the power of information warfare. The trend toward information warfare appears uniform across the conflict continuum with the exception of terrorism. The cases used in this thesis were selected from unclassified literature. They were selected for their ability to highlight the potential threat posed by information warfare tactics and techniques. The ongoing information revolution, coupled with the sensitive nature of computer systems for both business and defense, ensure that this is not a comprehensive examination of all computer related incidents but it is sufficiently broad to cover the entire low intensity spectrum of conflict.

Exploring the role that computers and networks have played in terrorist actions since 1970 will identify the trend in terrorism toward infrastructure warfare, and cyberterrorism.

5. Limitations

Information warfare is a concept that embraces many elements beyond simply attacking computers and communications networks. However, primarily focus will be on the portion of information warfare that deals with computers and their associated networks and only tangentially cover such topics as psychological operations. The revolutionary changes caused by computers present the possibility of revolutionary changes in the targets and conduct of terrorism.

In order to discuss the role of computers with respect to terrorism, we must understand their limits. Short of electrocuting one's self with the power supply or being so unfortunate as to walk under a falling machine, computers cannot, directly, kill or injure. That is not to say that there are not indirect risks of physical harm, nor direct risks of

economic injury. Computers may communicate to other devices that can cause death or injury. The direct risks of economic injury are perhaps the most significant of all the risks.

CHAPTER 2

TERRORISM AND CYBERSPACE

Terrorism is evolving to the worst in the 21st century. Information warfare, the current "hot topic" for the military, along with Command and Control Warfare, C2W, are two concepts that some argue will create or accelerate a "Revolution in Military Affairs." These ideas also suggest the possibility of a "Revolution in Terrorism Tactics and Remedies." Information age terrorism may take on two distinct forms: conventional terrorism, and cyberterrorism. While conventional terrorism continues to rely on physical violence, terrorists acquisition of high technology information warfare capabilities will allow a shift toward tactics focused on disruption and destruction all together. Information age terrorism, will employ weapons radically different from those used in the conventional one. This shift toward disruption in cyberspace, through the use of new technological weapons and with lesser reliance on the physical violence, may force a new definition of the classic conception of terrorism.

1. Information Warfare

The definition of Information Warfare has been extensively debated in the international press. The US Department of Defense has a classified definition of Information Warfare, but the public debate on the subject will be sufficient for the purposes of this thesis. Information Technology experts Drs. John Arquilla and David Ronfeldt capture the broad nature of information warfare in *Cyberwar is Coming!* In this work, they address the military and civilian, as well as the offensive and defensive components of information warfare. The spectrum of conflict is split into "netwar" and "cyberwar". They define "netwar" in these words:

“Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage or modify what a target population knows or thinks it know about itself and the world around it. A netwar may focus on public or elite opinion, or both, It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks.”⁶

By contrast, they consider Cyberwar the military cousin of netwar. While a diverse group of actors can conduct netwar at a variety of levels, cyberwar exists exclusively in the military realm.

“Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting, if not destroying, information and communications system, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, and so forth. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself.”⁷ Cyberterrorism, while utilizing some cyberwar tactics, lies in the realm of netwar.

Through an examination of cyber and netwar, Arquilla and Ronfeldt highlight the increasing importance of information control for military victory in the information age. In the future, information control may also be critical for successful terrorism or counter-terrorism activities.

The National Defense University in the United States has posited a working definition of Information-Based Warfare that outlines the offensive and defensive components of information warfare. It highlights the applicability of information as both a target and a weapon across the conflict spectrum:

“Information-based Warfare is an approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage especially in the joint and combined environment. Information-based Warfare is both offensive and defensive in nature – ranging from measures that prohibit the enemy from exploiting information to corresponding measures to assure the integrity, availability, and interoperability of friendly information assets... While ultimately military in nature, Information-based Warfare is also waged in political, economic, and

⁶ J. Arquilla & D. Ronfeldt, (Eds). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND, 2001, p. 144.

⁷ J. Arquilla & D. Ronfeldt, (Eds). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND, 2001, p. 146.

social arenas and is applicable over the entire national security continuum from peace to war and from 'tooth to tail.' Finally, Information-based Warfare focuses on the command and control needs of the commander by employing state-of-the-art information technology such as synthetic environments to dominate the battlefield."⁸

In his Advanced Concepts and Technology paper, "What is Information Warfare?" Martin Libicki, researcher on IW, outlines seven specific forms of information warfare:

command and control warfare, information-based warfare, electronic warfare, psychological warfare, hacker warfare, economic information warfare, and cyber warfare⁹. While most of these forms of conflict fall into the military realm, each of them is applicable to terrorism in the emerging information age.

There are two components of Information Warfare. First, your own information must be protected and trusted at all levels. During collection, the accuracy of the information received must be verified. During processing, information must be defended against theft, destruction and modification. Finally, during distribution of information to other elements, the means of transfer must be secure to ensure that information arrives at its destination in an unaltered format. The defensive portion of information warfare aims to ensure information confidentiality, integrity, and availability. Second, an effort to disrupt the information gathering, processing, and distribution functions of the enemy must be undertaken. The effort to manipulate the information of the enemy while protecting your own takes place on several levels. Information warfare is not just about computers sending electrons from point A to point B. It is not only the hardware and software but the "wetware" (computer slang for a human brain) that is critical to information warfare. The fundamental goal of warfare is to change the mind of the enemy and convince him to do

⁸ Working definition recognized by the Information Resources Management College of the National Defense University as of 11/16/93

⁹ Martin Libicki, *What is Information Warfare?* (Washington DC: National Defense University Press, August 1995), Internet <http://www.ndu.edu/ndu/inss/actpubs/act003/a003cont.html>.

one's will. The goal of information warfare is to accomplish this through the manipulation of the enemy's ability to control information.

While perceived as "less bloody", and "not really fighting", physical destruction can play an important role in information warfare. One of the tools of information warfare is infrastructure warfare, in which the infrastructure of an enemy is targeted with both "regular" technology (bombs, missiles, troops on the ground) and "information" technology, the attempt to utilize malicious software to disrupt and alter enemy telecommunications without physical destruction and to induce a psychological state in the enemy that will lead him to "do your will."

Information warfare is the quest to disrupt, disable, destroy, or modify an adversary's information and information systems while simultaneously protecting your own. While electronic attacks of a network via computer and modem are the "cleanest" means of information warfare, physical attacks on the network's infrastructure are also possible and should always be considered as an open option terrorists.

a. Command and Control Warfare (C2W)

The Chairman of the Joint Chiefs of Staff Memorandum of Policy Number 30, "Command and Control Warfare," identifies Command and Control Warfare (C2W) as the military component of information warfare¹⁰. Both terrorism and information warfare cover a larger spectrum of conflict than simply command and control, but the fundamentals of both are rooted in the ability to affect the thinking of the enemy. As a result, there are several useful parallels between C2W and terrorism in the information age.

¹⁰ Chairman of the Joint Chiefs of Staff, *Memorandum of Policy Number 30* (Washington D.C., 8 March 1993), p.3.

The "five pillars" of C2W (electronic warfare, physical destruction, operations security, psychological operations, military deception) are designed to help classify a military operation. Each of these pillars is also applicable to terrorism. An understanding of C2W is useful in examining both the internal and external working of terrorist organizations. Properly and accurately performing in all five areas enhances the ability of a terrorist organization to mount an offensive against its opponent. If one of the areas is weak, it can be exploited by the organization under attack and used to disrupt or destroy a terrorist organization. While the defending group targets the weakness of a terrorist group, the latter will target any perceived weakness of the defending group. This continual targeting and retargeting of actual and perceived weaknesses is the basis for determining the type of strategy that a defending group will use. If a terrorist organization is seen to have several glaring weaknesses in its Command and control (C2) structure, the defending group may find it most effective to pursue an offensive strategy in an effort to destroy the terrorist. If, however, the terrorist's C2 networks are hard to identify, target, and attack, the only option open to the defender is to establish a defensive strategy in cyberspace whereby the costs of attack are increased, and the benefits reduced. New technology has affected the C2W "balance of power" between terrorists and authorities. Counter-terror forces now have the capability to more closely monitor communications channels using increasingly sophisticated computers. Terrorists, however, can also use increasing computer power and publicly available encryption technology to secure their member's communications. Terrorists, in the past, operated in what J. Bowyer Bell described as a "dragonworld," where they were forced to live in fear of constant government surveillance¹¹. With the rise of secure voice and data communications; i.e., Pretty Good Privacy (PGP) for E-mail and PGPphone for Internet voice communication encryption,

¹¹ Bowyer Bell, "Aspects of the Dragonworld: Covert Communications and the Rebel Ecosystem," *International Journal of Intelligence and Counterintelligence*, 3-1 (Spring 1989): 15-43.

terrorists can emerge from the dragonworld. Conventional defensive C2W restrictions no longer exist for the information age terrorist, who can devote more time to offensive C2W and other acts without constantly worrying about secure communication.

Defense in cyberspace bears some resemblance to defense in the physical world. The most effective defense is to isolate a computer or network completely from the rest of cyberspace. If there is no access into a computer system because it has been removed from all networks, defending it will be easier. The primary concern for such a "stand alone" computer is the possibility of an authorized user inserting some form of malicious software. The problems associated with trusted individuals "going over" to the enemy camp have existed throughout history and are hardly unique to the information age. The second form of defense is similar to a point defense with access to a computer system challenged by an authentication and identification procedure. In this case, the computer asks for and verifies the password provided by the user. While "static" passwords that do not change are vulnerable to attack by random guessing, technology, such as the "smart card," exists to provide a constantly changing set of passwords that are nearly impossible to crack. Increasing the transmission paths available to data is akin to a defense in depth. As the data paths increase, the ability of an enemy to attack all of them successfully decreases. When one communication path is destroyed or degraded, data will instantaneously switch to one of the other available paths with no impact to the end user. The use of encryption to ensure the confidentiality and integrity of data consists of electronically scrambling, and thus armor plating, the data that is to be sent through cyberspace. Even if the data is intercepted and copied, its contents remain unknown to the enemy until they can decrypt it, which may take years.

The ever shifting nature of conventional terrorism causes difficulty for defender states who attempt to pursue an offensive strategy against terrorism. The inability to target and

attack small terrorist groups, plus the myriad of defensive techniques available to both state and substate actors will only increase the problems associated with countering conventional terrorists as to exploit the principles of information warfare.

2. Infrastructure Warfare

Infrastructure Warfare is an attack against the physical components of a state's networks, such as power and water distribution, telecommunications networks, rail lines, and roads. As related to information warfare, infrastructure warfare is defined as a physical attack on system components that would subsequently influence the ability to process or transmit information. As such, bombing the telephone, switching building that serve a specific location to isolate it from the rest of the world, or destroying the electrical grid that supplies power to a targeted system, would constitute infrastructure warfare. Terrorists have already proven that they are capable of physical destruction via numerous airline, building, and infrastructure bombings. Terrorists design these events to "send a message" to the world and to terrorize specific target audiences. Terrorist infrastructure warfare may utilize the same tools, such as bombs, with which the terrorist is familiar, but for a different purpose. Instead of attempting to "make a statement" by bombing a physical target for a physical impact, a terrorist group can bomb infrastructure targets to cause cascading failures (loss of electricity leads to loss of computers which leads to loss of communications, etc.) within a targeted system. These secondary effects of the bombing, which may only destroy equipment without causing personnel casualties, are the primary goal of the terrorist in infrastructure warfare.

3. Cyberspace

Cyberspace is a term coined to capture the essence of "where" computers work. While the physical components of computers and their networks are necessary for cyberspace to

exist, it is more than merely the sum of these parts. Winn Schwartau defines cyberspace as follows:

“Cyberspace is that intangible place between computers where information momentarily exists on its route from one end of the global network to the other. When little Ashley calls Grandmother, they are speaking in Cyberspace, the place between the phones. Cyberspace is the ethereal reality, infinity of electrons speeding down copper or glass fibers at the speed of light from one point to another. Cyberspace includes the air waves vibrating with cellular, microwave and satellite communications. According to John Perry Barlow, cofounder of Electronic Frontier Foundation, Cyberspace is where all of our money is, except for the cash in our pocket”¹².

The Defense Information Systems Agency, a branch of the US Department of Defense charged with conducting defensive information warfare defines cyberspace as:

“The electronic environment formed by the aggregate of global computing and telecommunications resources. Cyberspace is a virtual 5th dimension characterized by: no geographic, national, or temporal boundaries, no ownership, laws, or identity cards”¹³.

Cyberspace does not have a physical reality. One cannot physically "enter" cyberspace. It consists of the "virtual world" through which all electronic transactions take place. It is in this realm that the cyberterrorist will operate.

4. Origins of Terror

Although terrorism is one of the most ubiquitous words in the current affairs, political or conflict news of the present day, few agree on exactly what terrorism is. As the famous cliché goes: “one man’s terrorist is another man’s freedom fighter”. Hence, terrorists never call themselves as such, and will go to great lengths to evade such connections.¹⁴ Arguably, and unsurprisingly, the roots of terrorism could be found in religion, during the Middle East of the 1st Century. The Sicarii were an active Jewish group which set out to

¹² Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994), p. 49.

¹³ Robert Ayers (Chief, Information Warfare Division, DISA) presentation, "DISA and Information Warfare," to InfoWarCon'95, 7-8 September 1995, Washington, D.C.

¹⁴ Bruce Hoffman. *Inside Terrorism*. Paperback Edition, London: Indigo 1999, p 134.

target other Jews who collaborated with the Romans¹⁵. The Zealots were also a Jewish group that targeted the Romans and Greeks. These executions would typically be carried out in broad daylight in the presence of others. The objectives for such action were in part to inspire insurrection among the Jews against the Roman occupiers, and in part to send a message to the Roman authorities themselves. In his study of terrorism, Huffman showed how the understanding and perception of terrorism changed over the centuries¹⁶.

Terrorism was popularized during the French Revolution toward the end of the 18th Century with the *régime de la terreur*, which gave us the English word “terror”. It had then a positive connotation as it was the system by which order was established during an anarchical period in France.

Over time, however, its use became associated with anti-monarchy, anarchy, revolution, anti-establishment, violence and anti-government activity. The modern meaning of the word only emerged after the Second World War when terror was used to describe the anti-colonialistic, nationalistic and separatist revolts that were typically violent.

a. Defining Terrorism

An expert on terrorism, Alex P. Schmid, made an attempt to provide a broad definition of terrorism when he examined over a hundred definitions in 1984, and came up with 23 different characteristics that appeared in these definitions. The five most frequently occurring ones were (1) violence and force; (2) political; (3) fear and terror emphasized; (4) threat; (5) (psychological) effects and (anticipated) reaction. The United Nations in the 1970s tried in vain to come to an agreement on what was and what was not terrorism. Many of its members held the view that struggles against occupation or oppression, or

¹⁵ Walter Reich. *Understanding Terrorist Behavior*. Origins of Terrorism, Walter Reich (Ed). Baltimore: John Hopkins University Press, 1998, p.3.

¹⁶ Bruce Hoffman. *Inside Terrorism*. Paperback Edition, London: Indigo 1999 p. 136.

struggles for liberation, freedom or independence, even if they include acts of violence, should not be considered as terrorism¹⁷. Fueling the debate further is the media, who have been inconsistent in their description of events. A reason for the difficulty in defining terrorism is that terrorism is a political label¹⁸. Thus to label a group or act as “terrorist” effectively places a moral judgment on it, denies it political status, acceptance or recognition, and frames the consciousness of the masses.

In the light of the many events since the 1970s that involved all if not more than the five characteristics mentioned, the United Nations Office on Drugs and Crime (UNODC) has since adopted an academic consensus definition provided by Alex P. Schmid in 1988:

“Terrorism is an anxiety-inspiring method of repeated violent action, employed by clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby – in contrast to assassination – the direct targets of violence are not the main targets.

The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organizations), (imperiled) victims, and main targets are used to manipulate the main target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought”.

The short legal definition proposed by the same author in 1992 defined an act of terrorism as “the peacetime equivalent of a war crime”, since it is generally agreed that terrorists are known by a refusal to be bound by international rules of warfare and codes of conduct. However, the validity of this short form is now somewhat uncertain with a blurring of the lines between wartime and peacetime actions, especially with “the war against terror” undertaken by the U.S. military and its allies in Afghanistan and Iraq. The U.S. Homeland Security Act of 2002 defined terrorism as follows:

“The term “terrorism” means any activity that— (A) involves an act that— (i) is dangerous to human life or potentially destructive of critical infrastructure or key

¹⁷ Bruce Hoffman. *Inside Terrorism*. Paperback Edition, London: Indigo 1999, p. 140.

¹⁸ Martha Crenshaw. *Terrorism in Context*. Pennsylvania State University Press, 1995, p. 4.

resources; and (ii) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and (B) appears to be intended—(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping”.

The agencies of the U.S. government continue to provide their own definitions of terrorism, each reflecting their organizational characteristics and focus. They describe terrorism by the following definitions.

“The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives”. (*U.S. Federal Bureau of Investigation*)

“The calculated use of violence or the threat of violence to inculcate fear, intended to coerce or intimidate governments or societies as to the pursuit of goals that are generally political, religious or ideological”. (*U.S. Department of Defense*)

“Premeditated, politically motivated violence perpetuated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience”¹⁹. (*U.S. State Department*)

b. Motivations of Terrorism

There are probably as many motivations for terrorism as there are definitions. The three most common motivations are political, religious, and ideological. Of these, political motivation is the most prominent as it features in most definitions of terrorism. The direct causes of terrorism are unjust discrimination, a lack of opportunity for political participation, elite dissatisfaction, and precipitating events²⁰. The first factor stems from grievances experienced by one subgroup in the population, such as an ethnic minority, due to unequal rights or the desire to gain a separate, independent state. Grievances alone do not generate terrorist reactions, but they are more likely to occur if the discriminations are deemed to be unjust, and if violence is considered as a viable means to redress the

¹⁹ U.S. Department of State, *Patterns of Global Terrorism, 2003*, [<http://www.state.gov/s/ct/rls/pgrtrpt/2001/html/10220.htm>].

²⁰ Martha Crenshaw. *The Causes of Terrorism*. Comparative Politics, pp 381-385. July 1981

situation. Regimes that suppress opportunities for political participation, either by denying access to power or by persecuting dissidents, are bound to create dissension. In such situations are the seeds for revolutionary terrorism sown. Terrorism is also likely to occur when the young elite find themselves at odds with society and its general passivity. Student unrest is one such example of elite dissatisfaction, and may lead on to terrorist incidents. The last factor cited by Crenshaw derives from instances such as the use of unexpected and unusual force in response to protest or reform attempts by the government. This excessive use of force has created notable terrorist groups, such as the Irish Republican Army (IRA) and the Red Army Faction (RAF) of West Germany. Although the September 11 attacks were confined to New York and Washington D.C., airport security was immediately tightened not just in the U.S. but also in many parts of the world. As acts of political violence, the ramifications extend beyond the immediate target of violence, usually affecting the wider audience of the local population, and in many instances across national borders.

This wide-reaching impact of terrorism serves as a strong motivation for terrorists²¹. A terrorist group also needs to commit acts of violence as that has become what is necessary for the group to justify its existence. At the same time, it will deliberately steer away from any claims of success in achieving its espoused causes. This avoidance of success is paradoxical – while the objective is the cause, success can take it away, as once a terrorist group has achieved its objective, it would have nothing left to fight for.

Other experts cite three other possible motivations of terrorism: rational, psychological and cultural²². The rational motivation requires a businesslike approach which considers cost-benefit analysis and risk analysis as a critical part of the thought process. An error of

²¹ Jerrold M. Post. *Terrorist Psycho-logic: Terrorist behavior as a product of psychological forces*. Origins of Terrorism, Walter Reich (Ed). Baltimore: John Hopkins University Press. 1998.

²² David J. Whittaker (Ed.) *The Terrorism Reader*. New York: Routledge, 2001.

judgment could lead to the demise of the group itself. Psychological motivation encompasses the true believer of a cause, one who needs to belong to a group. At the same time, the group imposes a polarized “us versus them” outlook, with “them” as the evil ones, thereby justifying any violent action taken by the group. Moreover, a terrorist group must terrorize, if anything else to ensure continued self-esteem and worthiness of their label. Motivations for the cultural category deal with responses to threats against ones own existence. If a people feel that their ethnicity, religion, culture, language or even way of life is being suppressed or threatened by external influences, they may be prepared to resort to actions amounting to violence to ensure their survival. This will be especially so if their perception of the threat is such that they think it will capitulate in the face of violent action, as a result they will press ahead to the results they seek.

c. Terrorists and Cyberspace

Web sites are posted by various terrorist groups for specific purposes.

Some like jihad.net and aloswa.org were set up by Al Qaeda supporters to show support for Osama bin Laden, while others like 7hj.7hj.com teach the use of hacking to serve Islam²³. The Hizbullah were known to operate three sites as of February 1998:

hizbullah.org serves as the central press office, moqawama.org describes its attacks against Israel, and almanar.com.lb provides news and information²⁴. Many others are listed in the article “Al Qaeda and the Internet”, the most notable of which is alqeda.com which features international news on Al Qaeda, and purportedly contains encrypted information leading to more secure sites²⁵. This article also describes the use of the

²³ Bradley K. Ashley. *Anatomy of Cyberterrorism: Is America Vulnerable?* Maxwell AFB, 27 February 2003. p. 3.

²⁴ Dorothy E. Denning. *Information Warfare and Security*. New York: ACM Press 1999. p. 2.

²⁵ Timothy L. Thomas. *Al Qaeda and the Internet: The Danger of “Cyberplanning”*. Parameters. Spring 2003, p. 1.

Internet for cyber planning to support the terrorist cause through Web publicity, propaganda, research and information gathering, recruitment, planning and coordination. Specific activities include the use of the Internet for profiling, hiding identities, raising money, recruiting, information gathering, disrupting businesses, as well as for command and control, communications, propaganda and mobilization.

Initiating attacks in cyberspace may be a natural progression for terrorists. The value of the Web is so well acknowledged that almost every known terrorist group has a Web site. They cannot even be forced off, as they can either go to countries with broad free-speech laws, or take advantage of service providers who are unaware of their existence. For example, alneda.com was first hosted in Malaysia, subsequently in Texas and then Michigan, before being shut down in June 2002²⁶.

Electronic mail alongside cell phone surveillance has provided the U.S. NSA, FBI and CIA with valuable Intelligence. Reportedly, many Al Qaeda trainees were lax when it came to operational security pertaining to electronic mail and cell phones. Added to that was the use of the weaker 40-bit encryption or no encryption at all in their electronic mail or stored electronic documents, exposing them to eavesdropping and capture²⁷. In spite of these setbacks, it is evident that electronic mail – encoded, encrypted or otherwise – is a critical component of communications for many terrorist groups.

²⁶ Timothy L. Thomas. *Al Qaeda and the Internet: The Danger of "Cyberplanning"*. Parameters. Spring 2003, p. 2.

²⁷ James F. Dunnigan. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press Books, 2002, p. 158.

CHAPTER 3

CYBERTERRORISM

No single definition of the term “terrorism” has yet gained universal acceptance. Likewise, no single definition for the term “cyberterrorism” has been universally accepted. Labeling a computer attack as “cyberterrorism” is problematic because of the difficulty determining the identity, intent, or the political motivations of an attacker with certainty. Therefore, for the term “cyberterrorism” to have any meaning, we must be able to differentiate it from other kinds of computer abuse such as computer crime, economic espionage, or information warfare. The different views on cyberterrorism can be broken down to fundamental issues. We will discuss the disagreements about basic definitions of cyberterrorism, the threats that it poses, its utility to the terrorists, and its effects if played out. Any of these will lead to a different perspective on cyberterrorism.

1. Definition of Cyberterrorism

On October 21, 2002, in what was touted as “the most sophisticated and large-scale assault against these crucial computers in the history of the Internet”, nine out of the Internet’s thirteen core domain name servers were attacked for an hour with an overwhelming stream of traffic, effectively shutting them down.

Fortunately, there was no appreciable impact on the Internet itself since the critical information stored on those domain name servers was cached in thousands of other servers around the world²⁸.

²⁸ Wired News. *Servers Bounce Back from E-Attack*. Associated Press report Oct 22, 2002. [<http://www.wired.com/news/politics/0,1283,55957,00.html>].

But immediately after the attack, some warned that larger attacks were in the pipeline, and questioned if the Internet infrastructure was adequately robust to withstand similar if not worse attacks in future.

In September 2003 the Al-Farouq Web site, which is purported to be directly affiliated to Osama bin Laden's Al Qaeda, published a book on one of its Web sites entitled "The 39 Principles of Jihad", or more specifically, the 39 principles of *Al Qaeda's Jihad*, which literally means a struggle in the name of God, and also closely associated with the holy war concept. This is reflected in the "39 Principles". What is of particular interest are calls for followers to utilize the availability of modern technology to spread the message of their cause, including Internet Web sites and forums, as well as telecommunication tools such as SMS (smart messaging systems). In addition, the followers were called to "Perform electronic Jihad" by making use of their skills to "destroy American, Jewish and secular Web sites as well as morally corrupt Web sites"²⁹.

Also in 2003, an attack on the National Science Foundation's Amundsen-Scott South Pole Station, in which hackers from Romania broke into the station's servers and threatened to shut down the station's life support systems and sell information stolen from the servers unless they were paid a great deal of money. The FBI was able to help catch them before any harm was done, but the prospect was worrying: what if other stations could be conceivably held ransom in exchange for money or political actions?

These examples illustrate the problems in dealing with cyberterrorism. In the first example, denial-of-service attacks showed that while there were those who sought to disrupt if not disable the Internet, the identity of the perpetrators and the real motives behind the attack were unknown. Was it the work of several teenage whiz kids out to test their cyber skills, or a group of terrorists seeking to further their cause? It was also

²⁹ Joel Leyden. *Al-Qaeda : The 39 principles of Holy War*. News Agency. 4 September 2003

unclear why the attacks came to a sudden halt after an hour. Some speculated that this was only a test run and that larger attacks are to be expected. Others suggested that the attackers stopped after realizing that the attacks did not have the intended effect. Perhaps it was the work of some good Samaritans who wanted to send a warning sign to the DNS operators to secure their systems properly, since that was what several of the operators have done following the incident³⁰. In the second example, one of the most notorious terrorist groups today, Al Qaeda, is advocating the use of cyberspace as a means to further their cause, but the call is directed at defacing Web sites at worst. Significantly, there is no mention of using the Internet to achieve violence and destruction, although these people likely are planning such activities.

a. Expert Opinions

In the testimony to the Special Oversight Panel on Terrorism, Security expert Dorothy Dennings defined cyberterrorism as:

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

Denial of service attacks are clearly unlawful attack against computers, but it is not often known if the objectives are political or social. But Web sites sponsored by terrorist organizations are more apparently political and would therefore seem to conform to a cyberterrorist’s tactics. This definition is also echoed by J.T. Caruso of the U.S. FBI, in his testimony before House Subcommittee on National Security, Veterans Affairs and International Relations on March 21, 2002:

“Cyberterrorism – meaning the use of cybertools to shut down critical national infrastructures (such as energy, transportation or government operations) for the purpose of coercing or intimidating a government or civilian population.”

³⁰ Wired News. *Servers Bounce Back from E-Attack*. Associated Press report Oct 22, 2002. [<http://www.wired.com/news/politics/0,1283,55957,00.html>].

Many examples of cyberterrorism in the media seem to be derived from the definitions above. A 2001 Business World report listed some real examples of cyberterrorism³¹:

- The defacement of U.S. Web sites after the April 1, 2001 collision between a Chinese jet fighter and a U.S. surveillance plane;
- The theft of information from the U.S. Department of Defense computers regarding U.S. troop movements, by Dutch hackers during the 1990-91 Persian Gulf War (the hackers tried to sell the information to the Iraqis but the Iraqis thought it was a hoax);
- The penetration of computers at a U.S. Air base in Guam by a 15-year old Croatian youth.

However these examples would not satisfy definition above. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

With this qualification, it would seem that the many examples cited by the media have been misleading. Some have argued that there have been no acts of cyberterrorism to date precisely because of the above prerequisites.

b. Security Experts “Camps”

For the purposes of description and analysis experts opinions have been split into different “camps”.

³¹ Jovi Tanada Yam. *Bracing for cyberwar*. BusinessWorld Publishing Corporation. 4 October 2001.

The first camp belongs to the “death-knell” who warns that it is only a matter of time before a cyberterrorist attack happens. Since most countries and other non-state adversaries know that they cannot match the US in the conventional military realm, cyber warfare is an increasingly viable alternative.

This is accentuated by the growing reality that in many countries, their most valuable assets are in electronic storage and not their treasuries. With the information revolution, it has become easier to obtain the technical wherewithal to conduct IW activities using widely available commercial software and hardware. In addition, the Internet has provided a convenient and wide-reaching means for hacktivism – a fusion of hacking and activism – and other hacker activities. Each year, there are tens of thousands of computer attacks against the Pentagon. IW specialists estimate that with a budget of no more than \$10 million, a well prepared and coordinated attack by fewer than 30 computer hackers strategically located around the world could “bring the United States to its knees”, shutting down everything from power grids to air traffic control centers to emergency services. The basis for this assessment was probably made from the experience drawn from Exercise ELIGIBLE RECEIVER in 1997, in which a Red Team pretending to be North Korea was formed to carry out computer attacks against various government sites using hacking tools freely available from some 1900 Web sites on the Internet. Not only did they succeed in bringing down many key command-and-control systems, only 4 percent of those targeted were aware they were being attacked, and of these just 1 in 150 reported the intrusions to their superiors³².

The recent Slammer worm stopped Internet trading activities of the South Korean stock exchange³³. Had a similar worm been planted by the North Korean military to subvert the

³² CSIS Task Force Report. *Cybercrime... Cyberterrorism... Cyberwarfare... Averting an Electronic Waterloo*. Washington D.C.: Center for Strategic and International Studies, 1998.

³³ Jon Tullett. *Crying Wolf on Cyberterrorism?* SC Infosec Opinionwire. February 2003, p. 2.

South Korean defenses prior to a hypothetical invasion, the results could have been devastating for the South. Paradoxically, the goal of the “death-knell” camp is to ensure that its prophecies are never realized; actions taken as a result of the warnings should deny or at least reduce the probability of success for cyberterrorists.

The second camp comprises the “improbable” who believe that terrorists are more interested in physical violence and do not have the wherewithal to carry out sophisticated cyber attacks. So long as physical violence and destruction continue to draw publicity, fear and the appropriate public responses that feed their cause, there is little reason for a change of methods. A study on the prospects and implications of cyberterror found that the ability of a terrorist group to carry out cyberterrorist attacks depended on firstly, the group’s predilections toward cyberterror, and secondly, its means to do so³⁴.

The first requirement is not a given, since there are groups that prefer to stick to the more traditional means of physical destruction and violence. The second requirement implies a steep information technology learning curve that would take several years of effort for those groups that choose to develop an internal capability before any attacks can be effectively made. The combination of these two requirements significantly narrows the probability of cyber attacks by many terror groups. Some within the “improbable” camp think that the Internet is more likely to be used as a tool for cyberplanning than for cyberterrorism³⁵.

Thirdly there is the “nothing new” camp who claim that cyberterrorism is plain old terrorism executed in a different realm. Members in this camp distinguish it by calling it

³⁴ Dorothy E. Denning. *Cyberterrorism*. Global Dialogue, Autumn 2000. [<http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc>.]

³⁵ Timothy L. Thomas. *Al Qaeda and the Internet: The Danger of “Cyberplanning”*. Parameters. Spring 2003, p.3.

*technology-enabled terrorism*³⁶ or *information terrorism*³⁷. While there is no doubt that the threats posed by technology-enabled terrorism are real, the contention is that they are no different from the more well-known forms of terrorism. In the case of technology-enabled terrorism, however, protection must be commensurate with the nature of the threat. Thus, network security measures, intrusion detection systems, encryption and the like against electronic and network attacks are in order. One argument against cyberterrorism being merely terrorism in a different guise is whether cyberspace introduces new threats where there were none. A frequently cited example is SOLAR SUNRISE: in February 1998, two teenagers from California and one from Israel disrupted possible troop deployments to the Gulf when they launched attacks against the Pentagon's systems, NSA, and a nuclear weapons research lab using a well-known operating system vulnerability³⁸. While these three teenagers did not have terrorist intent, the means and potential damage that could have been caused are no different from what a cyberterrorist might attempt.

The "cry wolf" camp assert that threats have been exaggerated since there have been no known acts of cyberterrorism to date, and certainly none of the scale that was seen on September 11, 2001. The Symantec Internet Security Threat Report from January to June 2003 covered details of malicious code, Win32 viruses, the Slammer and Blaster Worms, spam activity, but made no mention of cyberterrorism or even terrorist-related cyber activities³⁹. Indeed, some have argued that the hype surrounding cyberterrorism is perpetuated by vendors for commercial gains. In addition, the more common forms of

³⁶ Dave Lang. *Cyberterrorism*. SC Infosec Opinionwire. February 2002, p. 3.

³⁷ Matthew G. Devost, Brian K. Houghton & Neal A. Pollard. *Information Terrorism: Can You Trust Your Toaster?* The Terrorism Research Center, 13 April 1996. [www.terrorism.com].

³⁸ CSIS Task Force Report. *Cybercrime... Cyberterrorism... Cyberwarfare...Averting an Electronic Waterloo*. Washington D.C.: Center for Strategic and International Studies, 1998.

³⁹ Symantec Security Response Newsletter, Oct 2003. [http://securityresponse.symantec.com]

cyberspace attacks, such as Web site defacement, denial-of-service attacks, Internet fraud, and scams, do not kill people or destroy property the way physical terrorist attacks do⁴⁰. Finally, there is the “realist” camp who advocates that the real cyber threats are not from terrorists but criminals who commit cyber crimes. This thinking is borne from statistical evidence which show that most of the illegal activities stem from scams, frauds, identity theft, credit card theft, as well as hackers who are not in it for the money. In November 2003, the London Financial Times reported that hackers were exploiting computer vulnerabilities to carry out cyber extortion against online businesses. By carrying out distributed denial-of-service (DDoS) attacks, they were able to bring down the sites of their targets and threatened more attacks unless the businesses paid up. The reality is that the rate at which new Web sites are created – more than one every four seconds – makes the job of law enforcement in cyberspace difficult. This is aggravated by the fact that the retention of computer talent in government agencies is constantly being threatened by the monetary lure of the private sector⁴¹.

While it is clear that there are different views on the threat posed by cyberterrorism, they all tend to agree that some form of threat exists, even if they disagree in its degree. They also all agree that the targets are rife and attractive.

Perhaps the question that needs to be answered is not what is the degree of the threat, but what has been or needs to be done to mitigate, address, counter, combat the threat.

⁴⁰ David Love, *Is Cyberterrorism a Serious Threat to Commercial Organizations?* SC Infosec Opinionwire. February 2003.

⁴¹ CSIS Task Force Report. *Cybercrime... Cyberterrorism... Cyberwarfare... Averting an Electronic Waterloo*. Washington D.C.: Center for Strategic and International Studies, 1998.

c. Differentiating between Cyberterrorism and Hacktivism

While some people use the term “cyberterrorism” to refer to any major computer-based attack on the government or economy, many terrorism experts would not consider cyberattacks by glory-seeking individuals, organizations with criminal motives, or hostile governments engaging in information warfare to be cyberterrorism. Like other terrorist acts, cyberterror attacks are typically premeditated, politically motivated, perpetrated by small groups rather than governments, and designed to call attention to a cause, spread fear, or otherwise influence the public and decision-makers. Hackers break in to computer systems for many reasons, often to display their own technical prowess or demonstrate the fallibility of computer security. Some on-line activists say that activities such as defacing Web sites are disruptive but essentially nonviolent, much like civil disobedience. Therefore they are not considered as cyberterrorists. Also it is important to distinguish between cyberterrorism and “hacktivism,” a term coined by scholars to describe the marriage of hacking with political activism. “Hacking” is here understood to mean activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software. Unlike hacktivists, hackers tend not to have political agendas.

2. Cyberterrorism Attractiveness

Cyberterrorism is the weapon of the weak. It appeals to fringe groups who cannot match the military might of their "oppressors" or perceived enemies. Many terrorist organizations aim to achieve a new "future order" if only by wrecking the present. There are several factors that make cyberterrorism an attractive weapon for terrorists:

a. Vulnerability

Vulnerability means the very linkages that enable information technology (IT) systems to function also provide vulnerable points that can be exploited by terrorists. Our sheer dependence on the system's functioning as planned is a source of great vulnerability. Deregulation and the increased focus on profitability have made utilities and other companies move more and more of their operations to the Internet in search of greater efficiency and lower costs. "Computerworld" journalist and former intelligence officer Dan Verton argues that the energy industry and many other sectors have become potential targets for various cyber disruptions by creating Internet links, both physical and wireless, between their networks and supervisory control and data acquisition (SCADA) systems⁴². These SCADA systems manage the flow of electricity and natural gas and control various industrial systems and facilities, including chemical processing plants, water purification and water delivery operations, wastewater management facilities, and a host of manufacturing firms. A terrorist's ability to control, disrupt, or alter the command and monitoring functions performed by these systems could threaten regional and possibly national security.

According to Symantec, one of the world's corporate leaders in the field of cybersecurity, new vulnerabilities to a cyberattack are being discovered all the time. The company reported that the number of "software holes", software security flaws that allow malicious hackers to exploit the system, grew by 80 percent in 2005. Still, Symantec claimed that no single cyberterrorist attack was recorded. This may reflect the fact that terrorists do not yet have the required know-how. Alternatively, it may illustrate that hackers are not sympathetic to the goals of terrorist organizations—should the two groups join forces, however, the results could be devastating.

⁴² Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terror*, Computerworld, August 16, 2003.

Equally alarming is the prospect of terrorists themselves designing computer software for government agencies. Remarkably, as Denning describes in "Is Cyber Terror Next?" at least one instance of such a situation is known to have occurred:

In March 2000, Japan's Metropolitan Police Department reported that a software system they had procured to track 150 police vehicles, including unmarked cars, had been developed by the Aum Shinryko cult, the same group that gassed the Tokyo subway in 1995, killing 12 people and injuring 6,000 more. At the time of the discovery, the cult had received classified tracking data on 115 vehicles. Further, the cult had developed software for at least 80 Japanese firms and 10 government agencies.

They had worked as subcontractors to other firms, making it almost impossible for the organizations to know who was developing the software. As subcontractors, the cult could have installed Trojan horses to launch or facilitate cyber terrorist attacks at a later date.

Despite stepped-up security measures in the wake of 9/11, a survey of almost four hundred IT professionals conducted for the Business Software Alliance during June 2002 revealed widespread concern⁴³. About half (49 percent) of the IT professionals felt that an attack is likely, and more than half (55 percent) said the risk of a major cyberattack on the United States has increased since 9/11. The figure jumped to 59 percent among those respondents who are in charge of their company's computer and Internet security.

Seventy-two percent agreed with the statement "there is a gap between the threat of a major cyberattack and the government's ability to defend against it," and the agreement rate rose to 84 percent among respondents who are most knowledgeable about security. Those surveyed were concerned about attacks not only on the government but also on private targets. Almost three-quarters (74 percent) believed that national financial

⁴³ Robyn Greenspan, "Cyberterrorism Concerns IT Pros," *Internetnews.com*, August 16, 2002. p. 3.

institutions such as major national banks would be likely targets within the next year, and around two-thirds believed that attacks were likely to be launched within the next twelve months against the computer systems that run communications networks (e.g., telephones and the Internet), transportation infrastructure (e.g., air traffic control computer systems), and utilities (e.g., water stations, dams, and power plants).

A study released in December 2003 appeared to confirm the IT professionals' skepticism about the ability of the government to defend itself against cyberattack⁴⁴. Conducted by the US House Government Reform Subcommittee on Technology, the study examined computer security in US federal agencies over the course of a year and awarded grades. Scores were based on numerous criteria, including how well an agency trained its employees in security and the extent to which it met established security procedures such as limiting access to privileged data and eliminating easily guessed passwords. More than half the federal agencies surveyed received a grade of D or F. The US Department of Homeland Security, which has a division devoted to monitoring cybersecurity, received the lowest overall score of the twenty-four agencies surveyed. Also earning an F was the US Justice Department, the agency charged with investigating and prosecuting cases of hacking and other forms of cybercrime.

Such studies, together with the enormous media interest in the subject, have fueled popular fears about cyberterrorism. A study by the Pew Internet and American Life Project found in 2003 that nearly half of the one thousand Americans surveyed were worried that terrorists could launch attacks through the networks connecting home computers and power utilities. The Pew study found that 11 percent of respondents were "very worried" and 38 percent were "somewhat worried" about an attack launched through computer networks.

⁴⁴ Reported in the *Washington Post* on January 31, 2004

b. Fear factor

The underlying agenda of terrorism is to generate fear through random, seemingly uncontrollable acts of violence. For many people, technology carries with it its own fear factor, stemming from its complexity, incomprehensibility, and seeming uncontrollability. The merger of these two sources of fear is a powerful one.

c. Anonymity

Cyberterrorism is more anonymous than traditional terrorist methods. Boundaries are blurred in cyberspace. The ordinary distinctions between public and private interests, war and crime, and geography are less clear. In cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart. Viruses can be imported into the country through information networks, telephone lines, or on disk media. Like many Internet surfers, terrorists use online nicknames—"screen names"—or log on to a website as an unidentified "guest user," making it very hard for security agencies and police forces to track down the terrorists' real identity. A cyberattack can be conducted remotely and anonymously, allowing the attacker to avoid detection and capture. It is often difficult or impossible to know if your system is under attack and by whom. Remote capability also complicates the investigation, pursuit, and judicial processes because of differences in international laws.

d. Attention

Cyberterrorism provides a way to assert identity and command attention. If terrorists choose to forego anonymity, an act of cyberterrorism would likely gain extensive media coverage as well as government and public attention. As the I LOVE YOU virus showed (described in chapter 5), cyberterrorism has the potential to affect directly a larger number

of people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want.

e. Availability and Low Cost

It is cheaper than traditional terrorist methods. Availability of the weapons of cyberterrorism and the potential for disruptive effects are rising, while financial and other costs are decreasing. A wide array of easy-to-use software attack tools is readily available without cost from thousands of web sites. For a minimum investment, attacks can be waged that are serious and costly; the terrorists can affect more people at less risk to themselves than with other types of terrorist weapons. All that the terrorist needs is a personal computer and an online connection. Terrorists do not need to buy weapons such as guns and explosives; instead, they can create and deliver computer viruses through a telephone line, a cable, or a wireless connection. "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb"⁴⁵.

f. Safety

This form of terrorism does not require the handling of explosives or bio-chemical agents or a suicide mission. Cyberterrorism can be conducted remotely, a feature that is especially appealing to terrorists. Cyberterrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retain followers.

g. Expertise

In the last few years, many automated attack tools have appeared on the Internet, making it much easier even for ignorant attackers to cause considerable damage. However, new

⁴⁵ National Research Council, System Security Study committee, *Computers at Risk; Safe Computing in the Information Age* (Washington D.C.: National Academy Press, 1991), p 7.

generations of hackers are growing up with ever more digital capability, and hacker networks are already huge. Hackers and insiders might be recruited by terrorists or become self-recruiting cyberterrorists.

h. Variety of Targets

The variety and number of targets are enormous. The cyberterrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth. The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit. Several studies have shown that critical infrastructures, such as electric power grids and emergency services, are vulnerable to a cyberterrorist attack because the infrastructures and the computer systems that run them are highly complex, making it effectively impossible to eliminate all weaknesses.

i. Fewer taboos

Cyberterrorism can be conducted with minimal loss of human life, and there are no global taboos associated with waging war against machines. However, some terrorist groups have made it clear that they are not deterred by the potential for human carnage, and it is possible to use cyberterrorism to cause human casualties.

j. Female Participation

Cyberterrorism can be conducted remotely and does not require the handling of explosives or bio-chemical agents or a suicide mission. This will allow for a better participation of female terrorists. It is easier for them to use keyboard than to use bombs. Female cyberterrorists will be able to use their expertise in order to be an active participant. Therefore, cyberterrorism would result in terrorist groups retaining a larger number of followers.

CHAPTER 4

CYBERTERRORISM THREAT

1. Motivations

In the section on terrorism, we saw that the main motivations for terrorism revolved around political, ideological or religious causes. If cyberterrorism were truly a convergence of terrorism and cyberspace, then the same motivations would apply for cyberterrorism, albeit in a different medium. Many of the Web sites set up by terrorist groups serve the objectives of politics, ideology or religion.

Indeed, cyberspace provides certain advantages over a physical medium.

For a start, it offers to cyberterrorism the benefit of remote and anonymous operations. It also avoids the need for handling physical weapons and explosives, and the attendant risk of spectacular failure of botched attempts when bombs explode prematurely.

Cyberterrorist attacks are also likely to reap as much publicity as physical ones⁴⁶.

Additionally, cyberspace has enabled small players to create massive disruption, as for example through the creation and release of the "ILOVEYOU" and "Nimda" viruses or the more recent Blaster worm. This means that terrorists groups can get onto the world stage and create disruption and destruction on a scale that belies their size⁴⁷.

Cyberspace attacks are not without disadvantages. Those viral or worm attacks that have had great reach were the result of the attacks going out of control; it may be difficult for cyberterrorists to control their attacks to inflict the desired level of damage. Cyber attacks

⁴⁶ Dorothy E. Denning. *Cyberterrorism*. Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, May 23, 2000. [<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>]

⁴⁷ CSIS Report. *Cyber Threats and Information Security: Meeting the 21st Century Challenge*. A report for the CSIS Homeland Defense Project. Washington D.C.: Center for Strategic and International Studies, May 2001, p. 5.

are probably less responsive to the whims of the terrorist leaders than physical attacks due to the lead time required to study the networks and gain access. Finally, as pointed out by the “improbable” camp in the previous chapter, a strong counter-motivation would be the effectiveness of tried and tested methods. It may still be easier to destroy a building with a car bomb than to take out all its computers with denial-of-service or worm attacks. This could well be the reason why little has been happening in comparison at the cyberterrorist front.

2. Actors

In order to fully appreciate the threat of cyberterrorism, another important issue to consider is what groups are likely to utilize cyberterrorism to further their political and social goals. It is important to identify these groups in order to define the threat and judge the sophistication of the cyber terrorists. Unfortunately, a cyber terrorist threat could come from countless sources. Individuals, countries, international terrorist groups, domestic groups, and numerous others have the capability to commit cyber terrorism. In addition, the existence of different cyberterrorist “camps” and forms of cyber attacks suggests that there may be more than just one type of cyberterrorist. Moreover, the nature of the medium enables cyberterrorists to be quite different from typical terrorists. Here we examine four possible categories of cyberterrorists and assess their threat.

Many of the well-known viruses such as the Morris worm, the “ILOVEYOU” virus, and the Chernobyl virus that have plagued cyberspace were the work of individuals. Recent history has also seen the likes of individuals who have created widespread damage, fear, and psychological trauma among the population, such as Ted Kaczynski (The Unabomber), Tim McVeigh (Oklahoma City Bomber) and John Muhammed (Washington D.C. sniper). Put the two types of individuals together and we get a sample of

cyberterrorists. Many virus writers do so for the adventure and intellectual challenge, not for the sake of creating havoc⁴⁸. Moreover, the damage created by viruses and worms tend to be economic in nature, and have not cost human lives. As such, a lone cyberterrorist is more likely to be a Kaczynski or McVeigh with relevant computer skills, rather than a hacker or virus writer intent on killing others. Given a lack of precedents, the threat of a lone cyberterrorist appears to be low, but not improbable.

A small group of technically-skilled extremists could combine their abilities to create a well coordinated cyberterrorist operation. The Japanese Aum Shinryko cult were so well-developed in their software capabilities that they acted as the software subcontractors to companies that were awarded contracts by the Japanese government. By the time the link was discovered in March 2000, the cult had already been receiving classified tracking data on Japanese police vehicles⁴⁹. Such groups may be considered to be a greater cyberterrorist threat than lone cyberterrorists because they have proven their ability to carry out such acts. In the case of the Aum Shinryko cult, they had already been found guilty of the Tokyo subway attack that killed 12 and injured 6000 others. Now their software abilities suggest that it would not take much for them to translate their violent goals to the next level in cyberspace.

Large religious terrorist organizations such as Al Qaeda with a track record in physical violence are another category that may embark on the cyberterrorism route. As it is, most of them have a presence in cyberspace and have even advocated electronic Jihad. The Al Qaeda cyber threat against the Defense Intelligence Agency threat-analysis methodology was measured based on the existence, capability, intentions, history, and targeting of the

⁴⁸ Dorothy E. Denning. *Information Warfare and Security*. New York: ACM Press 1999, p. 78.

⁴⁹ Dorothy E. Denning. *Cyberterrorism*. Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, May 23, 2000. [<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>]

threat and it was concluded that Al Qaeda posed a critical cyber threat to the U.S.⁵⁰ However, a potential shortcoming in this assessment is that Al Qaeda does not have a proven cyber capability, notwithstanding that Osama bin Laden had boasted of the existence of “Muslim scientists” among his strike force. While it may only be a matter of time before they strike, the cyber threat currently posed by Al Qaeda and similar groups may not be any more imminent compared to the previous category. Judging from the number of recent bombings attributed to such religious fundamentalist groups, and the technologically unsophisticated nature of the bombings, it would seem that they continue to favor the traditional methods.

The final category belongs to information-warfare groups that are sponsored or backed by hostile governments. There are at least two levels of information-warfare groups, each with differing capabilities and origins. At the official level there are cyberwarfare units formed by governments to attack enemy information systems, as well as to protect their own. A report on the military power of the People’s Republic of China cited the presence of “Special information warfare units [that] could attack and disrupt enemy C4I, while vigorously defending PRC systems”⁵¹. Strictly speaking they are not cyberterrorist outfits, but the scale and degree of harm that they were created to inflict are similar. These government units are restrained in peacetime by international treaties and therefore cannot openly carry out vulnerability scans of an adversary’s systems, for example. The same report also hints at the presence of Nationalistic hackers who form an unofficial organizational level. These are self-declared patriots who take it upon themselves to attack the information systems of other countries when they are in conflict. This type is

⁵⁰ Bradley K. Ashley. *Anatomy of Cyberterrorism: Is America Vulnerable?* Research Paper, Air War College, Air University, Maxwell AFB, AL. 27 February 2003.

⁵¹ IWS – The Information Warfare Site. *Annual Report On The Military Power Of The People’s Republic Of China*. 28 July 2003. [<http://www.iwar.org.uk/iwar/resources/news/china-io-2003.htm>]

not limited to some Chinese, since Dunnigan, security expert, reports widespread hacking by Russians, Taiwanese, Israelis, Indians, Pakistanis and Americans following international incidents such as those mentioned in the previous section⁵². Many of these hackers contravene their own national laws when they carry out such activities, but often they are left alone by their governments so long as their activities fall in line with “national interests”. Security expert Devost suggested the employment of hackers as a national resource because they have the requisite skills for attacking an adversary’s information systems⁵³. Some evidence exists to suggest the presence of a third level of hackers sitting between the first two. In 2001, Taiwan allegedly unleashed several viruses against China but the viruses spread around the world. Taiwan has not admitted to these incidents, but the scale and targets of the apparently anonymous attacks suggest that clandestine groups are operating with covert government links⁵⁴. This middle clandestine level appears to pose the most significant threat because they have many of the resources of the official groups and the freedom of action of the outlaw hackers.

3. Targets

In the Second World War, strategic bombing targeted the weak belly of the adversary, focusing on population and industrial centers in an effort to demoralize the frontline troops and undermine their war-making machinery. The information technology revolution and improved military technology have made possible precision bombing and targeting, thereby reducing significantly the killing of innocent civilians and the

⁵² James F. Dunnigan. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press Books, 2002 p.56.

⁵³ Matthew G. Devost. *Hackers as a National Resource*. Information Warfare – Cyberterrorism: Protecting Your Personal Security in the Electronic Age. Winn Schwartau (Ed). Second Trade Paperback Edition. New York: Thunder’s Mouth Press, 1996 p. 85.

⁵⁴ James F. Dunnigan. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press Books, 2002, p. 62.

associated political backlash. However, the information technology revolution has also shifted the balance of power to the commercial sector, as far as innovation, development, resources and the state-of-the-art are concerned. Thus it would seem that in the age of cyber warfare, attackers are now drawn towards those who rely heavily on information technology, or who would have much to lose by being denied it. In this case, the commercial sector would be as lucrative a target as the government. The frontline in cyber warfare has shifted back to the population and new industrial centers of information technology.

Computers, computer servers and computer networks are usually considered the *targets* of cyber attacks. As the October 2002 attack on the nine core Internet domain name servers showed, such attacks have indeed taken place and this scenario is therefore not unthinkable. In these denial-of-service (DoS) attacks, target computer servers are flooded with more messages than they can effectively handle, thus denying service to genuine users. In some cases such as distributed denial-of-service attacks, the flooding is from the accumulation of messages from many other “zombie” servers on which malicious programs had been secretly planted to make them collaborators in an illegal activity beneficial to them. One of the most spectacular attacks occurred between 7-9 February 2000 when a massive attack crippled popular Web sites like Yahoo.com, Amazon.com, CNN.com, ETrade, and EBay. During that period, it was estimated that the average surfing times were delayed by 26 percent, due to the additional traffic on the Internet as result of the attacks⁵⁵. These zombie servers could be considered both as targets and weapons of the cyber attack, as they first needed to be targeted for “conversion” before they became part of the attackers’ arsenal.

⁵⁵ James F. Dunnigan. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press Books, 2002.

Many cyberterrorism scenarios involve disabling the Internet or at least disrupting a significant portion of it. Notwithstanding that it will involve massive amounts of resources, coordination and know-how, disabling the Internet would surely cripple the communications means by which many organizations and agencies do their business and is therefore a high-payoff target. However, cyberterrorists who seek to disable the Internet must surely know that it would also disable their means to carry out further cyber attacks. So such scenarios should perhaps be refined to paint the Internet as the last thing to go down, not the first.

The cyberterrorism threat is not easily detected or anticipated. At best it can be deterred; at worst the system will have to absorb the first blow and recover quickly. Some scenarios suggest retaliation, but it is often difficult to determine the attacker and there may be associated legal issues.

4. Understanding the Threat

The gravity of the cyberterrorism threat may be measured from two parts: the vulnerability of targets which if exploited could lead to violence, physical destruction or death, and the ability and motivation of terrorists to carry out such attacks⁵⁶. There are many scenarios in which attacked information infrastructures can lead to destruction and death. For example if the computer systems of an air traffic control system (ATCS) are hacked into and manipulated, it could result in a collision of aircraft in mid-air.

Following FBI reports of Al Qaeda members researching information on the Supervisory Control and Data Acquisition (SCADA) infrastructure which manages U.S. water and wastewater systems, new scenarios emerged with terrorists taking remote control of such

⁵⁶ Dorothy E. Denning. *Cyberterrorism*. Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, May 23, 2000. [<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>]

systems and releasing dammed water onto civilian populations downriver⁵⁷. Other scenarios feature a blending of cyber attacks with physical ones (bombs or attacks on critical infrastructure). For example, a large bomb could be detonated in a crowded marketplace with the ability of emergency teams to respond hindered by a power and telecommunications failure caused by the cyberterrorist wing of the terrorist group. ELIGIBLE RECEIVER and SOLAR SUNRISE have shown that certain critical infrastructures could be susceptible to such incidents.

The second part of cyber threat assessment deals with the ability of terrorist groups to carry out cyber attacks. Of the four types of actors mentioned, the first three have a proven propensity for wanton and indiscriminate violence.

Since no cyberterrorism act has occurred yet, it is suggested that they either lack the means or will to do so. However, this state of affairs cannot be relied upon as the terrorist ranks are gradually filled with newer and younger recruits who have grown up with information technology. A more sinister threat of cyberterrorism is when cyber attacks carried out by any of the actors remained undetected. Those attackers that are discovered either lack sophistication or are too disorganized to conduct any coordinated attack. The more serious threats are likely unseen, complex and distributed. Attackers could conduct covert reconnaissance for years to ascertain critical information assets before execution of actual operations⁵⁸. Some have called this the new terrorism⁵⁹. In this scenario, Web site defacements, hacktivism and hacking intrusions are probably only the tip of the iceberg.

⁵⁷ Bradley K. Ashley, Lt. Col, USAF. *Anatomy of Cyberterrorism: Is America Vulnerable?* Research Paper, Air War College, Air University, Maxwell AFB, AL. 27 February 2003, p.5.

⁵⁸ CSIS Task Force Report. *Cybercrime... Cyberterrorism... Cyberwarfare... Averting an Electronic Waterloo*. Washington D.C.: Center for Strategic and International Studies, 1998.

⁵⁹ Sarah Gordon and Richard Ford. *Cyberterrorism?* Symantec Security Response White Paper 2002.

5. Possible Impact

The potential impact of various scenarios is described in the next chapter. The vast majority of past cyberattacks have been nuisance attacks, but experts warn that attacks by true terrorists are a matter of "when," not "if." If the apparent coordination and patience employed by the September 11 terrorists were applied to a multifaceted cyberterrorist attack, the results could be catastrophic. Matthew Devost paints this hypothetical picture:

“Imagine a well trained team of saboteurs, operating over several years, infiltrating several high technology companies like Microsoft or Novell, a few major automobile manufacturers, or a couple of airlines. Viruses or trojan horses are timed to detonate on a certain day, rendering computer systems inoperable. A small team of hackers infiltrates large computer, telecommunications, and power centers preparing them for denial of service attacks. Another team constructs several large EMP/T bombs and HERF Guns to be directed at targets like the Federal Reserve and Wall Street. Doomsday arrives, and the country's electronic blood stops flowing. No transfer of electronic funds, no stock exchange, no communications and power in a majority of locations, no traffic control, no air travel. . . and we have no one to blame”⁶⁰.

While this may be an extreme example, it is clear that a cyberattack of much smaller proportions has the potential for serious disruption of local networks and the systems on which emergency management depends.

6. Assessing the Threat

It seems fair to conclude that the current threat posed by cyberterrorism might be exaggerated to some limit. No single instance of cyberterrorism has yet been recorded. Cyberterrorism threat is quite severe for the developed countries, as we mentioned in the previous sections, but it does not represent the gravest threat to them. Their defense and intelligence computer systems are air-gapped and thus isolated from the Internet, it is difficult, but not impossible, to disrupt them.

⁶⁰ Devost, Matthew. National Security in the Information Age, p. 35.

The systems run by private companies are more vulnerable to attack but also more resilient than is often supposed; the vast majority of cyberattacks are launched by hackers with few, if any, political goals and no desire to cause the mayhem and carnage of which terrorists dream.

So, why has so much concern been expressed over the cyberterrorism threat?

The reasons are many. First, as Denning has observed, “cyberterrorism and cyberattacks are sexy right now. . . . [Cyberterrorism is] novel, original, it captures people’s imagination.”⁶¹ Second, the mass media frequently fail to distinguish between hacking and cyberterrorism and exaggerate the threat of the latter especially through certain analogies such as the following: “If a sixteen-year-old could do this, then what could a well-funded terrorist group do?” Ignorance is a third factor. Green argues that cyberterrorism merges two spheres—terrorism and technology—that many people, including most lawmakers and senior administration officials, do not fully understand the future impact of such a marriage and therefore tend to fear it. A fourth reason is that some politicians, whether out of genuine conviction or out of a desire to stoke public anxiety about terrorism in order to advance their own agendas, have played the role of prophets of doom. And a fifth factor is ambiguity about the very meaning of “cyberterrorism,” which has confused the public and given rise to countless myths.

Denning and other terrorism experts conclude that, at least for now, hijacked vehicles, truck bombs, and biological weapons seem to pose a greater threat than does cyberterrorism. However, just as the events of 9/11 caught the world by surprise, so could a major cyberassault. The threat of cyberterrorism may be exaggerated, but we can neither deny it nor dare to ignore it.

⁶¹ Dorothy E. Denning. *Cyberterrorism*. Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, May 23, 2000. [<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>]

CHAPTER 5

METHODS OF ATTACK

In order to fully appreciate the growing threat of cyberterrorism, it is important to discuss the capabilities of cyberterrorists. In order to determine the capabilities of cyberterrorists it is necessary to examine several possible hypothetical situations posed by experts in the field of cyberterrorism, and to highlight actual incidents that have occurred in the last several years.

1. Risk Factors

There are three key risk factors related to computer systems: access, integrity, and confidentiality. The proper functioning of information systems is predicated on restricted access to data and operations, on the integrity (accuracy and timeliness) of the data, and on the confidentiality of information that is intended to remain private.

If unauthorized parties gain access to a system, they can cause damaging actions to occur within the system. If a database is accessed and manipulated, the ripple effect can be enormous; the smallest change in a database can cause huge damage, change one number, and all resulting data becomes unreliable. If confidentiality is breached, private information may become public and sensitive data may fall into the wrong hands. Theft of passwords and user IDs can enable unauthorized access, and the cycle continues.

2. Types of Cyberterrorism

The following are some general types of cyberterrorism:

- * *Data destruction or corruption*: Using viruses, installation of malicious code, or other means to damage a system from within. This could include destroying or corrupting files, changing data in a database, or corrupting software programs within the system.
- * *Penetration of a system to modify its output*: Embedding code (e.g., Trojan horses or "logic bombs") to perform unauthorized functions at a later time.
- * *Theft*: System penetration with the goal of stealing information or sensitive data (e.g., password cracking and theft, "packet sniffing").
- * *Disabling a system*: Disruption of information structures (e.g., using e-mail bombings, spamming, denial-of-service attacks, or viruses) to crash or disable a system.
- * *Taking control of a system*: Taking over a system (e.g., an air traffic system, a manufacturing process control system, a subway or train system, a 911 communications system) to use it as a weapon.
- * *Website defacement*: Hacking into a website and changing its contents to spread misinformation, incite to violence, generate fear, or create chaos.

3. Possible Cyberterrorism Scenarios

Many potential scenarios for cyberattacks have been suggested, and there are undoubtedly many more that are equally possible. The following are some of the scenarios that have been discussed in cyberterrorism literature, along with selected examples of actual events that have occurred. Although safeguards are in place that would make some of these scenarios very difficult, the range of potential cyberterrorist scenarios indicates the extent of computer vulnerability.

- * *Power grid*: Attack the computer systems that control a large regional power grid. If the power is lost for a sustained period of time, people may die. Most life support, emergency response, law enforcement, and other systems depend on electrical power. If

a nuclear reactor is located in the region, a meltdown may occur, causing a major radiological incident that could cause mass casualties.

As an example, the U.S. power system is divided into four electrical grids supplying Texas, the Eastern States, the Midwestern States, and the Northwestern States. They are all interconnected in Nebraska. A unique aspect of the electrical grids, as with communication grids, is that most built-in computerized security is designed to anticipate no more than two disruptions concurrently. In other words, if a primary line went down, the grid would ideally shut off power to a specific section while it rerouted electricity around that problem area. If it ran into two such problems, however, the grid is designed to shut down altogether⁶².

* *Air traffic*: Break into an air traffic control system and tamper with the system in such a way that airplanes collide, resulting in mass death; or disable landing systems.

In one documented incident, someone took control of the computer system at a small U.S. airport and switched off the landing lights. This action could have killed many people.

* *Subway/train system*: Take over the operation of a subway or train system, to similar effect. In Japan, groups have attacked the computerized control systems for commuter trains, paralyzing major cities for hours.

* *Financial and business systems*: Disrupt banks, international financial transactions, and stock exchanges. Economic systems grind to a halt, the public loses confidence, and destabilization is achieved. It costs a billion dollars and takes six weeks to recover from a one-day bank failure. If Wall Street suddenly closed down, the United States would lose hundreds of billions of dollars.

⁶² Bowman, Stephen. *When the Eagle Screams: America's Vulnerability to Terrorism*. New York: Carol Publishing Group, 1994, p. 125. As quoted in Devost, Matthew G. *National Security in the Information Age*. University of Vermont Masters Thesis, May 1995. Accessed at: www.terrorism.com/documents/devostthesis.html.

* *Communications systems*: Invade public telephone networks, shutting down major switching hubs and disrupting emergency services, or invade the wireless networks on which we have become increasingly dependent. Extended denial-of-service could paralyze business, government agencies, airports, and some military installations. Hackers have invaded the public phone networks, compromising nearly every category of activity, including switching and operations, administration, maintenance, and provisioning. They have crashed or disrupted signal transfer points, traffic switches, and other network elements. They have planted "time bomb" programs designed to shut down major switching hubs, disrupted emergency 911 services throughout the Eastern seaboard, and boasted that they have the capability to bring down all switches in Manhattan.

* *Critical communications hubs*: Disable telephone company computers that service airports, fire departments, and other communications-dependent services.

In March 1997, a hacker in Massachusetts penetrated and disabled a telephone company computer that services the Worcester Airport. For six hours, service was cut off to the FAA control tower, the airport fire department, airport security, the weather service, and several private airfreight companies. The lost service caused financial damages and threatened public health and public safety.

* *Emergency alert and emergency response*: Disabling emergency alert systems, preventing the public from being notified of dangerous chemical releases or other emergencies; scrambling the software used by emergency services. A fired employee hacked into Chevron's computer systems, reconfiguring them and causing them to crash, and disabling the firm's alert system. The disabled alert system went undetected until there was a plant emergency involving a noxious release and the system could not be used

to notify the adjacent community. Thousands of people in 22 States and areas of Canada were put at risk.

* *Utilities*: Penetrate the computer systems of utilities to cause "accidents" affecting public health and services, compromise systems monitoring the water supply, change pressure in gas pipelines to cause valve failure, or bring down the system.

In Australia, someone penetrated a municipal computer system and used radio transmissions to create overflows of raw sewage along the coast.

* *Process control*: Take over the process control computers in a manufacturing line, e.g., change the formulation of a pharmaceutical or food product to make it unsafe; trigger oil refinery explosions and fires.

* *Military intrusion*: Disrupt military networks. Nearly everything the military does depends on computer-driven civilian information networks.

The U.S. Department of Defense websites experience about 60 cyberattacks per week.

* *Banking extortion*: Attack banking and other financial computer networks. One scenario is to hack into a large bank's computer system and leave a message threatening the bank with various forms of cyberterrorism, e.g., logic bombs or electromagnetic pulses to destroy the bank's files. Unwilling to reveal their vulnerability to the public, the bank might succumb to extortion.

* *Medical systems*: Hack into medical records or pharmacy systems and change vital data, causing dangerous changes in treatments and loss of confidence in the system. Corrupt, disrupt, or crash a hospital's computer system, putting many human lives at stake.

* *Business information systems*: A successful attack on just a few business information systems could cause a severe lag in the economy.

4. Computer Attack Methods

A computer attack may be defined as actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data.

Different attack methods target different vulnerabilities and involve different types of weapons, and several may be within the current capabilities of some terrorist groups.

Three different methods of attack are identified in this study, based on the effects of the weapons used. However, as technology evolves, distinctions between these methods may begin to blur.

- ❖ A physical attack involves conventional weapons directed against a computer facility or its transmission lines;
- ❖ An electronic attack (EA) involves the use of the power of electromagnetic energy as a weapon, more commonly as an electromagnetic pulse (EMP) to overload computer circuitry, but also in a less violent form, to insert a stream of malicious digital code directly into an enemy microwave radio transmission; and
- ❖ A computer network attack (CNA), usually involves malicious code used as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an organization or computer user. Other forms of CAN are enabled when an attacker uses stolen information to enter restricted computer systems.

While CNA and EA threats are “less likely” than physical attacks, they could actually prove more damaging because they involve disruptive technologies that might generate unpredictable consequences or give an adversary unexpected advantages⁶³.

⁶³ Jason Sherman, “Bracing for Modern Brands of Warfare,” *Air Force Times*, Sept. 27, 2004, [<http://www.airforcetimes.com/story.php?f=1-AIRPAPER-358727.php>].

a. Physical Attack

A physical attack disrupts the reliability of computer equipment and availability of data. Physical attack is implemented either through use of conventional weapons, creating heat, blast, and fragmentation, or through direct manipulation of wiring or equipment, usually after gaining unauthorized physical access.

In 1991, during Operation Desert Storm, the U.S. military reportedly disrupted Iraqi communications and computer centers by sending cruise missiles to scatter carbon filaments that short circuited power supply lines. Also, the Al Qaeda attacks directed against the World Trade Center and the Pentagon on September 11, 2001, destroyed many important computer databases and disrupted civilian and military financial and communications systems that were linked globally⁶⁴. The temporary loss of communications links and important data added to the effects of the physical attack by closing financial markets for up to a week.

b. Electronic Attack (EA)

Electronic attack, most commonly referred to as an Electromagnetic Pulse (EMP), disrupts the reliability of electronic equipment through generating instantaneous high energy that overloads circuit boards, transistors, and other electronics. EMP effects can penetrate computer facility walls where they can erase electronic memory, upset software, or permanently disable all electronic components⁶⁵. Some assert that little has been done by the private sector to protect against the threat from electromagnetic pulse, and that commercial electronic systems in the United States could be severely damaged by limited

⁶⁴ Steven Marlin and Martin Garvey, "Disaster-Recovery Spending on the Rise," *Information Week*, Aug. 9, 2004, p.26.

⁶⁵ Kenneth R. Timmerman, "U.S. Threatened with EMP Attack," *Insight on the News*, May 28, 2001, [<http://www.insightmag.com/news/2001/05/28/InvestigativeReport/U.Threatened.With.Emp.Attack-210973.shtml>].

range, small-scale, or portable electromagnetic pulse devices⁶⁶. Some military experts have stated that the United States is perhaps the nation most vulnerable to electromagnetic pulse attack⁶⁷.

Observers believe that mounting a coordinated attack against computer systems, using either larger-scale, smaller-scale, or even portable EMP weapons requires technical skills that are beyond the capabilities of most terrorist organizations. However, nations such as United States, Russia, and possibly terrorist-sponsoring nations such as North Korea, now have the technical capability to construct and deploy a smaller chemically-driven, or battery-driven EMP device that could disrupt computers at a limited range⁶⁸.

c. Cyberattack (CNA)

A computer network attack (CNA), or “cyberattack,” disrupts the integrity or authenticity of data, usually through malicious code that alters program logic that controls data, leading to errors in output. Computer hackers opportunistically scan the Internet looking for computer systems that are mis-configured or lacking necessary security software. Once infected with malicious code, a computer can be remotely controlled by a hacker who may, via the Internet, send commands to spy on the contents of that computer or attack and disrupt other computers.

Cyberattacks usually require that the targeted computer have some pre-existing system flaw, such as a software error, a lack of antivirus protection, or a faulty system configuration, for the malicious code to exploit. However, as technology evolves, this distinguishing requirement of CNA may begin to fade. For example, some forms of EA

⁶⁶ “Experts Cite Electromagnetic Pulse as Terrorist Threat,” *Las Vegas Review-Journal*, Oct. 3, 2001.

⁶⁷ Seth Schiesel, “Taking Aim at An Enemy’s Chips,” *New York Times*, Feb. 20, 2003.

⁶⁸ Michael Abrams, “The Dawn of the E-Bomb,” *IEEE Spectrum Online*, Nov. 2003, [<http://www.spectrum.ieee.org/WEBONLY/publicfeature/nov03/1103ebom.html>].

can now cause effects nearly identical to some forms of CNA. For example, at controlled power levels, the transmissions between targeted microwave radio towers can be hijacked and specially designed viruses, or altered code, can be inserted directly into the adversary's digital network.⁶⁹

5. Cyberterrorist Tools

To achieve these results, the cyberterrorist cannot use the weapons commonly employed in conventional terrorism. Their weapons exist nearly exclusively in cyberspace. These new weapons are unique in that they can simultaneously be more powerful and weaker than the weapons of the conventional terrorist. This apparent dichotomy exists because the laws of physics do not operate in cyberspace in the same manner as in the physical world. A conventional bomb will have some effect every time it is exploded in the real world. A software bomb when exploded in cyberspace may have an extraordinary effect the first time it is used as it normally exploits an existing weakness in a computer operating system. After that weakness has been corrected, an identical software bomb will do no damage to the targeted computer or its data.

a. Viruses

One of the most heralded weapons of a cyberterrorist or a hacker is the computer's virus. Computer viruses are programs designed to perform actions not intended by the operator. These actions include erasing or modifying the data in a computer's memory or storage with or without malicious intent. A virus is so named because it "lives" within a host system or program and cannot spread without some acting, often unwitting (such as using an infected disk, or receiving it by email), by the system operator. Viruses can be used in

⁶⁹ David Fulghum, "Network Wars," *Aviation Week & Space Technology*, Oct. 25, 2004, p.91.

an attempt to shut down a computer or even hold it hostage. The front page publicity granted the "Michelangelo virus" every march serves as an example of the publicity power generated by hostile virus. This particular virus was written to check the computer's internal clock/calendar and destroy the data on the infected computer on Michelangelo's birthday, March 6. The virus was widely publicized when released in 1992.

The **MICHELANGELO** virus, a nasty bit of high-technology vandalism designed to break out each year on March 6, the great artist's birthday, failed to cripple the world's computers. The Michelangelo virus was front-page news in 1992⁷⁰.

The **ILOVEYOU** virus and variants, for example, was estimated to have hit tens of millions of users and cost billions of dollars in damage. The February 2000 denial-of-service attacks against Yahoo, CNN, eBay, and other e-commerce Web sites was estimated to have caused over a billion in losses. It also shook the confidence of business and individuals in e-commerce.

To compete against virus detection and removal programs, virus writers have created a subset of the virus, known as a polymorphic virus. This type of virus changes itself slightly every time it is replicated or executed, thus denying a virus detection program a fixed set of "indicators" that the virus has infected a computer. The battle between virus writers and virus fighters will continue into the future, with each trying to outsmart the other. The sheer explosion in the number of viruses (in 1991 there were approximately 500 known computer viruses, by 1995 that number expanded to more than 5,000) is evidence of this threat.⁷¹ This exponential growth suggests that virus writers hold the initiative in the battle for cyberspace. For existing operating systems that are infected with

⁷⁰ Briefing, Denver Post 8 March 1995 business, C-2, Nexis.

⁷¹ Prevention Beats cure for Terminal Illnesses: Computer Viruses," *Daily Telegraph (London)*, 30 May 1995, 2

viruses, a cure cannot be developed until the virus is released into the system. Once released, the virus can be studied to find a method to prevent its further spread and remove it from the system. The computer community is striving to regain the initiative by developing operating systems that are more resistant to viruses. Despite these developments, those that attack computer systems will generally hold the initiative.

b. Trojan Horses

The second type of weapon is a trojan horse. True to its name, it is a program that does not appear to be destructive but releases a second program to perform a task unintended by the system operator. A trojan horse can be used to install a password "sniffer" program that collects the passwords of valid users and stores them for later use by an intruder posing as a legitimate user. Cyberterrorists can utilize this type of weapon for espionage to gain the information needed to access a system by impersonating legitimate users, thus compounding the problem of intrusion detection.

c. Worms

Worms are programs originally developed to travel through systems and perform mundane tasks, such as data collection or ensure of old data. While they can be useful, if misprogrammed or programmed with malicious intent, they can be extraordinarily destructive. A virus attaches itself to a host program, but a worm is designed to spread across a computer network independently. While normally programmed to perform a task on a network, a worm may also simply replicate itself on target computers while it continues to spread across a network. The Morris worm discussed in Chapter IV serves as an example of the damage a "non-malicious" worm can cause.

d. Humans

Computer operators are the vehicles by which viruses, trojan horses, and worms are initially programmed and then inserted into computer systems. In addition to utilizing software attacks on a computer system, a cyberterrorist or hacker can attack a computer system through the vulnerability of its operators. The hacker community commonly refers to this as "social engineering"⁷². Using a social engineering tactic, a cyberterrorist may impersonate a computer technician and call individuals within the targeted organization to obtain information to penetrate a system. Once in possession of legitimate log on information, cyberterrorists will have "legal" access to a system and can insert viruses, trojan horses, or worms to expand their control of the system or shut it down.

e. Electro-Magnetic Pulse Weapons

While not nearly as widespread as viruses, there exists a class of weapons that destroy computers and electronics through an electromagnetic pulse⁷³. The capability now exists to generate an instantaneous electromagnetic pulse that will overload and destroy the sensitive circuitry in advanced electronics and computer systems without the previously required detonation of nuclear weapons in the upper atmosphere. Any system that is within the limited range of these weapons will be disrupted or have its electronic components destroyed. While there have been reports of the military using such weapons in the GulfWar, there are no indications that any terrorist organization possesses or has used these weapons against computer targets⁷⁴. Press reports from Japan indicate that the

⁷² Ira Winkler, "Case Study: Social Engineers Wreak Havoc," in *InfoWarCon'95 Conference Proceedings, September 7-8, 1995*, by National Computer Security Association (Carusle PA: NCSA, 1995), F-1.

⁷³ James W. Rawles, "High-Technology Terrorism," *Defense Electronics*, January 1990, p. 74.

⁷⁴ Neil Munro, "Microwave Weapons Stuns Iraqis," *Defense News*, 15 April 1992, Nexis, p.2.

AUM Shinrikyo cult, incriminated in the sarin gas attacks on Tokyo's subway was attempting to develop a high powered microwave weapon, ostensibly for use against humans⁷⁵. While suspected of being powerful enough to incinerate a human body, they may have intended this weapon for use against electronic targets as well. An electromagnetic weapon does not leave a crater like a conventional bomb, nor does it modify the operating system of a computer. As such, detection of an attack becomes more difficult. These weapons have been named HERF (High energy Radio Frequency) Guns and EMP/T (Electro Magnetic Pulse Transformer) Bombs by Winn Schwartau in testimony before Congress⁷⁶. In the same manner as a fertilizer bomb can be assembled by a conventional terrorist, a cyberterrorist can manufacture an EMP/T bomb out of readily available electrical and electronic components.

f. High Energy Radio Frequency (HERF) Gun.

It directs a blast of high energy radio signals at a selected target to disable it. A HERF Gun can shoot down a computer, cause an entire network to crash, or send a telephone switch into electronic chaos. Any of these effects can create denial-of-service scenarios. A HERF Gun is simple and easy to build.

⁷⁵ Yomiuri Shimbun, "Aum Linked with Microwave Weapons," *The Daily Yomiuri*, 11 June 1995, Nexis, p.4.

⁷⁶ Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunder's Mouth Press, 1994, pp 171-189.

CHAPTER 6

CONCLUSIONS AND RECOMMENDATIONS

The face of terrorism is changing to the worst. While the motivations remain the same, we are now facing new and unfamiliar weapons. The intelligence systems, tactics, security procedures and equipment that were once expected to protect people, systems, and nations, are powerless against this new, and very devastating weapon. Moreover, the methods of counter-terrorism that our world's specialists have honed over the years are ineffectual against this enemy. Because, this enemy does not attack us with truckloads of explosives, nor with briefcases of Sarin gas, nor with dynamite strapped to the bodies of fanatics. This enemy attacks us with one's and zero's, at a place we are most vulnerable: the point at which the physical and virtual worlds converge.

Cyberterrorism represents perhaps a major threat to developed countries. Though thankfully actual incidents of cyberterrorism have been extremely rare, and there are no known fatalities from acts of cyberterrorism, the threat is quite severe.

Verton argues that "Al Qaeda [has] shown itself to have an incessant appetite for modern technology" and provides numerous citations from bin Laden and other al Qaeda leaders to show their recognition of this new cyberweapon⁷⁷. In the wake of the 9/11 attacks, Bin Laden reportedly gave a statement to an editor of an Arab newspaper claiming that "hundreds of Muslim scientists were with him who would use their knowledge . . . ranging from computers to electronics against the infidels." Sheikh Omar Bakri Muhammad, a supporter of Bin Laden and often the conduit for his messages to the Western world, declared in an interview with Verton, "I would advise those who doubt al

⁷⁷ Dan Verton, *A Definition of Cyber-terrorism*, Computerworld, Aug. 11, 2003, [<http://www.computerworld.com/securitytopics/security/story/0,10801,83843,00.html>].

Qaeda's interest in cyber-weapons to take Osama bin Laden very seriously. The third letter from Osama bin Laden . . . was clearly addressing using the technology in order to destroy the economy of the capitalist states."

"While bin Laden may have his finger on the trigger, his grandchildren may have their fingers on the computer mouse," remarked Frank Cilluffo of the US Office of Homeland Security in a statement that has been widely cited. Future terrorists may indeed see greater potential for cyberterrorism than do the terrorists of today. Furthermore, as Denning argues, the next generation of terrorists is now growing up in a digital world, one in which hacking tools are sure to become more powerful, simpler to use, and easier to access.

Cyberterrorism may also become more attractive as the real and virtual worlds become more closely coupled. For instance, a terrorist group might simultaneously explode a bomb at a train station and launch a cyberattack on the communications infrastructure, thus magnifying the impact of the event. Unless these systems are carefully secured, conducting an online operation that physically harms someone may be as easy tomorrow as penetrating a website is today.

Paradoxically, success in the "war on terror" is likely to make terrorists turn increasingly to unconventional weapons such as cyberterrorism. The challenge before us is to assess what needs to be done to address this ambiguous but potential threat of cyberterrorism—but to do so without inflating its real significance and manipulating the fear it inspires. First, a distinction must be drawn between cyberterrorists and terrorists who happen to employ technology. A member of al-Qaeda who uses steganography and high-level encryption to communicate with other members of his cell is not a cyberterrorist, despite his use of advanced technology. Similarly, the recent news that both al-Qaeda and the Taliban have been distributing recruitment DVDs and websites into the southern and

eastern provinces of Afghanistan does not represent cyberterrorism; both of these instances involve somewhat traditional terrorists utilizing advanced technology. A cyberterrorist would utilize only technology and computers to achieve his goals—the more traditional elements of terrorism, like bombs, would at best play a peripheral role (there may be some overlap at some point, but for most purposes the distinction is useful). That being said, cyberterrorism is one of the biggest threats because so few are aware of what it could accomplish. A worm that changes a single 1 to a 0 in the telecommunications network would cripple the entire phone system, both landlines and cellular systems. Phones would simply not work.

The relative weakness of infrastructure and information systems to terrorist attacks is a necessary, but not sufficient condition for information age terrorism, which this thesis has grouped into conventional terrorism, and cyberterrorism. To address the level of threat posed by these two types of terrorism, this thesis has examined some weaknesses in the system, and also the possible motivation for the use of information warfare by terrorism. While weaknesses and vulnerabilities may exist in the system, and the tools to exploit these weaknesses may be developed or purchased by terrorists in the future, the present concern over an "electronic Pearl Harbor" may be slightly off base.

Information warfare tactics do not create terror in the same way as conventional terrorist tactics. As such, a shift in the definition of terrorism is required to group cyberterrorism with conventional terrorism. Including cyberterrorism in the overall category of terrorism allows scholars and policy makers to place this new threat into a known framework that provides the foundation for further study and the development of prevention and response measures. Building on classic terrorism, cyberterrorism may shift toward a more "demassified" threat with shifting state sponsorship. The purpose of this new type of terrorism may be to send a very specific message via disruption and destruction of

systems. New technology will expand the struggle between terrorists and counter-terrorist forces into cyberspace where "classic" offense, defense, and deterrence do not exist. Instead, both sides will be forced to deal with the new opportunities and drawbacks that exist in cyberspace. The experience of both the business community and the governments is valuable in determining how to combat this new threat. An effective combination of this collective experience will provide the best solution to the problem of countering cyberterrorism.

1. Shifting Definition of Terrorism

An examination of the elements of terror and symbolic violence highlighted the value of physical violence in the creation of terror. While not as effective in inducing terror, information warfare tactics allow tomorrow's terrorist to cause great disruption with lesser physical harm to individuals. The violence of the cyberterrorist exists in the virtual world of cyberspace. While conventional terrorism will still involve physical destruction of property and human life, cyberterrorism will utilize cyberviolence and "virtual" destruction of data in cyberspace. While directly causing lesser casualties, this action will still fulfill the goals of advertising, morale building, disorientation, and response provocation. Some cyberterror actions, such as attacking safety or control systems (avionics, air traffic control, etc.) have the potential to create cascading failures that will lead to loss of life. Cyberterrorists will in many cases, have the option of including destruction along with disruption to create terror and a more permanent result. While we have yet to see the combination of political motivation and criminal activity in cyberspace, we cannot disregard the potential of this type of terrorism.

2. Impact of Cyberterrorism on the Future

Information warfare tactics allow a terrorist group to operate without the support of a large terrorist organization or a wealthy state sponsor. In addition, terrorists will utilize the emerging cryptography and global telecommunications system to climb out of the "dragonworld" of covert communications and enhance their ability to communicate in a secure fashion with members scattered across the globe. These tactics may have several effects on future terrorist organizations.

a. Demassification

First, terrorist groups may become more "demassified." In *The Third Wave*, Alvin Toffler describes how society is shifting away from large, centralized organizations to smaller, more distributed elements⁷⁸. The ability to steal \$10 million electronically overnight, and the ability to exercise command and control utilizing "off the shelf" commercial technology may sound the death knell for state sponsored terrorism. Groups that formerly took direction and were controlled or supported by state actors, will now move into cyberspace, supporting themselves through criminal activities and removing the need for basing by becoming distributed organizations around the world. This lack of state control and funding will remove one of the key elements in present counter-terrorism planning—the punishment or coercion of the sponsoring state. The freedom from state imposed restraints will also allow terrorists to target *all* states in the future, not only those directed by the sponsor.

b. New State Sponsors

The lower level of support required to execute a cyberterrorist strategy may have the opposite effect, actually increasing state sponsorship. Poor states that did not have the

⁷⁸ Alvin Toffler. *The Third Wave*. New York: William Morrow and Co., 1980.

means to support an international terrorist organization are now becoming connected to the world via the Internet and new telecommunications systems. The increasing numbers of connections from states that have sponsored terrorism in the past, such as Iran, as well as those that have not, is a new threat. These states may view cyberterrorism as an ideal tool with which to strike the information dependent first world. Cyberterrorism may also appeal to states as it has the added benefit of plausible deniability. There will be no large money, material, or communications "trail" to lead back to the sponsor state.

c. Targeted Message

While the world (and terrorist groups) are demassifying, industry and business are pursuing more "targeted" production and advertising. This strategy attempts to focus the manufacturing and selling of products to a select audience. Technology is emerging to allow advertising to just those customers who are most likely to purchase a product. Terrorists in the information age may also mirror this trend, with new techniques and weapons that allow them to affect a target audience without resorting to violence against the general population. This technology also allows a terrorist message or action to affect many more people than was possible before. Thus, the "target" for terrorism can be as large or as small as the terrorist sees fit. The growing, worldwide, interconnectedness of individuals and organizations may change the role played by the media in past terrorist events. While terrorists have staged many events in the last 25 years to garner maximum worldwide media attention ('72 Olympics, World Trade Center bombing on September 11, Airplane hijackings), the exponential growth of the Internet and the introduction of Direct Broadcast Satellites with more than 500 channels and an 18" receive dish may allow terrorists to formulate, create, and distribute their own "news" to millions around the globe. Al Qaeda used the Internet and World Wide Web extensively to promote their cause and get their "message" to sympathetic audiences around the world.

d. Rise of Disruption

The final change that information warfare tactics may bring to terrorism is a shift in terrorism itself. In the future, terrorist organizations may move toward tactics that attempt to achieve the terrorist goals with lesser physical violence. This corresponds to the current thinking about the future of warfare. John Arquilla and David Ronfeldt have stated:

“Warfare is no longer primarily a function of who puts the most capital, labor, and technology on the battlefield, but of who has the best information about the battlefield. What distinguishes the victors is their grasp of information, not only from the mundane standpoint of knowing how to find the enemy while keeping it in the dark, but also in doctrinal and organizational terms”.⁷⁹

In the information age, shifting the definition of terrorism to include violence in cyberspace may be necessary, where electrons are attacked, in the same manner as physical violence is presently included.

Despite these changes, many "classical" terrorist organizations motivated by "conventional" objectives will remain viable. Terrorist groups, regardless of their level of sophistication, will adhere to the logic of symbolic violence and the creation of terror.

While it is likely that conventional terrorist groups will evolve into hybrid groups employing both violence and information warfare cyberviolence, we may see the creation of new and unique terrorist organizations unlike those of the past, where close personal ties and ideology were necessary to maintain security. The terrorist organization of the future may not have any "homeland" other than cyberspace. While it is difficult to track selected individuals in just one country or region, tracking a small number of individuals who could be anywhere on the globe, who can communicate in a secure and instantaneous fashion with each other, is likely to pose an order of magnitude increase in the problem.

⁷⁹ Arquilla & Ronfeldt, (Eds). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND, 2001, p.141.

e. New Tools for Attacker and Defender

The "information age" provides many tools to assist in countering conventional terrorism. It also presents a host of new problems associated with countering cyberterrorism. The standard offense/defense and prevention/preemption/disruption dynamics of counter and anti-terrorism in the physical world do not have direct counterparts in cyberspace. In the virtual world, a small number of individuals, with the right information, are as powerful as large state actors. The "balance of power" in cyberspace can shift in a matter of seconds, with the insertion or deletion of several lines of code to a program, or the installation of a new security protocol. The lessons from past conventional counter and anti-terrorism tactics are only of limited value in understanding the effectiveness of offense and defense in cyberspace.

The initiative in cyberspace does not necessarily rest with those pursuing an offensive strategy. In keeping with conventional terrorism, it is the terrorist group that normally attempts to seize the initiative by launching an offensive attack on a symbolic target. This attack is usually meant to undermine the belief that the government can protect its citizens. The government is then forced to reexamine and often change the way it attempts to maintain security. In cyberspace, no government has promised to guarantee "safety and security" as they have in the physical world. In the anarchic world of cyberspace, each individual serves as their own sovereign state. The government has addressed the security of individuals only in limited form, with passage of several laws concerning computer security. The commercial sector has attempted to defend the individual with the introduction of virus detection and encryption programs. Neither business nor government has advocated an offensive posture against computer hackers and potential cyberterrorists. The focus has, out of necessity, been directed toward defense. The use of offensive tactics would work well if the enemy could be

unambiguously identified. A skilled cyberterrorist can make the identification of those responsible, a cornerstone of conventional U.S. counterterrorism policy, exponentially more difficult in cyberspace. Even if an attacker in cyberspace can be identified, the range of responses open to the defender is somewhat limited. In the case of an unsophisticated hacker or criminal, access to the network can be denied.

3. Combating the Threat

Whether there will be another catastrophic Intelligence failure like September 11 or not, it is a question of *when*, not *if*. So it is just as important to prepare to manage the damage as it is to prevent it⁸⁰. The Defense Science Board suggests that “deterrence in the information age is measured more in the resilience of the infrastructure than in a retaliatory capability”⁸¹.

Cyberterrorism needs to be fought with the same breadth of measures and intensity accorded to terrorism. Hence there is a need for an appropriate framework for law enforcement and intelligence gathering to thwart the efforts of cyberterrorists. In the U.S., initiatives include the PDD 63 (President Decision Directive), the establishment of the NIPC (National Infrastructure Protection Center), the ISACs (Information Sharing and Analysis Centers) for the private sector owners of critical infrastructures, and Infragard, a community of professionals with an interest in protecting their information systems.⁸² The Bush Administration has released the National Strategy to Secure Cyberspace document to consolidate the U.S. government’s commitment to fight cyberterrorism and other cyber

⁸⁰ Richard K. Betts. *Fixing Intelligence*. Foreign Affairs, January/February 2002.

⁸¹ CSIS Task Force Report. *Cybercrime... Cyberterrorism... Cyberwarfare... Averting an Electronic Waterloo*. Washington D.C.: Center for Strategic and International Studies, 1998, p. 3.

⁸² CSIS Report. *Cyber Threats and Information Security: Meeting the 21st Century Challenge*. A report for the CSIS Homeland Defense Project. Washington D.C.: Center for Strategic and International Studies, May 2001.

threats. The enactment of such laws did not pass without opposition from various groups. There have been outcries by the libertarian groups who feel that such powers are too wide-ranging and can lead to a significant loss of electronic privacy. They further question the availability of checks and balances to ensure restraint and prevent abuse by the executive authorities. Other methods of combating cyberterrorists involve the use of software decoys. Installing advanced software and hardware applications that will protect your systems from cyberterrorism acts.

In some respects, protection against cyberterrorism is an internal and international issue. Below are some of the domestic and global actions that have been taken to help protect against cyberterrorism.

1987: The Computer Security Act of 1987 was passed, requiring US Federal agencies to identify systems that contain sensitive information and to develop plans to safeguard them.

1996: The President's Commission on Critical Infrastructure Protection was established to analyze the vulnerabilities of and threats to critical national infrastructures, including telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. The Executive Order stated that threats include physical threats as well as threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats") and called for the government and private sector to work together to develop a strategy for protecting them and assuring their continued operation.

1997: The President's Commission on Critical Infrastructure Protection concluded that the U.S. infrastructure is increasingly vulnerable to attack and that local, State, and Federal officials are not prepared to deal with the problem.

1998: The National Infrastructure Protection Center (NIPC) a new FBI command center to fight cyberattacks against the nation's critical computer networks^{3/4}was established.

1998: National Security Council aide Richard Clarke was appointed head of the new office on infrastructure protection and counterterrorism. A new U.S. initiative was begun to protect telecommunications systems, banks, telephone networks, air traffic control centers, and other public and commercial networks.

2001: The Office of Homeland Security was established to integrate and coordinate counterterrorism efforts in the wake of the September 11 attacks. Its mission includes "efforts to protect critical public and privately owned information systems within the United States from terrorist attack."

2001: An international cybercrime treaty was signed, uniting countries in the fight against computer criminals.

4. State's Response to the Problem

The problems posed by the emergence of cyberterrorism mirrors many of the problems presented by information warfare between states. What is the correct balance between government protection and commercial sector protection? The possible solutions run the gamut from a completely government to a completely commercial protection of information. The best solution will likely lie somewhere between these two poles.

a. Government Response to the Problem

The government, through a variety of agencies is responsible for the vast majority of counter and anti-terrorism activities and policies in their countries. Governments meet

with other states to negotiate cooperative agreements concerning the prosecution of terrorists and their sponsor states. The U.S. military has been utilized on several occasions to respond to terrorism and signal the resolve of the United States to counter terrorism by force if necessary. This situation is not mirrored in cyberspace, where borders are meaningless and international standards are generally set by multinational technical committees with little government input. The nature of cyberspace creates several fundamental questions. While the government is committed to defending the rights of citizens in the physical world, with force if necessary, it has not made the same sweeping commitment to its citizens in cyberspace. While a computer may be physically located in the United States, the majority of its users may reside in another country.

The issue at the Government level is how to protect critical infrastructure systems from intrusion, attack, damage, and disruption by cyberterrorists. In an attempt to generate preparedness for cyberterrorism, the U.S. government has developed the National Strategy to Secure Cyberspace⁸³. The three objectives of the plan are to 1) “prevent cyber attacks against America’s critical infrastructures, 2) reduce national vulnerability to cyber attacks, and 3) minimize damage and recovery time from cyber attacks that do occur.”

i) Reducing Vulnerability

In 1996, the U.S. General Accounting Office (GAO) produced a report on information security and computer attacks at the Department of Defense. Its recommendations for reducing vulnerability to cyberattack include the following steps, which can be effectively applied to all levels of government and all sizes of organization.

1. Have a clear and consistent information security policies and procedures.
2. Continuously assess vulnerability to identify security weaknesses at individual installations.

⁸³ White House. “National Strategy to Secure Cyberspace.” Executive Summary. Available at [www.whitehouse.gov]

3. Undertake mandatory correction of identified network/system security weaknesses.
4. Mandatory reporting of attacks to help better identify and communicate vulnerabilities and necessary corrective actions.
5. Assess the damage to reestablish the integrity of information compromised by an attacker.
6. Use awareness training to ensure that computer users understand the security risks associated with networked computers and practice good security.
7. Make sure that network managers and system administrators have sufficient time, training and expertise to do their jobs.
8. Be prepared to apply prudent use of technical solutions such as firewalls and smartcards.
9. Ability to respond to any incident by aggressively detecting and reacting to attacks and tracking and prosecuting attackers.

ii) System Protections

Currently there are no foolproof ways to protect a system. However, three broad approaches can be used to reduce vulnerability to cyberterrorism: isolation, encryption, and security.

Most military classified information is kept on machines with no outside connection, to prevent unauthorized access to the information. Although this method can protect certain data files, isolation is less effective in protecting a system that by its very nature requires interface with other infospheres.

Another approach that is related to isolation is the use of firewalls. Firewalls are hardware and software components that protect one set of system resources from attack by outside network users by blocking and checking all incoming network traffic. A firewall filters access to a network. It may take the form of a computer, router, or other communications

device, or it may be a network configuration. A firewall defines the services and access that are permitted to each user. It screens all communications to a system, including e-mail messages (which may carry logic bombs). One firewall method is to screen user requests to check if they come from a previously defined domain or Internet Protocol (IP) address. Another method is to prohibit Telnet access into the system.

Encryption is software technology that locks computerized information to keep it private. Only those with an "electronic key" can decipher the information. Encryption does not protect the entire system only the encrypted data. An attack (e.g., a virus) designed to cripple the whole system is unaffected by encryption.

Security is the protection of information, systems, and services against disasters, mistakes, and manipulation so that the likelihood and impact of security incidents is minimized. Since full isolation is virtually impossible, and encryption is aimed at protecting specific data, not systems, having a program for system security in place is a vital aspect of protecting critical infrastructures.

A balance must be found between too much security (very restrictive use, high cost) and too little security (unrestricted use, low visible cost, but high danger). It is important that the value of the information and processes in the system is determined, and the risks identified, so that appropriate countermeasures can be implemented. A cornerstone of countermeasures is risk analysis and security policy.

b. Commercial Response to the Problem

The actions taken by individuals and industry to combat the "hacker threat" are, at present, the best response to a portion of the terrorist information warfare threat. As we have seen, the confidentiality, integrity, and availability of data are critical in the information age. The growing ubiquity of encryption raises the threshold to a level where it is not remotely cost effective to attempt to "brute force" decrypt a message for its

contents. With the further introduction of smart cards and random password authentication, plus the addition of new communication protocols that prevent "spoofing" or fooling the network into thinking you are someone else, the confidentiality of data is becoming a reality. The new protocols, used with encryption and "digital signatures" will ensure the integrity of data as well. The availability of data remains a lucrative target for cyberterrorists at present. This target is rapidly disappearing with the growing redundancy of communications paths that are becoming available to data. The loss of one ATM network did not cause a shutdown of all the ATMs, it only affected about 2% of ATM users.

All of the above actions were driven by the commercial sector, not by the government. We have entered an age where the military and the government no longer have the capability to develop technology and give the "spin-offs" to the commercial sector. Rather, the commercial sector has taken the lead in innovation and development of technology and the government and military are constantly trying to "spin-on" this technology by adapting civilian products to military use. This has leveled the playing field in cyberspace, for a cyberterrorist has the same access to this technology as the government.

c. Government/Commercial Response

A composite Government/commercial response may be the most beneficial in protecting against a cyberterrorist threat. The networks of the United States can be viewed in much of the same manner as postal routes. There are laws that protect the individual from unauthorized tampering with mail while it is in transit to its recipient regardless of the carrier (U.S. Postal Service, Federal Express, United Parcel Post, etc.). Senders of an authorized package have every right to assume that the government will ensure that their package is delivered intact and unopened to its final destination. In extreme cases, such as

letter bombs and illegal materials being sent, the government becomes involved in tracking and prosecuting those who abuse the system at the expense of public safety or in violation of the law. Materials that are detrimental to the national security of the United States naturally receive much attention from Federal authorities. It is up to the sender of each package to ensure that they properly wrap it for shipment. If it is information that is unimportant, they can send it on a postcard, with the writing openly visible to anyone who may see the card. The more sensitive the information, the more tightly wrapped the package becomes. Encryption serves as the "wrapping" on the message sent out via public networks. The more sensitive or important the information, the higher the level of encryption required to ensure that the message will be authentic and intact when it reaches its destination. While unencrypted E-mail may be adequate for some matters, other correspondence will require increasingly higher levels of classification for protection. With the diffusion of encryption technology, it will become increasingly easy to ensure confidentiality of all messages. In the postal analogy, the government does not guarantee service by all companies in the delivery service. Rather, it maintains a level of general safety in which all can operate. Thus, both public and private utilities and telecommunications carriers can expect the government to become involved when a major problem occurs. While each company is responsible for "low level" problems, such as routine security at warehouses and the collection of overdue bills, the government will assist in correcting "high level" problems where lives are at stake due to the content of the material being shipped. The government, in effect, protects the individual from the carrier and the carrier from the individual.

The difficulty in the age of information is determining what constitutes a cyberspace letter bomb and how it is different from a benign cyber-postcard. Where is the level between "low level" and "high level" problems to be drawn? The anarchic nature of

cyberspace has prevented any attempts at close regulation by the government. Every individual must take a certain level of responsibility for their own "safety" in cyberspace. While U.S. citizens have a reasonable expectation of security within the borders of the United States, the ability of the U.S. government to protect them decreases as they venture further abroad. The same is true in cyberspace, where a user in a closed network had a reasonable expectation of security. As soon as users connect that network to the Internet, it is open for attack by anyone. It is up to the user to prevent low level attacks by "locking his doors" and following good computer security practices. In so doing, a computer user can defeat all but the most advanced opponents in cyberspace. In cases where the information is deemed to be sufficiently important, the government can be called in to assist in defense of that information and its associated network.

5. International Response to the Problem

Cyber terrorism is a fairly recent threat; therefore, there is still speculation as to who is ultimately responsible for combating cyber terrorism. The issue is how to protect critical infrastructure systems from intrusion, attack, damage, and disruption by cyberterrorists. Developed countries must consider the following elements when building a counter-Cyberterrorist program:

- They must accept that while the theories of terrorism stand true, the way in which they approach counter-terrorism, in this case, counter-CyberTerrorism, must change.
- They must cooperate and share intelligence in ways they have never have before.
- They must enlist the assistance of those individuals who understand the weapons they are facing and have experienced fighting these wars.
- They must learn the new rules, the new technologies, and the new players.

Unfortunately, one cannot learn how to fight this very unconventional warfare from someone who hasn't been there, nor from someone whose experience is in the old ways and old technologies. The old data processing, auditing, and computer security models in use today are obsolete. On this battlefield, against this weapon, the terrorist is already far ahead. The building of a counter-CyberTerrorist team must be real-time and dynamic, as the weapons will continually change, to morph, in an attempt to beat you, your systems, and your people.

Further, there is a real danger that cyber terrorists, hostile nations, and others will launch attacks that cause catastrophic damage, potentially leading to loss of life or widespread economic failure. The question arises then whether an international cyber arms control treaty might diminish the criminal and national security threats, while promoting greater cyber peace. Such a treaty might pertain to the development, distribution, and deployment of cyber weapons, or it might apply only to their use. It might relate primarily to criminal law, or it might govern the conduct of nation states in the domain of international law.

The purpose of this paper is to address obstacles and options for implementing a cyber arms control treaty. It is concerned mainly with computer network attacks and the cyber weapons deployed in those attacks. These weapons ("hacking tools") include software and methods for sabotaging systems and data and for launching computer viruses, worms, and denial-of-service attacks. After reviewing obstacles, the paper presents options for overcoming these obstacles. Particular attention is given to the Council of Europe's (CoE) draft Convention on Cyber Crime. If adopted, the convention will be the first international treaty to address criminal law and procedural aspects of various criminal acts against computer systems, networks, and data. As official observers, the United States, Canada, Japan, and South Africa could sign along with the European members.

The treaty has raised significant concerns regarding privacy and corporate liabilities and responsibilities, however, so its final outcome is yet to be determined. Obstacles to be effective, a cyber arms control treaty must overcome obstacles in several areas: enforcement, security, privacy, free speech, corporate liabilities and responsibilities, and foreign policy.

a. Privacy and Personal Freedom

To investigate crimes in cyberspace, law enforcement agencies need the capability to search and seize digital evidence and to intercept network communications. To facilitate these operations, they have asked for hardware and software tools and, in some cases, additional legal authorities. In the United States, for example, the FBI developed Carnivore, now called DCS1000, to support court-authorized Internet wiretaps. When installed at a subject's Internet Service Provider, DCS1000 intercepts particular message traffic belonging to the subject, for example, all e-mail messages sent to or from the subject, as specified in the court order. In the United Kingdom, the Regulation of Investigatory Powers (RIP) bill has provisions that facilitate government monitoring of Internet traffic and provide access to encryption keys. These law enforcement advances have raised privacy concerns. Opponents of Carnivore argue that the tool could be misused in order to conduct mass surveillance or otherwise acquire evidence that was not legally permitted, although no evidence of abuse was put forth. Opponents of RIP argue that the ability of the government to demand encryption keys sets a dangerous precedent. My understanding, however, is that the British government cannot compel keys from parties who claim to have lost or forgotten them. The Council of Europe's draft Convention on Cyber Crime has been criticized for failing to address privacy issues concerning access to stored data and electronic surveillance. The European Union

Advisory Body on Data Protection and Privacy (“Working Party”) expressed the opinion that the draft Convention did not adequately harmonize the safeguards and conditions for protecting privacy among signatory states. Data about an individual could be handed over to foreign governments with lower standards for privacy protection than required by EU countries. The Center for Democracy and Technology found the treaty to be unbalanced: “it includes very detailed and sweeping powers of computer search and seizure and government surveillance of voice, email and data communications, but no correspondingly detailed standards to protect privacy and limit government abuse of such powers.” If a cyber arms control treaty prohibited certain cyber weapons, the process of policing the Internet for these weapons would raise additional privacy issues. Scanning the personal computers of citizens would violate the privacy laws of many nations. Free Speech Restrictions on cyber weapons, particularly source code and scripts, would raise significant legal issues in countries with laws protecting speech. In the United States, speech is protected under the First Amendment, and software is considered to be a type of speech. Not all forms of speech are given full legal protection, however.

b. International Agencies

In the battle against cyber terrorism, Interpol has played a significant role on the international level. Interpol has 178 member countries, making it the second largest international organization, second only to the United Nations. Interpol serves as a link between law enforcement agencies of member countries. Member countries give information to Interpol to disperse among other member countries, such as wanted criminals, missing persons, and stolen property. Interpol also sponsors working groups on many international criminal issues, such as computer crime, corruption, environmental crime, trafficking in women and children, and other issues. Furthermore, Interpol has a database containing over 300,000 criminal files.

In order to combat cyber terrorism, Interpol is attempting to facilitate data sharing between member nations, conducting operational information analysis, sponsoring training in cyber terrorism issues, and providing intelligence to member nations.

Another step being taken on the international level to combat cyber terrorism is the formulation of joint working groups. An example of this is the India – U.S. joint working group on counter terrorism. The working groups have been able to increase countries' exchange of information, strengthen investigative cooperation, facilitate the signing of mutual legal assistance treaties, and have accomplished several other significant anti terrorism agreements. The India – U.S. joint working group also introduced a bilateral cyber security forum, specifically focusing on cyber terrorism issues and information security.

6. Difficulties in Implementing Security Measures

Although there are many protective measures available for private corporations, there are several hurdles preventing corporations from implementing them. First, implementing all of the necessary protective measures is expensive for private corporations. Depending on the size of the corporation, it could cost hundreds of thousands of dollars for a consultant to determine the corporations' vulnerabilities and install protective measures.

Additionally, security technology advances fairly rapidly, and the cost of new and updated security systems and software may become expensive. Also, educating the majority of a corporation's employees on cyber terrorism and preventative measures can be expensive.

Second, determining a corporation's computer systems vulnerabilities, installing security software, and upgrading it is very time consuming. [209] It takes time away from what the corporation was originally formed, and decreases profits.

Third, many of the security systems and complex technological advances in cyber terrorism protective software are confusing and difficult to learn. It often takes a computer security specialist to determine what the corporation needs for security and how to install it.

Finally, many private corporations do not want to report cyber terrorist incidents to the authorities. It is embarrassing for a private corporation to have its network's security breached. Also, this type of event causes negative publicity for the corporation. The corporation's competitors could use this information against them, and the corporation will most likely lose business.

Although the preceding hardships make preparing for and protecting against a cyber terrorism attack difficult, the current risk of imminent cyber terrorism attacks are too high to neglect implementing a security system. All it takes is one sophisticated and complex attack to destroy a small, medium, or large corporation. If the attack does not ruin the corporation, the cost of the repairs may be extremely high, and the corporation's goodwill may be lost.

7. Recommended Strategies to Counter Cyberterrorism

The difficulty in pinning down exactly what needs to be done is the biggest challenge that the securitizing actors face with regards to cyberterrorism. It's clear that doing nothing will only leave critical systems open to attack. It is possible for a Wall Street firm to be hacked and shut down, which would create absolute havoc. An exact course of action, though, is far from certain: better training, perhaps, or maybe just more time to develop usable defenses.

As a conclusion for this thesis, in order to counter Cyberterrorism, I recommend a program that is based on some form of international cooperation. First, the transnational

nature of cyberterrorism calls for a transnational response. The actions of individual states are insufficient. Affected states need to agree on the kinds of conduct that should be proscribed and adopt laws making such conduct criminal.

In addition to ensuring universal condemnation of serious forms of misconduct, any effective system for punishing cyberterrorism will require the full range of cooperation afforded by states to each other in mutual legal assistance and extradition treaties. The nature of cyberterrorism also requires national commitments to undertake special efforts to search for, secure, and preserve usable evidence. The speed with which cyber-related evidence can be lost, and the frequency with which it will be located in foreign jurisdictions, makes it necessary to have the consent of states in advance to some forms of searches that reach into their territories, as well as agreements to assist in seizing equipment and other assets and to provide usable evidence and other forms of cooperation. It is insufficient, moreover, for states merely to agree to perform conventional services for each other. They will have to be prepared to implement technologically adequate measures, as these are developed.

Securing agreement from all states connected to the international information infrastructure for these far-reaching forms of cooperation will certainly be more difficult than securing agreement on the conduct to be proscribed. No multilateral consensus yet exists on providing legal assistance and extradition in cyber cases. States must be convinced that such cooperation is in their best interests, as in the areas of civil aviation and international banking. To overcome claims or fears of improper extraterritorial activities, states should agree that all measures undertaken in pursuing a cyber investigation will be performed in a manner consistent with the law of the state that is asked to perform such services. To overcome claims or fears that cyber investigations or prosecutions could compromise domestic constitutional protections, no state should be

required by the international commitments it undertakes to compromise its national standards of conduct.

Because cyber systems and programs are designed with efficiency and ease of use rather than security as the primary objective, states should consider adopting technological measures that go beyond investigative cooperation. Technological breakthroughs, of the sorts to enhance protection against, and to improve investigation and prosecution of, cyberterrorism should be encouraged and widely implemented. To achieve such cooperation will require overcoming the antiregulatory perspectives of private-sector participants who have built and continue to develop the information infrastructure.

One necessary response to this resistance is to build private sector control into the process of developing solutions and formulating standards and practices for enhancing cyber security.

A program based on these principles and proposals should eventually overcome resistance to a multilateral convention to deal with cyberterrorism. Escalating damage and the inadequacy of current efforts are increasing the pressure on governments—and through them on Internet Service Providers (ISPs), major companies, and private standard-setting bodies—to respond effectively. Efforts by governments reacting to recent major attacks have focused on seeking new powers, such as stiffer sentences, the right to arrest and/or search without prior judicial approval, and other inadequate and damaging measures. Knowledgeable legislators and industry leaders should eventually turn to more useful and appropriate options.

Apart from the dangers of increasing police powers, relying on prosecutors to plan and implement solutions in a highly technical area in which private control is regarded as a substantial advantage may well be ineffective even in satisfying the need for better security.

Those who support adoption of a multilateral approach to deal with this transnational problem must be encouraged by the fact that states have consistently adopted multilateral solutions to deal with technologies that affect populations across national boundaries. As technology advances, new technologies with transnational impact that require transnational controls have repeatedly led to multilateral arrangements; agencies have been created to deal with such international areas as air travel, shipping, and telecommunications.

The information infrastructure faces analogous challenges. Its security and efficiency will be materially increased through international implementation of principles, standards, and practices specifically designed for this field of activity. The optimum manner of achieving these objectives in this particular field is a multilateral treaty with the necessary commitments to cooperate in investigating and prosecuting an agreed range of conduct, and an international agency with authority to accomplish (through measures analogous to those widely in use by other agencies) the legal and technological objectives essential to create a more secure cyber world.

8. Futuristic Perspective

While the government may be called upon to assist in the defense of cyberspace, the doctrinal and organizational foundations have not yet been established to allow for this involvement. Further study of this problem is necessary to ensure that any government involvement is proportional and effective. While cyberspace can place individuals and states on equal footing, the state clearly retains an advantage in the physical world. This advantage may provide a useful tool in the prosecution of cyberterrorism. While the doctrine of asymmetric response was utilized during the Cold War to deter a nuclear exchange, a cyberspace equivalent of this doctrine may prove useful in the information

age. If a state commits to defending cyberspace, the first course of action is likely to be the securing of systems to prevent unauthorized access. By raising the threshold of skill and technology required to penetrate a system, amateurs and unskilled cyberterrorists may be deterred from pursuing an offensive in cyberspace. By securing systems from "low level" attacks, the various government agencies involved in counter and anti-terrorism will be free to pursue the "high level" threats that are sure to exist in cyberspace. It remains to be seen if an offensive response, such as a military strike against a computer center or selected organizations, will be tolerated by the citizens of the United States. Will people be willing to launch an air strike against computer terrorists in the same fashion as they were launched against terrorists training bases in Afghanistan? The implications of an offensive, asymmetric response to the terrorist problem must be explored, as a response that exists exclusively in cyberspace may not be sufficient to deter, or even slow down a cyberterrorist. At the dawn of the information age, the borders of any State are no longer secure. We must recognize the potential threat and adjust our thinking to formulate an effective individual and state response.

BIBLIOGRAPHY

Books:

J. Arquilla & D. Ronfeldt, (Eds). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND, 2001.

Matthew G. Devost. *Hackers as a National Resource. Information Warfare – Cyberterrorism: Protecting Your Personal Security in the Electronic Age*. Winn Schwartau (Ed). Second Trade Paperback Edition. New York: Thunder's Mouth Press, 1996.

James F. Dunnigan. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press Books, 2002.

Bruce Hoffman. *Inside Terrorism*. Paperback Edition, London: Indigo, 1999.

Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunder's Mouth Press, 1994.

Alvin Toffler. *The Third Wave*. New York: William Morrow and Co., 1980.

Alvin Toffler and Heidi Toffler. *War and Anti-War*. New York: Little, Brown and Co., 1993

Edward Waltz. *Information Warfare: Principles and Operations*. Massachusetts: Artech House, Inc., 1998.

Articles:

Illena Armstrong. "Real Risk or Shadow? The Threat of Cyberterrorism". *Articles and Features*, January 2003. [<http://www.scmagazine.com>].

Richard Clarke, "Vulnerability: What Are Al Qaeda's Capabilities?" *PBS Frontline: Cyberwar*, April 2003. [<http://www.pbs.org>].

Barry C. Collin. "The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge." [<http://afgen.com/terrorism1.html>]

Scott Berinato. "The Truth About Cyberterrorism." 15 March 2002
[www.cio.com/archive/031502/truth_content.html]

Computer Emergency Response Team Coordination Center (CERT / CC) Statistics 1988-2003. [http://www.cert.org/stats/cert_stats.html].

CSIS Report. Cyber Threats and Information Security: Meeting the 21st Century Challenge. A report for the CSIS Homeland Defense Project. Washington D.C.: Center for Strategic and International Studies, May 2001.

CSIS Task Force Report. "Cybercrime... Cyberterrorism... Cyberwarfare... Averting an Electronic Waterloo". Washington D.C.: Center for Strategic and International Studies, 1998.

Dorothy E. Denning. "Information Warfare and Security". New York: ACM Press 1999.

Dorothy E. Denning. "Cyberterrorism". Global Dialogue, Autumn 2000.
[<http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc>].

Dorothy E. Denning. "Cyberterrorism". Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, May 23, 2000. [<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>].

Dorothy E. Denning. "Is Cyber Terror Next?" Georgetown University, November 2001.
[<http://www.ssrc.org/sept11/essays/denning.htm>].

Ronald L. Dick. "Cyber Terrorism and Critical Infrastructure Protection". 24 July 2002
[www.fbi.gov/congress/congress02/nipc072402.htm]

Brian Fonseca, and Heather Harreld. "Guarding Against Cyberterrorism." 17 October 2001
[www.infoworld.com/articles/fe/xml/01/10/22/011022fealert.xml]

Sarah Gordon and Richard Ford. "Cyberterrorism?". Symantec Security Response White Paper 2002.

Mark Grossman. "Cyberterrorism." 15 February 1999
[www.mgrossmanlaw.com/articles/1999/cyberterrorism.htm]

Serge Krasavin. "What is Cyberterrorism?", Computer Crime Research Center, Apr. 23, 2004. [<http://www.crime-research.org/analytics/Krasavin/>].

Martin Libicki. "What is Information Warfare", ACIS Paper 3. Washington, D.C.: National Defense University, August 1995.

David Love. "Is Cyberterrorism a Serious Threat to Commercial Organizations?" SC Infosec Opinionwire. February 2003.

Ellen McCarthy. "Americans Fear Cyberattacks from Terrorists", Study Shows. The Washington Post. Washington D.C.: September 3, 2003.

Michael J. Miller. "The Cyberterrorism Threat."
[www.pcmag.com/article2/0,4149,61365,00.asp]

Esteban Parra. "The Nation's Computerized Infrastructure is an Obvious Terrorism Target."
[<http://www.delawareonline.com/newsjournal/business/2002/12/16thenationscompu.html>]

Mark M. Pollitt. "Cyberterrorism – Fact or Fancy?"
[www.cs.georgetown.edu/~denning/infosec/pollitt.html]

Paul Rodgers. Protecting America Against Cyberterrorism. U.S. Foreign Policy Agenda.
Volume 6, Number 3, November 2001

Symantec Security Response Newsletter, Oct 2003. [<http://securityresponse.symantec.com>].

Timothy L. Thomas. "Al Qaeda and the Internet: The Danger of "Cyberplanning".
Parameters. Spring 2003.

Dan Verton, "A Definition of Cyber-terrorism", Computerworld, Aug. 11, 2003,
[<http://www.computerworld.com/securitytopics/security/story/0,10801,83843,00.html>].