NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

INFORMATION AGE TERRORISM:
TOWARD CYBERTERROR

by

Matthew J. Littleton

December, 1995

Thesis Co-Advisors: John Arquilla
James Wirtz

Approved for public release; distribution is unlimited.

19960405 093

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1995	Master's Thesis

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
INFORMATION AGE TERRORISM: TOWARD CYBERTERROR	
6. AUTHOR(S) Matthew J. Littleton	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited.	

13. ABSTRACT *(maximum 200 words)*

The growing ubiquity of computers and their associated networks is propelling the world into the information age. Computers may revolutionize terrorism in the same manner that they have revolutionized everyday life.

Terrorism in the information age will consist of: conventional terrorism, in which classic weapons (explosives, guns, etc.) will be used to destroy property and kill victims in the physical world; technoterrorism, in which classic weapons will be used to destroy infrastructure targets and cause a disruption in cyberspace; and cyberterrorism, where new weapons (malicious software, electromagnetic and microwave weapons) will operate to destroy data in cyberspace to cause a disruption in the physical world.

The advent of cyberterrorism may force a shift in the definition of terrorism to include both disruption and violence in cyberspace in the same manner as physical destruction and violence. Through the use of new technology, terrorist groups may have fewer members, yet still have a global reach. The increasing power of computers may lower the threshold of state sponsorship to a point where poor states can become sponsors and rich states are no longer necessary for terrorist groups to carry out complex attacks.

This thesis explores the shift toward information warfare across the conflict spectrum and its implications for terrorism. By examining the similarities and differences with past conventional terrorism, policymakers will be able to place information age terrorism into a known framework and begin to address the problem.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Information Warfare, Terrorism, Cyberterrorism, Technoterrorism, Counterterrorism	150
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

Approved for public release; distribution is unlimited.

INFORMATION AGE TERRORISM: TOWARD CYBERTERROR

Matthew J. Littleton
Lieutenant, United States Navy
B.A., Duke University, 1990

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF ARTS IN NATIONAL SECURITY AFFAIRS

from the

NAVAL POSTGRADUATE SCHOOL
December 1995

Author: _____
Matthew J. Littleton

Approved by: _____
John Arquilla, Thesis Advisor

_____
James Wirtz, Thesis Advisor

_____
Frank Teti, Chairman
Department of National Security Affairs

ABSTRACT

The growing ubiquity of computers and their associated networks is propelling the world into the information age. Computers may revolutionize terrorism in the same manner that they have revolutionized everyday life.

Terrorism in the information age will consist of: conventional terrorism, in which classic weapons (explosives, guns, etc.) will be used to destroy property and kill victims in the physical world; technoterrorism, in which classic weapons will be used to destroy infrastructure targets and cause a disruption in cyberspace; and cyberterrorism, where new weapons (malicious software, electromagnetic and microwave weapons) will operate to destroy data in cyberspace to cause a disruption in the physical world.

The advent of cyberterrorism may force a shift in the definition of terrorism to include both disruption and violence in cyberspace in the same manner as physical destruction and violence. Through the use of new technology, terrorist groups may have fewer members, yet still have a global reach. The increasing power of computers may lower the threshold of state sponsorship to a point where poor states can become sponsors and rich states are no longer necessary for terrorist groups to carry out complex attacks.

This thesis explores the shift toward information warfare across the conflict spectrum and its implications for terrorism. By examining the similarities and differences with past conventional terrorism, policymakers will be able to place information age terrorism into a known framework and begin to address the problem.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As the world enters the information age, the military 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.

This thesis identifies three categories of potential information age terrorism: conventional terrorism, technoterrorism, and cyberterrorism. Conventional terrorism destroys or threatens a symbolic target of violence in the physical world. Conventional terrorists may use information warfare tactics to plan and execute these actions more effectively. Technoterrorism is designed to have an effect in cyberspace using physical means. This type of terrorism includes bombing infrastructure targets (power, telecommunications, etc.) to create a disruption in cyberspace. Technoterrorists do not utilize physical destruction, such

as bombing a power station, to convey a message. Rather, they rely on the attendant cyberspace disruption to garner publicity for his cause. Cyberterrorism is terrorism that operates exclusively in cyberspace. The cyberterrorist could utilize an entirely new class of weaponry, possibly including malicious software or electromagnetic pulse generators, to manipulate or destroy information in cyberspace. Because cyberterrorists do not operate using "conventional" techniques, the lessons learned from previous counter and anti-terrorism efforts might be of limited value.

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.

I. INTRODUCTION

Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb[1]

A. BACKGROUND

As the world enters the 21st century, the information revolution will continue to propel the United States into the "third wave" of development according to Alvin and Heidi Toffler.[2] The shift from an industrial economy and society to one focused on information and its transfer will characterize the third wave. As discussed in *The Third Wave* and their most recent work, *War and Anti-War*, the way a state wages war is similar to how it makes wealth. This idea might be applied to terrorism and revolutionary violence.

Lewis Gann's *Guerrillas in History* provides an overview of substate violence across history.[3] Occasionally, as in the Welsh use of the longbow, substate groups possess weapons superior to those of the state. Substate actors, unless being supplied by another state, normally possess weapons that are inferior to those of the target state. They often use weapons stolen from, or discarded by, the state. As the technology, complexity, and lethality

---

[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.

[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).

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." 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.

As the world shifts into the "third wave," where information and its control are rapidly becoming *the* most important considerations for the advancing societies of the first world, will we 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 under defended targets, (embassies, airplane hijackings, hostage taking, airplane bombing) they have done so through evolution, not innovation. Bruce Hoffman contends, "What innovation does occur is mostly in the methods used to conceal and detonate explosive devices, not in their tactics or in their 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

---

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

it is merely a matter of time before we are faced with a major information warfare attack, there are several reasons that terrorists may not actively pursue these techniques.

B. PROBLEM STATEMENT

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. The United States 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* people to have an effect *on* people. However, cyberterrorism may utilize a 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. This cyberspace disruption would cause a disruption in the physical world. The violence that is normally associated with terrorism may shift into "cyberspace" where bits and bytes, not people, are attacked. To understand the potential shift in terrorism, this thesis splits information age terrorism into three categories: conventional terrorism, technoterrorism, and cyberterrorism. Appendix A provides a summary of the critical elements of each category.

This thesis will also analyze 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; it might cause serious damage in the future. While it may not fit accepted definitions of terrorism, 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 IW tactics in the third wave.

C. DATA

While the United States 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

---

[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) I-9.

examination of all computer related incidents but it is sufficiently broad to cover the entire "low intensity" spectrum of conflict.

This thesis will examine the role of information warfare in espionage and crime using cases involving the United States. The role of telecommunications assets in the Solidarity movement in Poland, the Tiananmen Square uprising, and the Zapatista movement in Mexico will be highlighted to show the increasing value of information warfare to insurgents and rebels and the increasing importance of computer connectivity. Exploring the role computers and networks have played in terrorist actions since 1970 will identify the trend in terrorism toward infrastructure warfare, technoterrorism, and cyberterrorism. Finally, the 1988 Internet Worm incident caused by Robert Morris will be utilized as an example of both the costs and benefits information warfare tactics offer to a terrorist.

D. LIMITATIONS

Information warfare is a concept that embraces many elements beyond simply attacking computers and communications networks. This thesis will, however, focus primarily 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.

II. AN EVOLVING CONCEPT

A. INFORMATION AGE TERRORISM

Terrorism will change 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 Affairs." Information age terrorism may take on three distinct forms: conventional terrorism, technoterrorism, and cyberterrorism. While conventional terrorism will still rely on physical violence, terrorists acquisition of high technology information warfare capabilities will allow a shift toward tactics focused on disruption rather than destruction. Information age terrorism, while continuing to use "conventional" weapons, will also employ weapons radically different from those used in conventional terrorism. This shift toward disruption in cyberspace, through the use of new weapons and without the use of violence in the physical world, may force a redefinition of the classic conception of terrorism.

1. Information Warfare

The definition of Information Warfare has been extensively debated in the open press. The Department of Defense has a classified definition of Information Warfare contained in DOD Directive TS3600.1, but the public debate on the subject will be sufficient for the purposes of this thesis. 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":

> 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 knows 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]

Cyberwar is 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 systems, 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.

---

[6]John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, 12 (1993): 144.

[7]Arquilla and Ronfeldt, 146.

The National Defense University (NDU) 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 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]

Martin Libicki of NDU has also examined the concept of Information Warfare and its implications for the future. In his Advanced Concepts and Technology paper, "What is Information Warfare?" Libicki 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 warfare.[9] While most of these forms of conflict fall into the military realm, each of them is applicable to terrorism in the

---

[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.

emerging information age. The form described as hacker war (warfare against computer networks) is split into three areas by Libicki: the physical, the syntactic, and the semantic.[10] The physical attack of computer networks is classified as technoterrorism by my typology. The attack of computer systems at the syntactic level (attack on the flow of electrons within the network) and at the semantic level (attacks on the veracity of a network's information--fooling the computer into producing an output that is incorrect) are defined as cyberterrorism because they exist exclusively in the realm of cyberspace.

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 the 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

---

[10]Libicki, Chapter 7.

information warfare. The fundamental goal of warfare is to change the mind of the enemy and convince him to do your will. The goal of information warfare is to accomplish this through the manipulation of the enemy's ability to control information. This places information warfare in the camp of Sun Tzu. Michael Handel captures the essence of information warfare by quoting both Clausewitz and Sun Tzu who states, "For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill." This effort to win without fighting runs counter to Clausewitz, who believed that combat and bloodshed were an integral part of warfare. "Kind-hearted people might of course think there was some ingenious way to disarm or defeat and enemy without too much bloodshed, and might imagine this is the true goal of the art of war. Pleasant as it sounds, it is a fallacy that must be exposed."[11] While contradictory, both quotes apply to terrorism in the information age. 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."

---

[11]Michael I. Handel, *Masters of War: Sun Tzu, Clausewitz and Jomini* (London: Frank Cass and Co., 1992), 75.

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 option open to terrorists.

a. Command and Control Warfare (C2W)

Chairman of the Joint Chief's of Staff Memorandum of Policy Number 30, "Command and Control Warfare," identifies Command and Control Warfare (C2W) as the military component of information warfare.[12] 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.

---

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

Figure 1 displays how offensive and defensive C2W is viewed in the military.[13]

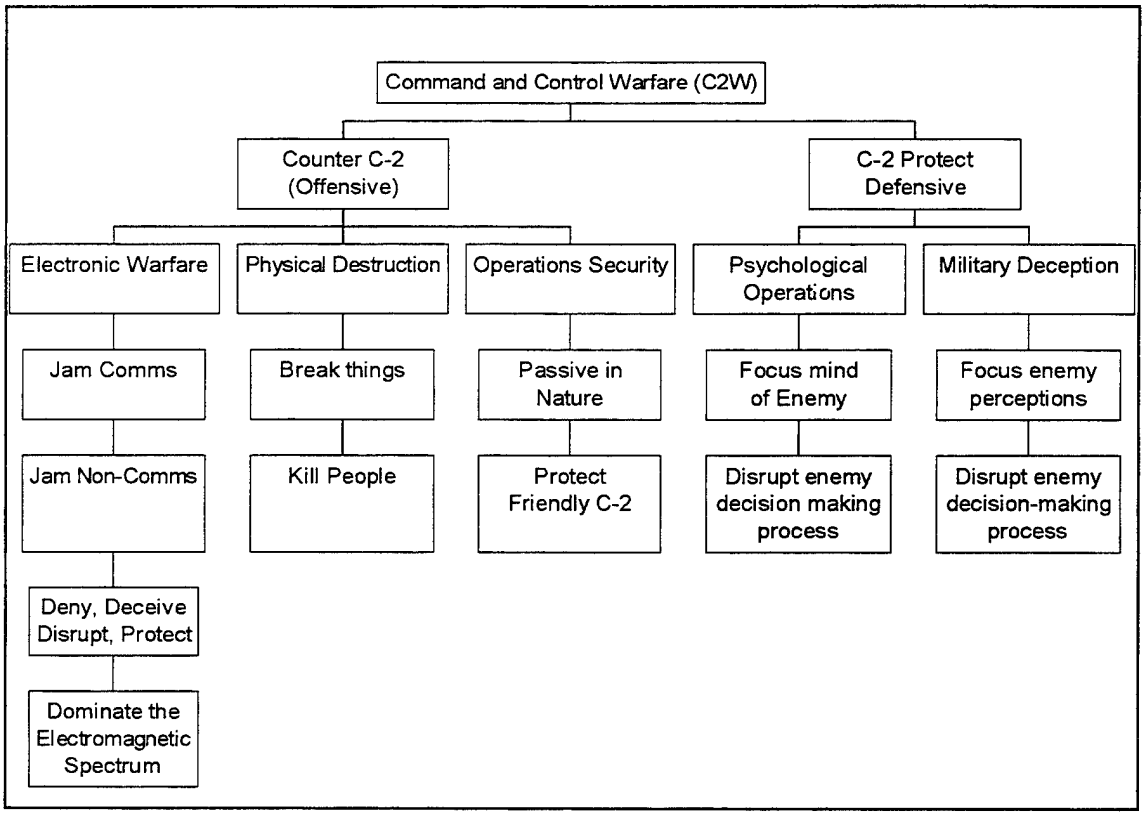

Figure 1

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 workings of terrorist organizations.

---

[13]Wayne J. Rowe, *Information Warfare: A Primer for Navy Personnel* (Newport: U.S. Naval War College, 1995), 10.

Properly 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 terrorist group 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 C2 structure, the defending group may find it most effective to pursue an offensive strategy in an effort to destroy the terrorists. If, however, the terrorists' 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 surveillance.[14] With the rise of secure voice and data communications (i.e., Pretty Good

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

Privacy (PGP) for E-mail and PGPphone for Internet voice communication encryption), 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 (by accident, natural causes, or malicious action), 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 they 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 buildings 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, an 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."[15]

The Defense Information Systems Agency, a branch of the 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

---

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

characterized by: no geographic, national, or temporal boundaries, no ownership, laws, or identity cards.[16]

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. Cyberterrorism

The term cyberterrorism refers to the use of information warfare tactics and techniques by terrorist organizations to affect cyberspace. The cyberterrorist will operate exclusively within cyberspace and will not physically destroy any of the infrastructure that supports the existence of cyberspace. While cyberterrorists wish to have an impact on the actions of real people in the real world, they operate within the virtual world of cyberspace to manipulate these actors. Thus, if cyberterrorists wished to take down a telephone system or an electric grid, they would attack the computers controlling the system and not its subsidiary physical components.

a. Weapons of the Cyberterrorist

The weapons of the cyberterrorist are not designed to kill people or break physical objects. Rather, they exist exclusively to destroy or modify computer data. The weapons and the targets are the electrons moving within cyberspace. While it is possible to

---

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

attack this data without any human interfaces, the human is usually the weakest link in a computer system.

Joseph Seanor of CIBIR Corporation, a computer crime investigative group, recently discussed the "Methods of Operations" of Cyberterrorists. His definitions provide a useful starting point to examine how cyberterrorists may attack their targets. The critical element in cyberterrorism, and information warfare in general, is knowledge. While the "tools" of the cyberterrorist (computers, modems, phone connections) are nearly universally available, the knowledge of computer systems and their weaknesses (while becoming increasingly common) is not as easily obtained. Individuals who have the requisite level of knowledge to become cyberterrorists fall into three main categories. The first is a "hacker" defined as a "person that breaks into computers to prove that it can be done. Some are destructive in nature, others are purely joyriders." The second category is the cyberpunk, "a harder edged computer hacker, one that enjoys technology and uses that technology to make money or act as an anarchist." The third category is the cypherpunk, "a person that is interested in the use of encryption to protect the privacy and the use of decryption methods to access other protected files."[17] Paul Strassmann notes that, with the skills resident in these groups, several risks to computer systems exist:

> Pest Programs
>
> -Trojan horse attacks- implanting malicious code, sending letter bombs.

---

[17]Joseph Seanor, speech *The Cyber-Terrorist* presented to InfoWarCon'95 7-8 September, 1995, Washington, D.C.

-Logic bombs- setting time or event bombs
-Malevolent worms- denying access to distributed resources
-Virus Attacks- attaching code to programs and replicating it

Bypasses

-Backdoor attacks- using existing flaws in software for exploitation
-Authorization attacks- password cracking, hacking control files

Active Misuse

-Creating, modifying, denying service, entering false or misleading data
-Incremental attacks- using salami tactics
-Denials of service- launching saturation attacks

Passive Misuse

-Browsing- reading and copying with apparent authorization
-Interference, aggregation- exploiting database searches, traffic analysis
-Indirect misuse- preparing for subsequent misuses, off-line pre-encryptive matching, factoring numbers to obtain crypto keys, autodialer and voice-mail scanning.[18]

To achieve these results, the cyberterrorist cannot use the weapons commonly employed in conventional terrorism. While a conventional terrorist finds a fertilizer bomb effective in blowing up a building or other symbolic target, a technoterrorist will find the same bomb useful in destroying a critical node in a network to cause disruption. Cyberterrorists have no use for physical explosives. 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 the physical world. A

---

[18]Paul A. Strassmann, speech *Information Terrorism* presented at NDU 10 April 1995, Washington D.C.

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.

Several cyberterrorist weapons can have an impact on the networks of today and tomorrow.

(1) Viruses. One of the most heralded weapons of a cyberterrorist or a hacker is the computer 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 action, often unwitting (such as using an infected disk), by the system operator. Viruses can be used in 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 ease of identifying and removing the Michelangelo virus has resulted in publicity about it *not* attacking computers:

> MICHELANGELO VIRUS FAILS TO SURFACE: 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 font-page news in 1992.[19]

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.[20] This exponential growth suggests that virus writers hold the initiative in the battle for cyberspace. For existing operating systems that are infected with 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.

(2) 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

---

[19]Briefing, Denver Post 8 March 1995 Business, C-2, Nexis.

[20]"Prevention Beats Cure for Terminal Illnesses: Computer Viruses," *Daily Telegraph (London)*, 30 May 1995, 26.

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.

(3) Worms. Worms are programs originally developed to travel through systems and perform mundane tasks, such as data collection or erasure 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.

(4) 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."[21] Using a social engineering tactic, a cyberterrorist may impersonate a computer technician and call individuals within the targeted

---

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

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.

(5) 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 pulse.[22] 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 Gulf War, there are no indications that any terrorist organization possesses or has used these weapons against computer targets.[23] Press reports from Japan indicate that the 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 humans.[24] While suspected of being powerful enough to incinerate a human body, they may have intended this weapon for use against electronic targets as well.

---

[22]James W. Rawles, "High-Technology Terrorism," *Defense Electronics*, January 1990, 74.

[23]Neil Munro, "Microwave Weapons Stuns Iraqis," *Defense News,* 15 April 1992, Nexis.

[24]Yomiuri Shimbun, "Aum Linked with Microwave Weapons," *The Daily Yomiuri*, 11 June 1995, Nexis.

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 (ElectroMagnetic Pulse Transformer) Bombs by Winn Schwartau in testimony before Congress.[25] 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.

5. Technoterrorism

Technoterrorism is the intermediate step between "conventional" terrorism and "cyberterrorism." The technoterrorist understands the importance of high technology networks and C2 systems to a "third wave" state. Unlike the cyberterrorist, the technoterrorist will target and attack those systems that exist in the physical world to disrupt cyberspace. Thus, the computer itself (hardware rather than software) is the target of the technoterrorist. The technoterrorist will use "conventional" weapons such as bombs and physical destruction to destroy or disable those systems that control cyberspace.

6. Terrorism

The debate over the definition of terrorism is as old as the term itself. As the world moves into the information age, expanding the definition of terrorism to include actions taken inside cyberspace as well as the physical world may be necessary. There are several elements

---

[25]Schwartau, 171-189.

that run through the many definitions of terrorism. The first critical element is physical violence. At some point in terrorism, an individual or group must believe that they are being threatened with violence. The second element is the political nature of terrorism. The violence caused by a terrorist action must have some larger political goal than the physical action itself. The debate surrounding the definition of terrorism is addressed in Appendix B, which contains an overview of some of the more popular definitions in the literature. An understanding of the violent and political elements of terrorism are most important for this study.

One of the popular selling points of information warfare is that it is a less violent and destructive form of warfare in which the combatant states wage war with electrons in cyberspace. While the ability of states to wage relatively bloodless war is yet to be seen (the Persian Gulf war began to approach this standard in terms of allied casualties), the potential to create mass chaos and insecurity in a society via information warfare techniques may appeal to terrorists. As discussed in Chapter III, the definition of terrorism must be adapted and applied to those events that extend beyond mere physical violence and include what can be called "cyberviolence," or violence in cyberspace, where electrons, not people are destroyed. In addition, disruption, not destruction must be included as a tool to be utilized by cyberterrorists.

The evolving concept of information warfare will influence terrorism in the information age. Every advance in computing power continues to increase the usefulness of computers and their associated networks to law-abiding citizens. Simultaneously, these

computers increase the power of the weapons available to cyberterrorist and criminals. The implications of computer technology's dual nature, as both a tool and weapon, must be understood in the information age. The military information warfare tactics that exploit this dual nature may be used against the United States by future cyberterrorists. As such, it is important to include information warfare as a potential component of information age terrorism.

III. THE SHIFTING NATURE OF TERRORISM

A. TOWARD CYBERTERROR: THE SHIFTING NATURE OF TERRORISM

1. Defining Terror

How should traditional notions of terrorism be modified to accommodate the new phenomena of cyberterrorism? An answer to this question will be provided by examining the components of Thomas Perry Thornton's definition of terror: "a symbolic act designed to influence political behavior by extranormal means, entailing the use or threat of violence."[26]

a. Symbolic Violence

Terrorism, it is often noted, is the weapon of the weak against the strong. Terror is utilized to overcome seemingly insurmountable odds facing terrorists if they were to pursue their cause with conventional military means. Terrorists will typically strike out against targets that will resonate with the group they wish to influence. Thornton states that "the relatively high efficiency of terrorism derives from its symbolic nature. If the terrorist comprehends that he is seeking a demonstration effect, he will attack targets with a maximum symbolic value."[27] While Thornton is primarily concerned with insurgency, the value of attacking a symbolic target is applicable to terrorism. As an even weaker entity than the

---

[26]Thomas Perry Thornton, "Terror as a Weapon of Political Agitation," in *Internal War: Problems and Approaches*, ed. Harry Eckstein (New York: Free Press of Glencoe, 1964), 73.

[27]Thornton, 77.

revolutionary, the terrorist must strike out against symbolic targets in hopes of gaining publicity and garnering support for a cause. If the cause is the eventual overthrow of the government, then the terrorist must attempt to build this support into an effective insurgency. Thornton continues to state that the most important symbolic targets for a terrorist/insurgent, "are those referring to the normative structures and relationships that constitute the supporting framework of the society."[28] If these symbolic targets are destroyed, then the insurgent has succeeded in isolating individuals from the society in which they formerly felt secure and protected. In the information age, some of the structures that constitute the "supporting framework" of society are likely to be the high technology networks that allow individuals to communicate, access their money, and be employed. Thus, they are ideal targets for symbolic violence.

The intention of the terrorist or insurgent must be used to evaluate the "symbolic" nature of the chosen target. Intent drives the symbolism. An examination of the intent helps to differentiate between simple crime, which already exists in both the physical world and cyberspace, and terrorism. Philip Karber highlights this distinction:

> The symbolic concept of terrorism provides two crucial distinctions between terrorism and revolution and between terrorism and other forms of violence. If the objective of violence is the acquisition of useful objects (money, weapons, etc.) or the denial of such resources from the enemy, this action is robbery, assassination, sabotage, etc.,; "if, on the other hand, the objective is symbolic expression, we are dealing with terror"(Thornton). This highlights the distinction between terrorism and revolution, for symbolic violence can be used not only to propagandize the overthrow of a system, but also as a means

[28]Thornton, 77.

> of interest articulation to effect the system's output. When the "establishment" is unwilling to listen to nonviolent protest, terrorism permits the frustrated communicator, as staged by one terrorist, "to maximize significance and minimize getting caught."[29]

The cases examined in Chapter IV highlight the ability of criminals to perpetrate crime in cyberspace, all that remains for terrorism to follow is a shift in the intent of the actors.

Through information warfare attacks, cyberterrorists can utilize non-physical symbolic violence to articulate their message. Cyberterrorists can now manipulate a mass communication medium to convey a message directly, rather than relying on potentially incorrect or "slanted" reporting of an act of symbolic violence. The increasing ability to reach millions of individuals directly on the Internet or via a Direct Broadcast Satellite system offers "frustrated communicators" a non-violent alternative route to publicity.

Alex P. Schmid divides the symbolic value of terrorist acts into two separate categories. The first, *denotative*, categorizes those events that are "specifically and literally referring to an object or event." The second category, *metaphorical*, refers to a target that stands for "something other than what it appears to be."[30] These two distinctions will become increasingly "fuzzy" in the third wave if a state's high technology networks (upon which it relies for national security, wealth, and connectivity) become the target of terrorists. The

---

[29]Philip A. Karber, "Urban Terrorism: Baseline Data and Conceptual Framework," *Social Science Quarterly* (Vol. 52, Dec. 1971) 527-528 as cited in Alex P. Schmid, *Political Terrorism* (New Brunswick: Transaction Books, 1983), 83.

[30]Alex P. Schmid, *Political Terrorism* (New Brunswick: Transaction Books, 1983), 83.

goals of the terrorist may be to garner attention (metaphorical) *and* weaken some economic or defense system (denotative) through attacking a network.

b. Influence on political behavior

The second element of Thornton's definition is that terror is an "act designed to influence political behavior." This portion of the definition focuses on political terrorism vice other forms, such as criminal or pathological terrorism. While no universally accepted definition for terrorism exists in the literature, political terrorism is concerned with changing the actions of either the incumbent regime (insurgent terrorism), other groups (vigilante terrorism), or the population at large (regime or state terrorism).[31] The introduction of information warfare techniques will affect the conduct of all three types of terrorism but not the terrorist's intention to influence political behavior.

c. Extranormality

The extranormality of terrorist means and targets is critical to understanding the effectiveness of terrorist violence. Schmid states that, "normal occurrences lead to standardized responses and coping mechanisms. Terrorist violence breaks the pattern of normal human actions."[32] It is precisely because terrorist actions fall so far outside the "norm" of violence accepted in society that they generate such an extraordinary reaction. Schmid identifies five elements of extranormality: the weapon, the act, the time and place, covert and clandestine nature, and violation of rules of conduct.

---

[31]Alex P. Schmid, *Violence as Communication*, (Beverly Hills: Sage, 1982), 60.

[32]Schmid, *Political Terrorism*, 107.

(1) The Weapon. Terrorists have a long history of utilizing "common" weapons such as knives, guns, and bombs to commit acts that exist outside the realm of accepted behavior (murder, assassination, airline and embassy bombings). These weapons take on new dimensions in the minds of the victims and target audience. The fear of the unknown and the increasing potential of terrorists utilizing Weapons of Mass Destruction (WMD), as evidenced by the sarin gas attacks in Tokyo, produces terror as a result of such powerful weapons being controlled by a sub-state, non-sanctioned actor. As the information age arrives, the possession of information warfare skills by smaller and smaller groups of individuals may signal the arrival of a new WMD, a Weapon of Mass Disruption, in which both the state and sub-state actors are equally equipped to inflict this disruption.

(2) The Act. While the use of chemical weapons and the destruction of buildings has been commonplace in the "normal" realm of state on state warfare, gassing civilians in a subway and the destruction of an embassy, airplane, or federal building with a bomb clearly lies outside the bounds of accepted, and even criminal, behavior. Since a cyberterrorist act has yet to be committed, the first act will, by definition, be outside the bounds of the normal. At the very least, it will be unique.

(3) The Time and Place. The third extranormal element is the time and place of the attack. In terrorism, there is no "declaration of war" between two states that prepares the population for violence between the state and an enemy. Thus, a terrorist attack is usually a "bolt from the blue," designed to create terror in the target audience due, in part, to its unexpectedness. As Schmid states:

> The place of the terrorist act is also unpredictable. There are no frontlines, there is no battlefield. The sudden outbreak of violence can occur at home, during a sportive event or in a cinema, in a barroom or on the marketplace–places which have the character of zones of peace. The contrast between the familiar surroundings and the violent disruption enhances the fear. Their is a sporadic, irregular pattern to the violence, whereby no one can be really certain that he is not facing imminent danger the very next moment. The thought where and when the next attack will take place and who will be the victim is on everybody's mind of those who belong to the targets of terror.[33]

The ability to stage an attack nearly anywhere is an element that will become increasingly important in the information age. If terrorists wish to attack a state's key networks utilizing information warfare methods, they will be able, from one location, to attack either parts of the system or the entire system itself. The "no frontlines or battlefield" situation is already reality in "cyberspace" where there are no borders. Using information warfare methods for attack allows a terrorist on the other side of the world to pose the same level of threat as one in the room next door.

(4) Covert and Clandestine Nature. This applies equally to insurgent and state terrorism. An insurgent terrorist group must, by design, remain covert and clandestine to continue to operate. The dawn of the information age presents new tools for a terrorist organization to communicate securely with its members while simultaneously enhancing the clandestine nature of the group. Additionally, the information age provides another set of tools to the anti-terrorist forces for use against the terrorist.

---

[33]Schmid, *Political Terrorism*, 108.

(5) Violation of rules of conduct. Coupled with the lack of a battlefield or front line is the lack of any rules of engagement or laws of war. The Geneva Convention does not apply to terrorists or their victims. Schmid again highlights the effect this has on individuals:

> The adherence to social norms in human interactions makes behavior predictable and thereby contributes to a sense of security. Whenever manmade violence occurs we look for a reason and generally find it in a breakdown of the actor-victim relationship. The terrorist, however, has generally not had such a relationship at all. The victim is often not his real opponent, he is only an object to activate a relationship with his opponent. The instrumentalization of human beings for a cause of which they are not part in a conflict in which they are often not active participants strikes many observers as extranormal.[34]

The victims in cyberspace will never "see" their attacker, nor are they likely to have any relationship with their attackers in the "real" world. Rather, the interaction will occur exclusively in the anonymous realm of cyberspace.

In summary, the "extranormal means" of a terrorist act are designed to prevent the victim or the target audience from placing the event into a known framework. The inability to classify the threat or devise a solution utilizing normal procedures leads to the creation of terror. Thornton states, "knowledge and understanding of the source of danger provide the victim with a framework within which he can classify it, relate it to his previous experience, and therefore take measures to counter it."[35] If the cause of the danger is unknowable and unpredictable (i.e., caused "randomly" by terrorists), a state of anxiety,

---

[34]Schmid, *Political Terrorism*, 109.

[35]Thornton, 83.

characterized, "by fear of the unknown and unknowable" will be achieved. If the threat is great enough, the result is a state of despair characterized by the perception of the threat as "so great and unavoidable that there is no course of action open to him that is likely to bring relief."[36] As the reliance on computerized systems for the conduct of everyday life increases, the level of disruption and disorientation that would be caused by their failure also increases.

d. Violence

The final element of Thornton's definition of terror, "entailing the use or threat of violence" deserves close attention as the ability to threaten or use physical violence in cyberspace is nonexistent. Thornton bluntly states that, "a nonviolent program could hardly qualify as terrorism"[37] Unfortunately, the varying definitions of violence in the literature on terrorism are second only to the varying definitions of terrorism itself. A critical component of most definitions is that violence entails physical harm to a person or object. Paul Wilkinson's definition is a good representation of the "physical" school:

> [V]iolence is defined as the illegitimate use or threatened use of coercion resulting, or intended to result in, the death, injury, restraint or intimidation of persons or the destruction or seizure of property.[38]

As terrorism moves into the information age, the definition of violence must include cyberviolence. While the destruction of data is not a physically violent act, and will not

---

[36]Thornton, 80-81.

[37]Thornton 75.

[38]Paul Wilkinson, *Terrorism and the Liberal State* (New York: New York UP, 1986), 24.

always place a human life in jeopardy, it should still be treated as terrorism. If the goal of the cyberterrorist is to create terror, the best course of action may be to resort to a physically violent act, or attack a computer system that will place lives in immediate jeopardy, such as aircraft control systems. If cyberterrorists are unable to create the perception of a physical risk to their audience, they will be unable to create a sense of terror. They may, however, be able to fulfill several other objectives of terrorism.

2. Objectives of Terrorism

Thornton addresses several objectives in his examination of terror as a weapon. The first objective is morale-building within the terrorist group. The second objective is advertising, in which the group attempts to announce its existence and place its concerns before the target audience. Terrorists have historically used this "propaganda of the deed" to force debate on their goals. The recent bombing of the Murrah Federal building in Oklahoma City is an example of how a symbolic target can force debate on issues far afield from the actual terrorist event. In this case, not only the building (which housed numerous federal agencies), but the date (anniversary of the resolution of the Waco, TX standoff between the BATF and the Branch Davidians) were symbolic. The symbolic nature of the attack riveted the nation's attention on the subsequent Waco and Ruby Ridge hearings in Congress and re-ignited a controversy over the conduct of several government law enforcement agencies.

When attempting to change the government through an insurgency, another objective, according to Thornton, becomes critical to the terrorist:

> *Disorientation* is the objective *par excellence* of the terrorist, removing the underpinnings of the order in which his targets live out their daily lives. The primary responsibility of any incumbent group is to guarantee order to its population, and the terrorist will attempt to disorient the population by demonstrating that the incumbent's structure cannot give adequate support.
>
> The demonstration is, however, but one aspect of the disorientation process. On a much deeper level, the objective is the isolation of the individual from his social context. . . . The ultimate of the terrorization process, as Hannah Arendt conceives it, is the isolation of the individual, whereby he has only himself upon whom to rely and cannot draw strength from his customary social supports.[39]

If the information age continues to create a society that is dependent on computers for communication and basic order, the disruption of these computers will be critical for the creation of disorientation. A government must ensure that those systems upon which it relies to maintain order and control are adequately defended against attack by terrorists and insurgents. In the United States, where 95% of the communications needs of the military are carried on the Public Switched Network (PSN), composed entirely of commercial carriers such as AT&T and MCI, it has been difficult to determine the proper role of the government in ensuring the security of these systems.[40]

A final objective of a terrorist organization is provoking a response by the incumbent group. Terrorists cannot directly control the government response to an act of symbolic violence. Often, a terrorist organization will commit a violent act in hopes that the government will over-react in its response. While there may be pressure to "do something"

---

[39]Thornton, 83.

[40]Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," *Washington Post*, 16 July 1995, C-3.

against the terrorists, the terrorist organization can only start the process of government action, not control it. As such, the government must take care not to play into the hands of the terrorist organization by over-responding.

> Ideally, suppression should be accomplished by routine methods of law enforcement, but if the terrorists are effective–and especially if the incumbents perceive themselves to be in a crisis situation–it is almost inevitable that extraordinary repressive measures will be taken. In combating an elusive terrorist, the incumbents will be forced to take measures that affect not only the terrorist but also his environment, the society as a whole.[41]

The repressive nature of the countermeasures on society as a whole lead to a confirmation of the terrorist's statements against incumbents. In attempting to punish the terrorists, the government often punishes the people, leading to further disorientation and a fixation of blame onto the incumbents for the terrorist actions. This action-repression spiral is a key component of a terrorist group seeking to cause government overreaction.

The terrorist and government actions may, however, have the exact opposite effect from that just discussed. Ted Robert Gurr has labeled the negative aspects discussed by Thornton "backlash."[42] When a terrorist commits a violent act, there is always a risk that the action will be seen as so completely unacceptable that support from within the group will be withdrawn. This phenomenon also exists outside the group. The general population will blame the *terrorist* and not the government for their suffering and will tolerate, if not

---

[41]Thornton, 86-87.

[42]Ted Robert Gurr, "Terrorism in Democracies: Its Social and Political Bases," in *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, ed. Walter Reich (New York: Cambridge University Press, 1990), 94.

welcome, repressive measures to eradicate the terrorists. Terrorists may ameliorate this problem through the use of cyberterror, in which they can attack symbolic targets in cyberspace without the need to kill "innocents" in the physical world. Destroying a computer or its data is unlikely to elicit the same emotional reaction as killing children.

All of the above can be summarized in the concept of the "tactical path" (Figure 2) that both the government and a terrorist group must follow. This concept, postulated by Dr.

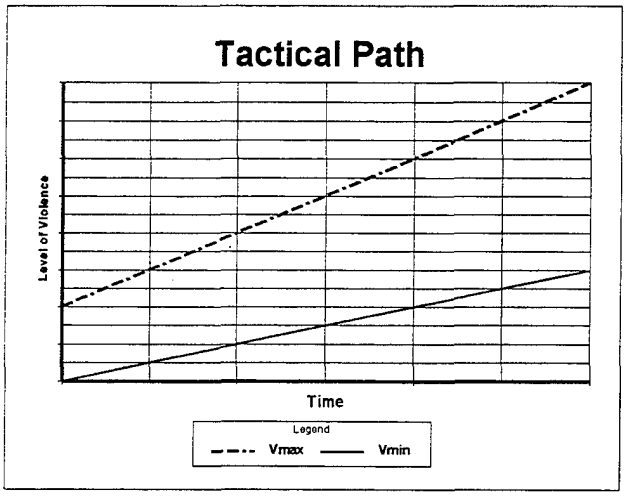

Figure 2

Gordon McCormick of the Naval Postgraduate School, states that there is both a V_{min} (minimum level of violence) and a V_{max} (maximum level of violence) that is acceptable to 1) the terrorist group's members and supporters, 2) society at large (the target audience). If a terrorist organization falls below the V_{min}, then it will lose its "place in the spotlight" and be relegated to the level of a nuisance or petty crime that is not worthy of the emotionally and politically charged term terrorism. If a terrorist group crosses the V_{max}, then it will experience backlash, losing support from within and raising the level of repression that the government

can use to defeat the terrorist group. The government's tactical path is similarly bounded. If it falls below the V_{min}, the public will perceive it as not responding to the terrorist situation. If the government response exceeds the V_{max}, the public will perceive it as unduly repressive, thereby fulfilling one of the terrorist's main objectives of provoking an excessively harsh and repressive countermeasures campaign.

While cyberviolence enables the terrorist to attack symbolic targets without resorting to physical violence, there is likely a similar "tactical path" for cyberviolence. The critical difference between cyberterror and conventional terror is disruption vice destruction. As such, the bounds of the two tactical paths are different. If terrorists use cyberviolence to kill individuals (through failure of critical computer controlled safety systems) the public will evaluate their actions on the conventional terrorism "tactical path" since the results of the action include destruction. If the event causes disruption exclusively, it will then be evaluated on a cyberterrorist tactical path. While the upper and lower bounds of each path are somewhat fluid, a general understanding of the limits is possible. The V_{max} of cyberterrorism, judged in the number of people disrupted, is likely to be an order of magnitude greater than that of conventional terrorism in which people are killed. While several events, such as the shutdown of Japanese rail systems and the Internet (discussed in Chapter IV) disrupted millions of people, both the public and government responses were muted in comparison to the sarin gas attacks on the subways in Japan and the bombing of Pan Am 107 over Lockerbie. We have not yet seen a group cross the V_{max} on the cyberterror tactical path.

3. Ability to Cause Terror From Cyberspace

Information warfare attacks can be a form of symbolic violence but can they create terror? We have seen that the components of symbolic violence are many and varied, with the critical target for insurgents being the social system of their target audience. In conventional terrorism one of the main objectives of a terrorist act is the creation terror. This is best done by removing individuals from society and placing them in some form of physical jeopardy. Do information warfare tactics and techniques offer a terrorist the ability to do both at once? The exploding reliance on computers and telecommunications in the "third wave" world have created a definite vulnerability in the information age.

> The sinews of the post-industrial society are already taking shape - the network of electronic data-processing and communications - and these sinews are already becoming more vulnerable to disruption and terrorism. The service industries, in particular, are increasingly inter-independent, and ripe for attack by fraudsters, hackers, eavesdroppers, disrupters, and extortionists.[43]

Indeed, the actions of hackers have left no doubt about the vulnerability of the world's computer systems. President Bush addressed this vulnerability at the highest levels of the U.S. government with the release of National Security Decision Directive 42 in 1990.

> Telecommunications and information processing systems are highly susceptible to interception, unauthorized access, and related forms of technical exploitation as well as other dimensions of the foreign intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements.[44]

---

[43]Richard Clutterbuck, *Terrorism and Guerrilla Warfare: Forecasts and Remedies* (New York: Routledge, 1990) 18.

[44]Schwartau, 127.

The capability clearly exists to target the new "sinews" of our computer networked society. As evidenced by the Morris worm attack, it requires no external state support. Rather than being heavily dependent on money, people, and force in the manner of conventional terrorism, it is primarily dependent on information and knowledge of how to penetrate systems.

In the information age, the value of our networks to national security, government, and business is increasing at an exponential rate. Our financial networks, which move trillions of dollars a day, are an often cited example of the damage a terrorist attack on them would cause.[45] This ability to move money electronically is vital to our economic well being and is a symbol of United States wealth and power. In the same way that U.S. embassy buildings and civilian aircraft were attacked as symbolic targets in the 70s and 80s, the networks that are the manifestation of U.S. economic and political strength may become targets in the future. That the networks are vulnerable and a symbolic target does not automatically dictate that they will become targets of terrorist organizations. Rather, the efficiency with which these targets can cause fear, anxiety, and despair through terror will dictate when, if ever, terrorists will attack them.

Terror is a psychological state that can be sparked through physical acts. The "use or threat of violence" in the definition of terror as forwarded by Thornton exists exclusively in the physical world and does not "exist" in the same form in cyberspace. Terrorists can achieve the goal of disorientation at an individual level, "by physically withdrawing the

---

[45]Schwartau, 64.

individual from his environment and isolating him (as in "brainwashing" techniques)." Since a terrorist organization cannot isolate each person in its target audience, it uses symbolic violence in an attempt to destroy the social framework of society so that the individual thinks he is alone in his anguish even though he may be physically undisturbed.[46]

In the information age, relationships are increasingly being built upon the "Global Network." This may give rise to the popular concept of a "Global Village." Communities of individuals separated by thousands of miles and state borders are springing up every day. These "virtual communities" only exist through the "cyberspace" connection afforded by new communications and computing technology. These communities are an ideal target for isolation by "cyberterrorists." While isolating the members of these communities from each other temporarily is possible for a terrorist group, the members are likely to have ties to a local community that provides their primary "social framework."[47] If the members of the group relied entirely on their virtual community for their social framework, however, then a small group of people could effectively achieve the goal of disorientation within that virtual community as its members are already physically separated from one another. Removing their "cyberspace" ties with one another is an effective way to begin their isolation. Depending on how terrorists carry out the disruption of connectivity between the members, it could last for several hours, days, or weeks. With the increasing redundancy of telecommunications assets,

---

[46]Thornton, 83.

[47]Martin Libicki, *The Mesh and the Net* (Washington, D.C.: Institute for National Strategic Studies, 1994), 97-119.

it is unlikely that service would be disrupted for more than this period of time. The same disruption of service may occur through "natural" means, (fire, flooding, natural disaster) and would cause some concern within the community but would not create terror. That the same end result (disruption of service) does not produce the same psychological reaction is based on the individual's perception of the problem. The disruption and isolation generated by "natural causes" fits readily within the victims' cognitive framework allowing them to take actions to overcome their difficulties. If a terrorist organization covertly causes a low level of disruption, the citizens of the virtual community will not be able to classify the threat or they will classify the threat as the actions of "hackers," petty criminals, or as a government conspiracy. Only when the level of disruption escalates and cannot be controlled or understood by the "virtual citizens," will terrorists create anxiety and despair. For a cyberterrorists to be taken seriously, they must cause massive damage to their "cybertargets" to avoid the attack being evaluated within the public's known framework. If the terrorist wants to perform a "soft-kill" on a major system, the amount of information (hard to obtain) required is extraordinary while the amount of equipment (easy to obtain) is minimal. While it is more "elegant" to bring down a system with no visible signs through programming, it is *far* easier to bomb a "key node" in the computer system with explosives to disable its power or information flow. The networks connecting virtual communities are lucrative targets because they span conventional country borders and exist exclusively in cyberspace.

The "control" of cyberspace is a seam in U.S. society that a terrorist organization can exploit. The uproar generated by the U.S. government's proposal to mandate a specific hardware encryption method (the Clipper chip for telephones), which would still allow for government surveillance, highlights the lack of popular government solutions to problems in cyberspace. In addition, the government dismantled the National Science Foundation network (a major Internet backbone) in April 1995. Commercial service providers have taken over the services provided by the NSFNet.[48] While in the past, access to the Internet was nearly exclusively via educational, government or scientific institutions, at present, commercial connections and "host" computers are growing rapidly. The commercial (.com) domain is the fastest growing sector of the Internet over the last two years and the growth continues at an exponential rate.[49]

Since cyberspace is essentially uncontrolled by any government or individual, a question of who is responsible for its defense will be asked in the wake of sustained attacks. If no satisfactory answer is provided, the terrorists may be able to shift the target audience's anger toward the group (most likely the government) that they believe should be responsible for maintaining the security of cyberspace. Since the virtual community will most likely span several different countries, the opportunity exists for a terrorist to affect a worldwide target audience and achieve maximum impact for minimum effort.

---

[48]Cynthia Bournellis, "Internet '95," *Internet World*, November 1995, 52.

[49]Bournellis, 47.

While "cybercommunities" are vulnerable to information warfare attack, can terrorists influence U.S. society at large via Information Warfare? Can they truly create terror by exploding software bombs instead of fertilizer bombs? The answer may lie in the increasing levels of computerization in everyday life and the blind faith that is coming to be placed in computers. The importance of these computers is discussed by Winn Schwartau:

> In 1968, Marshall McLuhan said that emerging information networks are "direct extensions" of our own nervous systems. Losing an ATM machine, according to that reasoning, is the equivalent of a leg or an arm. People panic when their computer goes down.[50]

A terrorist blowing up or hijacking an airplane has a definite impact on the public. It is a media event that is widely publicized and speculation runs rampant over who committed the crime and for what reason. It is likely to cause fear in the public and perhaps anxiety in some. Some travelers may, due to their fear, opt not to use air transportation. In the majority of cases, the act of blowing up the airplane is not meant to punish the passengers, or even to deter air travel, but rather it is a symbolic act meant to bring the terrorist issue into the forefront of the media and thus, the world's attention. To create terror in the general public, there must be some perceived threat of violence. The large percentage of the population that has, and will, use air transportation can identify with the passengers who are killed in a plane bombing. They begin to ask, "Am I next?" and "Do I have any control over this situation?" While McLuhan may have been right in saying that networks are becoming an extension of our nervous systems, it is unlikely that individuals will value them as highly as arms or legs.

---

[50]Schwartau, 77.

When one or many ATMs go down, there is little hope of terror being created as a result. There is no threat to the physical well being of the ATM user. This situation, if caused by cyberterrorists, may cause anger and frustration, but causing terror is unlikely. If, on the other hand, ATM machines started to electrocute their users on a seemingly random basis, it may provoke a sense of terror in the ATM user community.

In an unlikely twist of fate, the World Trade Center bombers did cause a large number of individuals to lose access to their money via ATM machines. A major snowstorm on the East Coast of the United States caused the roof of Electronic Data Systems (EDS) Corporation's New Jersey computer center to collapse. The backup plan for EDS was to relocate their operations to an alternate site. Unfortunately, companies that the World Trade Center bombing displaced were using the EDS backup site. As a result, the ATMs that EDS serviced were forced to shut down, affecting 6% of the 83,000 teller machines in the United States. While damaging to EDS, the individual bank customer lost no data or money. In fact, the redundancy of the ATM communications system, with many machines being served by several different networks (Plus, Cirrus, etc.), 98% of those affected by the EDS outage had alternate access to their money via a different network.[51] The loss of ATMs, while not directly intended by the bombers, did not cause massive panic or a run on any bank. The flexibility and redundancy of the existing networks, although individually vulnerable to disruption, were sufficient to allow the flow of money to continue without major interruption.

---

[51]Rusty Graham, "Storm, Bombing Work 1-2 Punch on Local ATMs," *Temple Daily Telegram*, 18 March 1993, Business section, Nexis.

This incident highlights the difficulty that a technoterrorist may face in the future with the increasing redundancy and multiple networking of vital systems. When one or several nodes are destroyed, the signals normally processed by that node are simply rerouted to another node to reach their destination. With the increasing reliance on centralized switching in the telephone industry, the loss of just one switch can have widespread effects, as demonstrated by the 1988 fire that destroyed a Chicago area switch and resulted in the shutdown of O'Hare Airport and the loss of telephone service to a widespread area. Should cyberterrorists attack several nodes simultaneously, they may be able to create a disruption that would be more widespread than the physical destruction of just one node. While the cyberdisruption is likely to be larger, its effects will be less permanent than the physical destruction caused by conventional or techno-terrorists.

Brian Jenkins highlights the difficulty that information warfare attacks have in generating terror:

> Will we see a more sophisticated 'white collar' terrorism, that is, attacks on telecommunications, data-processing systems, or other targets intended to produce not crude destruction but widespread disruption? Perhaps, but disruptive 'terrorism' of this type does not appear to be particularly appealing to today's terrorist groups. Such operations are technically demanding, and they produce *no immediate visible effects.* There is no drama. No lives hang in the balance. There is no bang, no blood. They do not satisfy the hostility nor the publicity hunger of the terrorists.[52]

---

[52]Brian Jenkins, "Future Trends in International Terrorism," *Current Perspectives in International Terrorism*, eds. Robert O. Slater and Michael Stohl (New York: St. Martin's Press, 1988) 258.

In the future, terrorists may no longer need terror or physical violence to create the disruption and publicity that they desire. While the "kinder and gentler" cyberterrorist of tomorrow may be able to create disruptions without resorting to conventional destructive tactics, these information warfare skills may be used to augment the destructive nature of acts committed by conventional terrorists. The level of destruction and chaos caused by an act can be increased by interfering with the authorities ability to communicate and respond.

Information age terrorism, in its cyberterror form, may be non-violent and not directly utilize terror. It must, however, be treated as terrorism as it will fulfill nearly all the other objectives of terrorism and poses a serious risk to information dependent societies.

IV. SHIFT TOWARD INFORMATION WARFARE ACROSS THE CONFLICT SPECTRUM

Information warfare tactics are being employed across the spectrum of conflict. The increasing importance of computers and their attendant networks make them primary targets for both state sponsored espionage and crime.[53] Terrorists have recognized the value of energy distribution networks and some computer installations. At the level of insurgency and rebellion, information warfare tactics have been used to subvert state controls of the media and for communications between the rebel leadership and their worldwide support base.

A. USE OF INFORMATION WARFARE IN STATE SPONSORED ESPIONAGE AND CRIME

The advanced information warfare techniques of computer penetration, surveillance, and exploitation developed by the following states can be utilized for terrorism as well as espionage and crime. There is a long history of state sponsorship of terrorism in the 20th century. Often the goal of computer penetrations is to provide easy access for future penetrations. In effect, foreign states are conducting information warfare espionage to have "turn key" access to U.S. systems in the future. The only difference between these acts of computer espionage and terrorism is the addition of a political motive or goal to the criminal nature of the penetration. States may, in the future, choose to provide this information to a

---

[53]Peter E. Sakkas, "Espionage and Sabotage in the Computer World," *International Journal of Intelligence and Counterintelligence* 5-2 (Summer 1991): 155-202.

sponsored terrorist group for use against the United States. As such, a careful examination of past and current information warfare activities at the state level is important as it may identify future terrorist targets or tactics likely to be used by state sponsored terrorist groups.

Who can perpetrate an organized "computer attack" against the United States? A study of the threat by Wayne Madsen addresses these issues. He classifies foreign nations into one of four categories of computer advancement:

> (1) highly advanced, (2) operationally advanced, (3) basic development, and (4) initial development. France, the United Kingdom, Japan, China, and the United States represent the first category, and their intelligence agencies are highly advanced in the science of electronic eavesdropping and computer intelligence gathering. Russia, India, Ukraine, and Colombia represent the second category. While Russia and India, arguably, have first-rate intelligence-gathering organizations, their high technology capabilities still lag behind those of the first category but are improving steadily. Libya, Ghana, and Bolivia fall into the third category. Their intelligence agencies will soon have high technology capabilities. Zaire, Ethiopia, and Tanzania represent the fourth category: their intelligence organizations lack high technology capabilities and their embryonic computer and data communications systems are vulnerable to the capabilities of the nations in the first three categories.[54]

While this is a comprehensive list of states, the threat continues to grow. This is due to the increasing rate of computer power and technology available to sub-state actors, such as "hackers." In the past, one needed to have the power and resources of a state behind them to conduct an effective worldwide SIGINT operation. Now, a few people can conduct a computer intelligence (COMPINT) effort with limited funds. Whereas access to remote sites to place antennas or military overflight of territory was a prerequisite for SIGINT, the most

---

[54]Wayne Madsen, "Intelligence Agency Threats to Computer Security," *International Journal of Intelligence and Counterintelligence* 6 (Winter 1993): 440.

critical element of COMPINT is the knowledge of how to exploit a computer system. As cyberspace is a nonphysical reality, borders and geographic location of the target system are meaningless in a COMPINT effort. Since the world's computers are becoming increasingly interconnected, a modem to connect to the Internet and a desktop computer, coupled with a talented computer user, are all that is required to start intelligence gathering. With the power of desktop computers doubling every 12-18 months, the computing power that previously only a government or large corporation could afford now sits in homes across the world. While state powers have exploited these assets in the past, substate actors may exploit them easily in the future.

1. Who is Targeting the United States?

a. Soviet Union/Russia

The first computer hacker incident to garner national attention was sponsored in part by the Soviet Union to gain access to Western technology and defense information. This incident was the subject of a book, *The Cuckoo's Egg*, by Clifford Stoll.[55] A group of West German hackers, who were operating on their own, approached the KGB in East Berlin and began to sell the "product" of their hacking. Later touted as a "KGB spy ring," the hackers attempted to break into scores of military, government, and business computers to provide information to the Soviets. While the hackers thought that military items would be high on the KGB shopping list (some were), most of the requests centered on high technology

---

[55]Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York: Doubleday, 1989).

computer programs and equipment design. The Soviets desired the "source code" for sophisticated and widely used computer operating systems. With this knowledge, the Soviets could create their own team of "hackers" to penetrate systems in the West.

The operating system that runs a computer exists in two forms, the "source code" which a human can read, analyze, and understand when printed, and the "compiled" version, which translates the operating system "source code" into "machine language," the actual ones and zeros that the computer understands but is completely unintelligible to humans. The process of compiling the source code is similar to encryption. The machine language can be decompiled (decrypted) with the result being only similar, not identical, to the source code. Thus, any "source code" is one of a computer programming company's most closely held secrets. Knowledge of the "source code" makes it easier for a hostile competitor or state to identify what bugs exist in the program or even insert its own bugs, recompile the code, and replace the operating system with their altered version, all without the knowledge of the end user. In this manner, the Soviets were attempting to "get the keys to the filing cabinet rather than its contents" via their computer hackers. There are indications that the Soviet efforts to acquire this information were far more extensive than using the "amateur" hackers as their KGB contact told them that they had "competition" and many of its desires were met without the hackers providing the product. This knowledge, exploited by terrorists, could result in massive disruption of computer systems on a worldwide basis.

The computer penetration attempts by the Soviets/Russians continue. Wayne Madsen observes that "the Institute of Automated Systems (IAS) in Moscow hosts the

National Center for Automated Data Exchanges with Foreign Computer Networks and Data Banks (NCADE). During Soviet rule, NCADE had a special program to broaden linkages between Soviet computer users and foreign data networks and databases to obtain valuable software programs that the Soviets could not normally obtain because of Western export restrictions."[56] Using these channels, the Soviets penetrated a German computer and obtained production information on the Tornado fighter aircraft in 1984. As recently as 1989 a Soviet Attaché, LtCol Yuri Pakhutsov, was expelled from the U.S. for allegedly attempting to acquire information on government computer security practices and capabilities.[57] While the KGB of the Soviet Union was well organized and ran its "information warfare" attacks from several directorates, the current state of organized Russian computer espionage efforts is not clear. Statements made by retired Russian intelligence officers, even after the KGB-Hannover Hacker spying scandal, leave open the possibility that computer espionage efforts continue.

> Colonel Barkovsky was not hesitant to state that the Russian Federation has embarked on a major programme of establishing information service networks throughout the country. Not elaborated upon was whether the Russian intelligence services will take advantage of the information-gathering capabilities provided by these networks.[58]

---

[56]Madsen, 419.

[57]"Soviet Attaché expelled as 'computer spy'," *Jane's Defence Weekly* 18 March 1989, 438.

[58]Wayne Madsen "Retired KGB Officers Refuse Comment on Russian Computer Espionage," *Computer Fraud and Security Bulletin* Jan. 1994, Nexis.

One can only assume that the Russians are continuing their programs to acquire and target high technology in the United States.

Claire Sterling, in her book *The Terror Network,* claimed that the Soviet Union was a major sponsor of terrorism across the world.[59] While the dissolution of the Soviet Union and the economic problems of Russia have clearly limited its ability to fund large terrorist operations, the cost involved in sponsoring cyberterrorism is significantly lower. The knowledge gained by the Soviets during Cold-War espionage efforts may (with or without the approval of the Soviet leadership) find its way into the hands of cyberterrorist organizations. This flow of information is potentially more damaging than the flow of arms and explosives to conventional terrorist organizations.

b. Bulgaria

Bulgaria has been a "breeding ground" for computer viruses during and after Communist rule. In the early 1990s, the Bulgarians had developed thirty unique viruses with more than 100 different variations and were releasing them at a rate of one per week.[60] The "Hannover hackers" of *Cuckoo's Egg* fame also identify the Bulgarians as active in computer intelligence. Madsen cites the National Intelligence Service (foreign and domestic intelligence), and Razuznavatelno Upravleniye na Ministerstvoto (RUMNO) (Military intelligence) as the Bulgarian intelligence organizations most likely to be involved in computer

---

[59]Claire Sterling, *The Terror Network* (New York: Berkeley, 1982).

[60]Madsen, "Intelligence Threats" 426.

intelligence gathering.[61] It has also been rumored that a new "virus library" that allows anyone, not just a skilled programmer, to write a virus by "picking and choosing" among several options was first developed in Bulgaria. This system has the potential to produce thousands of new viruses to be unleashed at random or specific targets. A cyberterrorist bent on bringing a system down could singlehandedly generate a flood of viruses to infect the targeted computer. Even if virus detection software was installed, the chances are good that a virus could be created to evade detection.

c. France

France freely admits that it conducts intelligence operations against its allies and its enemies on the "economic front." As we move into the information age, the distinction between friends and enemies begins to blur. Madsen targets the Direction de la Surveillance du Territoire (DST) and the Directorate Generale de la Securite Exterieure (DGSE) as the agencies involved in COMPINT. In addition the Groupement de Communications Radio-electriques (GCR), the French NSA, maintains a close working relationship with France Telecom and, like the U.S. NSA, has strict rules on the use of encryption products within France, allegedly so that they can "break" the encryption and eavesdrop on communications within France.

Recently, the French government disclosed a document instructing the DGSE to gather intelligence on 49 U.S. aerospace and defense firms. The methods to obtain this

---

[61]Madsen, 450.

information included bugging of Air France flights and breaking and entering of hotel rooms of visiting business executives to photocopy business materials.[62] The Hughes Aircraft Company has been a favorite target of the French. The DGSE targeted Hughes for information on its HS 601 communication satellite, fiber optic anti-tank weapons, the Phoenix AIM-54 air to air missile, and various electro-optical sensors.[63] The Hughes Corporation decided (ostensibly for business reasons) to cancel its attendance at the Paris Air Show after the revelations of French targeting. Another "aviation" scheme of the French involved the collection and exploitation of telemetry signals from a Boeing test flight of its new 747-400 aircraft. A French SIGINT and technical team were sent to Washington state to intercept and analyze the test flight data for the benefit of Airbus research.[64] While not a direct computer penetration, the components that the French were most interested in were the computer controlled navigation and flight control systems. The knowledge gained from Boeing's telemetry data enabled them to develop similar systems for their own aircraft. Additionally, should the detailed knowledge of computer controlled aviation systems fall into the hands of a technologically sophisticated terrorist organization, the potential to create terror is substantial. A terrorist organization would only have to convince the public that it is capable

---

[62]Michael J. McDermott, "Is International Marketing a game of spy versus spy?" *Brandweek* 20 June 1994, 31.

[63]Ronald E. Yates, "Cold War: Part II, Foreign Intelligence Agencies have New Targets- U.S. Companies," *Chicago Tribune*, 29 Aug. 1993, C1.

[64]Peter Schweizer, *Friendly Spies* (New York: Atlantic Monthly Press, 1993), 122.

of causing the controls of a particular type of airplane to stop responding to pilot inputs to create large concern over flying in that particular type of airplane.

d. Japan

The Japanese place a high priority on intelligence gathering through both "official" and corporate intelligence networks. Japan's international telecom carrier, NTT "routinely cooperates with Japanese intelligence to tap the phone lines of competitors." In addition, Madsen asserts that the Japanese target U.S. satellite communications stations. "A 1987 classified CIA report, *Japan: Foreign Intelligence and Security Services*, claimed that the second most important Japanese intelligence priority was the gathering (in many cases by computer) of technological and scientific developments in the United States and Western Europe."[65] The efforts of Japan in the "high tech" sector are not simply related to "computer break-ins" but rather to acquire design specifications in an effort similar to that of the Former Soviet Union. While the Soviets were attempting to obtain source codes and hardware that they were unable to build themselves, the Japanese were working to save money on R&D by stealing advanced U.S. technology and then bringing similar products to market simultaneously with their U.S. competition. Peter Schweizer outlines the story of a corporate spy who sold Hitachi copies of IBM's *Adirondack Workbooks*, a series of books that held the secrets to future IBM technology. Hitachi was able to use this information to develop computer hardware that was nearly identical to IBM's but cheaper since Hitachi did not bear

---

[65]Madsen, 436.

the development costs. This case was "broken" by a Silicon Valley "sting" operation run by the FBI that initially targeted the Soviets. Japanese aggressiveness in pursuing this technology led them into the trap. The end result was an out of court settlement, reportedly for 300 million dollars between the Japanese and IBM. The information that an intelligence gathering effort obtains may be used by a sponsored terrorist organization to target a specific business or industry.

e. China

Chinese intelligence employs its large ethnic community abroad for many purposes. It is now clear that computer penetration was one of those functions. Andrew Wang, a Chinese immigrant, was arrested for stealing the source code of several programs from Ellery Systems. These programs were designed to "run" the emerging National Information Infrastructure.[66] This source code, as previously discussed, would allow a foreign intelligence agency or terrorist group to identify and exploit loopholes in the "new information superhighway" that would carry everything from benign E-mail to national security data.

f. Germany

The Germans appear to have taken their cue from the success of such amateur hacker groups as the "Chaos Club" and the "Hannover Hackers" that worked with the KGB. According to Schweizer, the Germans created "Project Rahab," named after the biblical

---

[66]Stephen Keating, "Global Intrigue on Info Highway, Local Case Alleges Chinese Piracy," *Denver Post*, 24 April 1994, A1.

character who helped the Israelites infiltrate Jericho, in the mid 1980s to develop a "professional" hacking capability. The project was developed by the Bundes Nacrichten Dienst's (BND) Christian Stoessel, who wrote the initial "point paper" proposing hacking into foreign data bases for intelligence purposes. The project was a joint effort between BND's Division I (HUMINT), Division II (SIGINT) and Division IV (HQ). In addition to the intelligence professionals, other technical experts from a variety of outside institutions were recruited, resulting in a staff of approximately 70 people. While focused initially on retrieving information, the Project Rahab staff soon turned to offensive measures that could be of use in a time of conflict, including a variety of viruses that could be inserted into target computers. Schweizer claims that the Project has "accessed computer systems in the Soviet Union, Japan, France, the United States, Italy, and Great Britain."[67] Included in the "hacks" of the Rahab staff is penetration of the SWIFT network, a dedicated international banking network that carries the majority of worldwide bank transfers. The implications of this information falling into terrorist hands are clear.

g. Iraq

Both sides waged information warfare, it appears, during the Gulf War. A Schweizer claims that a major computer penetration effort was launched during Desert Storm. A Government Accounting Office Report reinforces this claim as it outlines the efforts of Dutch hackers to penetrate U.S. unclassified military computers. The hackers exploited

---

[67]Schweizer, 161-2.

several well-known weaknesses and were able to penetrate a computer system that directly supported Operation Desert Storm. While the hackers did not attempt to shut down any of the penetrated systems, they did attempt to modify the software to provide easy access in the future.[68] While the Dutch hackers have not been publicly linked to Iraqi intelligence efforts, a similar incident, involving a German citizen was detected during the Gulf War.[69]

Lawrence Livermore Laboratories were used by "hackers" in an attempt to find information on the Patriot missile system. In this instance the actions of a third party "proxy" for Iraq had the potential to cause damage to the safety of troops on the ground, the integrity of air defenses in Israel and thus, cause a weakening of the allied coalition against Iraq. As Iraq is a known sponsor of terrorist organizations, it may turn to its proxies to carry out a cyberterror campaign against the information systems of enemy states.

h. Swiss

The Swiss, who have a long history in cryptography, may have perpetrated an information warfare attack against other nations. The Swiss firm of Crypto AG, which sells encryption technology and hardware to nations such as Iraq, Iran, Libya and Syria, has been accused of "bugging" their crypto equipment and listening in on "encrypted" communications. Furthermore, it is alleged that the Swiss firm is really owned by the German BND and that

---

[68]Government Accounting Office, *Hackers Penetrate DOD Computer Systems*, Statement of Jack L. Brock before Senate Subcommittee on Government Information and Regulation, 20 November 1991, 1-4. GAO/T-IMTEC-92-5.

[69]Madsen, 437.

the U.S. National Security Agency has played a leading role in the bugging.[70] While the firm has vehemently denied this charge, it raises several interesting information warfare possibilities. If supposedly "secure" crypto units were bugged without the knowledge of a client nation, the possibility exists that other computers or items of "high tech" equipment have been modified with less than honorable intent. Several stories have appeared on the Internet discussing both software and hardware "flaws" distributed in products. One such flaw disabled a computer program after one month of use. The possibility exists that a program could "lock up" a computer after a certain time period or after it received a certain activation command. Computer hardware, such as printers and circuit boards could also be shipped with "logic bombs" in their programs that would cause the equipment to cease functioning. The known cases that have been discussed have all been "benign" errors by public companies that have been rapidly fixed once identified. If, however, a foreign power were to insert its own bug in the software's source code *before* shipment and not activate the program until hostilities were imminent, a substantial portion of an affected computer network could be disabled.

i. Seychelles

The island nation of the Seychelles has undertaken a high technology campaign against enemies of its government in England. The nation was able to exploit the British telephone system and conduct wiretaps against several targets. The information obtained with

---

[70]"Suspicions Surface About Bugged Swiss Encryption Units," *Computer Fraud and Security Bulletin*, October 1994.

these wiretaps resulted in the assassination of an exiled anti-government leader.[71] The Seychelles demonstrate the potential threat that even a small country can pose to a superpower by using information warfare techniques. In the information age, even the smallest state or terrorist group has a chance to impact the global network.

j. Israel

While not responsible for the creation of the "Friday the 13th" virus, (supposedly developed by a Palestinian to protest the 40th anniversary of the end of the Palestinian mandate) the computer links between Israel's intelligence service and the United States served as a conduit for the virus to spread to the United States. The Israelis used a "low tech" solution to enter U.S. databases- they recruited Jonathan Pollard. While unable to "break" DIA's computers, Israel could obtain information that Pollard retrieved from computer systems and delivered to his handlers.[72] This highlights the constant "human" factor in all of intelligence. Even if your computer cannot be accessed by any type of modem or network and is sitting inside a Tempest approved enclosure, an enemy agent can still physically break-in, or have an employee access the machine, copy the information from that computer onto a floppy disk and simply walk out of the building with it. Information that would have taken a wheelbarrow to get out of a secure facility now fits on a single diskette. While "hackers" may not "break into" some of their target computers, they are still able to analyze the type of information on the computer and possibly gain some information on the type of hardware and

---

[71]Madsen, 440.

[72]Wolf Blitzer, *Territory of Lies* (New York: Harper and Row, 1989), 68.

operating system that runs the computer. While this does not help the hacker, it may allow for more "classic" espionage action to be taken by a foreign organization, such as bribing or blackmailing someone on the "inside." As Jay Peterzell highlights, "NSA has figures that make the insider threat look soberingly real. An agency log of cases involving computer crime or computer espionage showed that up to 90% of known security breaches are the work of corporate or government insiders."[73]

Israel was also involved in halting a second Patriot missile computer hacking operation. Israel detained an 18 year old for attacking U.S. defense computers to retrieve information on the Patriot missile system. Charges were not brought against the hacker, possibly to downplay the incident and not highlight existing weaknesses in computer security.[74]

B. USE OF COMPUTERS IN REVOLUTION

The use of computers in revolutions highlights the importance of information control for authoritarian regimes. Without tight control of information flow, regimes cannot control the activities of dissidents. The increasing interconnection of the world provided by computers allows dissidents to "bring in" the rest of the world. They instantly broadcast atrocities and repression to a worldwide audience, with the attendant publicity often preventing a harsh crackdown by government forces.

---

[73]Jay Peterzell, "Spying and Sabotage by Computer; The U.S. and its adversaries are tapping databases--and spreading viruses," *Time*, 20 March 1989, 25.

[74]Madsen 434.

1. Poland

A 1987 article in *Datamation* examined the use of computers in the Solidarity movement in Poland:

> Necessity and the spread of information technology have bred a computer-savvy opposition in Poland that is capable of breaking into tv news broadcasts, producing alternative information that contradicts government data, and developing publishing and distribution systems that can spread the opposition's cause quickly and efficiently.[75]

The Solidarity movement used information warfare tactics to get their message out to the largest possible number of Polish citizens. The actions of three astronomers and a local engineer exemplify the ability of a few individuals to influence thousands with information technology. These individuals intercepted the state-run television broadcast signal, determined the characteristics of the signal, and then used their computer equipment to time and configure their own signal. They broadcast this signal over the same frequency as the state signal, allowing 60,000 television viewers to see both signals concurrently. These viewers saw the message, "Enough price increases, lies, and repressions. It is our duty to boycott the election."[76] The government arrested and tried the four for this action. After being held for four months, they were convicted and ordered to pay fines ranging from $80 to $120. During their trial, the prosecutor claimed that the voting turnout was ten to 20 percent lower than average in the region that viewed the pirate television broadcast.

---

[75]Buck Bloombecker, "Of Systems, Solidarity, and Struggle," *Datamation*, 33, 21 (1 November 1987): 47, Nexis.

[76]Bloombecker, Nexis.

The Solidarity movement also used computers to perform an independent prediction of the election results. This independent check ensured that the "official" government estimates were not inflated. The struggle for the Solidarity movement was not merely to show that the official count was wrong according to Konrad Bielinski, a leader of this project. "Rather, we wanted to achieve something more, namely to take away from the state its monopoly over giving us information about ourselves."[77]

The movement also capitalized on the advantages of information technology to provide secure, reliable communication between members. Anyone can encrypt and transport a massive amount of data on disk. In addition to being easier to conceal, a computer disk is easier to destroy than a pile of paper.

2. Tiananmen Square

The Chinese dissidents involved in the Tiananmen Square protest in 1989 did not target computer systems, but rather utilized new technology, primarily the fax machine and the Internet, to ensure that word of what was happening in China made it out of the country. Students in the United States then took the information that was flowing out of China and sent it back into the country via fax machines. Through the use of this technology, the dissidents prevented China's leadership from controlling the flow of information. While telecommunications assets were restricted in the weeks following the massacre,

---

[77]Bloombecker, Nexis.

telecommunications connectivity facilitated its initial reporting and continuing coverage with the rest of the world.

3. Zapatistas

The Zapatista uprising in southern Mexico provides another example of rebel organizations exploiting high technology. The Zapatista leadership has used the Internet to establish a worldwide organization of supporters that are beyond the control of Mexico's government. Zapatista leadership communiqués are issued via the Internet, instantly spreading their message to a worldwide audience without any interference by the Mexican authorities or news media interpretation. In the same manner as China during the Tiananmen Square uprising, Mexico lost the ability to control the flow of information both out of, and into, the country. The information received from inside Mexico fostered extensive media coverage, limiting the repressive options open to the government. While not terrorism, the ability to form transnational networks and ensure that the message of an organization is heard on a world stage is a tool that terrorists will exploit in the future. If there were no rapid communications channels out of the jungles of southern Mexico, it is likely that the Mexican government would have been able to use much harsher methods to repress the rebellion.

While the actions of rebels and dissidents are not always terrorism, these incidents highlight the fact that a small number of people can have a worldwide impact and generate international publicity for their cause without government interference. These capabilities will appeal to terrorists in the information age.

C. THE RISE OF TECHNOTERRORISM

1. Electrical Distribution Networks

Electrical distribution and energy systems have been favorite targets of terrorists. The use of computers to run these networks makes them an ideal cyberterrorism target. However, as an examination of conventional terrorist and military attacks on energy systems demonstrates, these targets may be of limited value to the cyberterrorist.

Statistics show that there were 240 total attacks on "Domestic Energy-related and Military Targets" from 1970 to mid 1980. The most popular of the targets were powerlines and powerstation/substations.[78] This trend continued through 1988 with 283 recorded incidents of subnational attacks on energy systems in the United States. A worldwide target summary shows that power pylons and power lines remained the number one target with power substations being the third most popular target.[79]

Thomas E. Griffith, in his thesis entitled *Strategic Attack of National Electrical Systems*, studies the military benefits accorded a state by attacking an enemy electrical system in a time of war. The apparent lack of utility in attacking electrical systems in war may apply to terrorists as well:

---

[78]Lisa Maechling and Yonah Alexander, "Risks to Energy Production and Trade," in *Political Terrorism and Energy: The Threat and Response*, eds., Yonah Alexander and Charles K. Ebinger (New York: Praeger, 1982), 140.

[79]Congress, Senate, Committee on Governmental Affairs, *Vulnerability of Telecommunications and Energy Resources to Terrorism*, 101st Cong., 1st sess., 7-8 February 1989, 252-257.

> Strategic attacks on national power system can be useful in fulfilling national security aims, but only under specific conditions. First, the target country's power system should be vulnerable to destruction by being very concentrated with very few interconnections. Second, the strategy behind the attacks should be focused on stopping war production over the long term. To strike electric power to affect civilian morale, increase costs to the leadership, or impact the military will waste missions and could prove counterproductive to the political aims of the war.[80]

The "critical node" identified by Griffith is the transformer station, where power is "stepped-up" or "stepped-down" for transmission and distribution. The components at some of these sites are custom built and could take up to eighteen months to manufacture if they are destroyed in an attack.

The most recent concerted attack on energy systems in the United States was undertaken in California by a group calling itself the "Earth Night Action Group" who cut down two wooden power poles and toppled a 100-foot transmission tower in April of 1990. The result of this attack was the loss of power to 92,000 customers for up to a day.[81] The group struck at isolated targets rather than the transformer substations, thus lessening the impact of their action. In the late 1970s, the "New World Liberation Front" bombed a Pacific Gas and Electric transformer near San Francisco that disrupted power to 75,000 homes for approximately two hours. PG&E transformers and offices were bombed 16 times between 1975 and 1978, leading Research West, a detective agency specializing in terrorism, to call

---

[80]Thomas Griffith, "Strategic Attacks of National Electrical Systems" (M.A. thesis, School of Advanced Airpower Studies, 1994), 59.

[81]Elliot Diringer, "Environmental Demonstrations Take Violent Turn," *San Francisco Chronicle*, 24 April 1990, A3.

PG&E the "prime victim of terrorism in the United States."[82] As press reports have indicated, electrical lines themselves are the most accessible targets for terrorists or criminals. In the United States, up to 300 electrical insulators can be shot off by hunters and pranksters in a single day.[83] These actions are not a concerted effort to bring down the electrical system by an organized group. Rather, they are random acts of vandalism for which the flexibility of the electrical system can compensate. Should an organized group simultaneously attack several critical nodes (step-up/down transformers) across the United States, the potential for disruption increases. Chuck Lane's statements before Congress indicate that the system is vulnerable, but it is robust enough to withstand nearly all attacks:

> In summary, this investigation concluded that the networks [energy and telecommunication] of the United States are vulnerable to multisite terrorist attacks, that is, that targets are likely to be destroyed. However, the redundancy of built into the networks make them very dependable, and the real question is what level of service would be lost from such an attack. In many cases the consequences appear to be manageable. In a few cases, perhaps too many cases, the consequences are potentially catastrophic.[84]

While the physical vulnerability of electrical system components to destruction is real, David Hinman states, "the flexibility of the system is its greatest security. Our security plans must be built upon this fact in order to have maximum effectiveness."[85]

---

[82]Susan Ager, "Byline," *Associated Press*, 17 March 1978, Nexis.

[83]Stephen Bowman, "Lights Out: Electrical Systems an Easy Target for Terrorists," *Denver Post,* 29 May 1995, 74.

[84]Congress, Senate, 7, 11.

[85]Congress, Senate, 70.

Still, the capability exists, with relatively unsophisticated technology to disrupt power to a large portion of an electrical grid by targeting its critical nodes. While the weapons technology (firearms, explosives, etc.) are readily available to a terrorist group, some research is required to obtain the knowledge necessary to identify and target critical nodes in the energy system. Unfortunately, this information is publicly available. The information contained in public documents mandated by the Department of Energy, Federal Communications Commission, and Department of Transportation can be used by terrorists to plan attacks on infrastructure targets. According to a Government Accounting Office report of December 1988, a mock terrorist team utilized information obtained from a public library to plan an attack on the Strategic Petroleum Reserve in 1987.[86]

While infrastructure systems in the United States remain vulnerable to physical attack, Dr. Robert K. Mullen, does not believe that these incidents will increase in the future, despite a growing terrorist presence in the United States:

> That being said, there are no indicators of which I am aware, insofar as trends in the U.S. are concerned, that would suggest to me the threat to energy assets here is substantially different from what the recent historical record indicates. The presence in the U.S. of terrorist support groups does not alter this view.[87]

While the fragility and relative open nature of electrical systems has been heralded in the press, it is the secondary effects of such attacks that concern individuals like Norman Leach:

---

[86]Congress, Senate, 10.

[87]Congress, Senate, 248.

> Any terrorist group with access to moderate amounts of explosives could shut down any city in the United States simply by destroying local transformer sites. Not only would vital industries and defense programs be affected but the ensuing blackouts would cause riots in the streets that would threaten the stability of the government.[88]

While certainly a contributing factor to the civil unrest experienced in New York City's famed blackouts of 1965 and 1977, the removal of electrical power from a city is neither a necessary nor a sufficient cause for "riots that would threaten the stability of the government." The riots in the streets of Los Angeles following the Rodney King verdict as well as the riots (disguised as celebrations) after major sports championships are won show that disturbances can happen with a fully functional electrical system. The Labor Day 1988 Seattle blackout, in which over ⅓ of the city was without power for 4½ days, proves that a blackout does not produce riots and looting. In fact, the incidence of crime in the affected area went *down*, not up, due to an intense police presence.[89] The ability to cause a riot with a blackout alone is thus suspect. While a terrorist group may be able to exacerbate a crisis situation that it has fomented with the addition of a blackout, a blackout in isolation is not a failsafe way to "ignite the masses."

While the above situation has focused primarily on the physical attack of energy systems to cause disruption, the increasing computer control of these and other infrastructure systems provides a potential target for a terrorist group. The California Department of Water

---

[88]Norman S. Leach, "Terrorism in Your Own Back Yard," *Security Management,* 33, 5 (May 1989): 56, Nexis.

[89]Congress, Senate, 63.

Resources recognized the risk inherent in these systems in 1991 when they implemented strict physical security control measures to protect their central computer center. The computers contained at the center were used to control the release of water from the major dams in the state. The increased security was a result of a perceived increase in the terrorist threat during Operation Desert Storm.[90]

The possible physical risks, such as the shutdown of power plants or release of water from behind dams, will continue to increase as computerization of control systems continues. The true "critical nodes" of any system lie in its command and control network. By striking at this link to disable or control the system, a terrorist precludes the necessity to attack elements of a distributed system physically, such as transformers or pumps.

There are many parallels between energy systems and information warfare targets. Critical nodes exist in all networks that will impair the entire system. Attacking anything but these critical nodes may result in a minor degradation of service or, if the system is correctly designed, no disruption at all. Thus, the attacks on energy distribution system components such as power lines and pylons cause limited disruption for regional customers but widespread outages are very rare. While the information on the physical layout and vulnerabilities of an energy system exist, it has not been a particularly effective terrorist target. This may be due to the lack of organizational and manpower assets available to a terrorist group. In addition, those targets that are "critical nodes" may have enough security to prevent their destruction.

---

[90]Robert Crabbe, *United Press International* (Sacramento), 25 January 1991, Financial report, Nexis.

The pattern of terrorist attacks on electrical systems may provide an insight into information age terrorism. If systems can be engineered to be redundant in some areas (and thus able to recover from attack) and defended in others (to prevent attack), it may mitigate the risks of widespread outages.

2. Attacks on Computer Systems

While the public has perceived buildings and airplanes as the primary targets of terrorists, attacks on computers were involved in 60% of conventional terrorist acts by 1989.[91] The pattern of criminal computer attacks, together with terrorist activity, suggest that there may be a shift toward cyberterrorism as a physically less risky means to achieve both criminal and terrorist ends.

a. Europe and the United States

In the 1970s the Italian Red Brigades launched 27 attacks against companies that did business in the electronics, computer, and weapons sectors. In 1980, the French organization Comite Liquidant ou Detournant les Ordinateurs (Computer Liquidation and Deterrence Committee or CLODO) undertook a series of attacks on computer companies in the Toulouse region. The organization released a statement to the press, "We are workers in the field of dp (data processing) and consequently well placed to know the current and

---

[91]Marvin J. Cetron, "The Growing Threat of Terrorism," *The Futurist*, 23, 4 (July 1989): 20, Nexis.

future dangers of dp and telecommunications. The computer is the favorite tool of the dominant. It is used to exploit, to put on file, to control, and to repress."[92]

A Belgian Group, the Cellueles Communistes Combattants (Fighting Communist Cells) conducted a series of bombings in September 1984 directed against Honeywell Controls and Litton Industries. In November 1984, the same group attacked the Brussels office of Motorola. Computers were prime targets in each of these attacks.

Similar attacks have occurred in the United States. IBM's offices in White Plains N.Y. were bombed in March 1984. The group claiming responsibility for the attack, the United Freedom Front, distributed a newsletter that stated "IBM is a death merchant . . . The computer is an integral part of the fascist South African government's policies of racist repression and control."[93]

The CLODO group struck again in 1983 by firebombing a Sperry-Univac computer room in Toulouse to protest the U.S. invasion of Grenada. Upon putting out the fire, the message, "Reagan attacks Grenada- Sperry Multinational is an American accomplice." was found spray painted on an interior wall.[94]

While the attacks on computer systems failed to cause any major political victory for CLODO, they did heighten the awareness that European computers are vulnerable

---

[92]John Lamb and James Etheridge, "DP: The Target of Terror," *Datamation* 32 (1 February 1986): 44, Nexis.

[93]Lamb and Etheridge, Nexis.

[94]Reuters North European Service, "Attack Against U.S. Computer Firm" 26 October 1983, Nexis.

to attack. A 1979 report by the Swedish Defense Ministry recommended that the government become involved in monitoring computer security of both public and private computers. While the proper role of the government in computer security remains open for debate, an article in the French daily *Le Figaro* states that computer attacks might be more harmful to national security than the assassination of random politicians.[95]

b. Japan

In 1985 in Japan, the Middle Core Faction, a terrorist group consisting of approximately 300 individuals, attacked the commuter rail system to cause massive disruption during the height of rush hour. The group used C2W techniques to carry out its attack by first cutting strategic power and communications cables that fed the computer controls for the rail system. Secondly, the group jammed police and rescue radio frequencies in an attempt to hamper and delay response by the authorities. While no one was injured in this attack, it caused a major commuting delay affecting 6.5 million commuters and cost the Japan National Railways more than $6 million in lost ticket sales.[96] Rather than blowing up or tampering with the physical destruction of one rail, the group focused on the critical node (control circuits) and disabled the entire system by using technoterror, attacking physical targets to cause a disruption in cyberspace. The disruption was extensive enough that the Centralized Traffic Control Office of Japan National Railways (JNR) was forced to stop

---

[95]"France: Terror by Technology," *The Economist*, 19 April 19 1980, 44, Nexis.

[96]Eugene Moosa, "Hundreds of Police Hunt for 300 Rail Saboteurs," *Associated Press*, 30 November 1985, Nexis.

operation. While the attacks were successful in creating disruption, the effects were short lived, with most of the severed cables back in full service within 24 hours.[97] This attack, while creating problems for millions of commuters, was also linked to specific objectives. The first was to show solidarity with the National Railways Locomotive Engineers' Union, which was on strike to protest the planned privatization of the JNR. The second goal may have been to influence the trial of Hiroko Nagata, the leader of the Extreme Leftist United Red Army. Her hearing was delayed because the rail shutdown prevented her defense lawyer from making it to court on time.[98]

The combination of computer controls and energy systems raises new possibilities for terrorists. While targeting of energy systems in the past has relied primarily on the physical destruction of key assets to disrupt service, the potential vulnerability of the control systems poses an even greater risk.

c. Political Motivation

The rise of Information Warfare tactics may allow tomorrow's terrorists to focus their attacks on certain individuals to change their policies or courses of action. The increasing reliance on computers has opened new avenues for blackmail and political pressure. In 1984, a hacker penetrated TRW's credit report computers and obtained some incriminating information about a past small-claims court dispute involving then incumbent Congressional

---

[97]Moosa, Nexis.

[98]Japan Economic Newswire, "Radical Guerrilla Assaults Stop JNR Train Runs," 29 November 1985, Nexis.

candidate Tom Lantos of California. This information was passed to his opponent who further distributed the information to the press to discredit Lantos. In a second act of political computer crime, a hacker gained access to Representative Ed Zshau's computer system in Washington, D.C. and erased his data, including his correspondence and constituent database.[99]

These events highlight the potentially selective nature of future cyberterrorism and crime. With a skilled computer operator, a terrorist group may be able to penetrate systems to manipulate a small number of people. Instead of attacking the public to affect a target audience, cyberterrorists may choose to affect the target audience to achieve their ends directly.

d. Environmental Groups

While "conventional" terrorist groups have targeted computer systems in the past, "eco-terror" groups, such as Earth First, have advocated attacking computer systems. In 1987, the group published a manual that advocated both physical destruction of computer equipment (conventional terrorism) and software and data manipulation/destruction (via cyberterrorism). The manual also included techniques to reduce the risk of being caught by using advanced hacking techniques.[100] The risk of cyberterrorism exists on all fronts. It is

---

[99]Douglas E. Campbell, "The Intelligent Threat,"*Security Management* 33, 2 (March 1989): 19A, Nexis.

[100]Campbell, Nexis.

not merely limited to the "classic" conventional terrorist group. Any group with a strong interest or agenda will be able to attempt cyberterrorism.

e. Criminal Activity

Criminal activity directed at, or using, computers is receiving increasing attention in the press. The expansion of the Internet to include commercial ventures has sparked a debate over the correct level of security that should be afforded individuals in cyberspace. As terrorism is often crime with different intent, several criminal acts will be explored in this section. First, the case of a Russian hacker attempting to steal more than $10 million highlights the vast amount of money being transferred in cyberspace. Second, the attempt to use computer viruses to hold computers hostage or attack a specific company will be examined. Finally, the possible physical risks to individuals as a result of criminal cyberspace activity are addressed in the case of a Texas professor.

(1) Citibank. The use of computers and computer technology to perpetrate crimes has already occurred. Citibank recently "lost" $10.2 million electronically to a team of Russian hackers. A closer examination of the facts involved in this incident reveals some strengths and weaknesses of computer crime. First, the authorities can use the same technology employed by the cyberterrorist or criminal to track and capture him. Someone can, however, remain anonymous in cyberspace if they are not seeking financial gain, as virus writers have proven.

This incident, according to John Mohr, vice president of the New York Clearing House, is unique in that it utilized a personal computer.[101] It appears that Vladimir L. Levin, a Russian computer expert employed by AO Saturn, a St. Petersburg trading company, broke into Citibank's computer system using stolen account identification numbers and passwords. With this information, he made 40 transfers from Citibank to accounts set up by accomplices in California and Israel. These transfers occurred from June to October 1994 and were tracked by Citibank to determine who was responsible for the crime. While Citibank allowed the transfers to continue, the accounts into which he was transferring the money were frozen. While Levin attempted to transfer more than $10 million in this period, Citibank has recovered all but $400,000. Amy Dates of Citibank had the following answer when questioned about the level of security at Citibank: "We move half a trillion dollars a day through the payment system. Compare that to the $400,000 they were able to withdraw. We think we have the right level of security."[102] Despite these statements, Citibank implemented a new computer protocol to increase transaction security.

It is still unclear how Levin obtained the account numbers and their associated passwords, but an investigation is continuing into the possibility of inside help. Citibank, has implemented a new security system for its computer accounts that entails the use of "smart cards" that will generate a new password for each transaction. This technology

---

[101]Saul Hansell, "Citibank Fraud Case Raises Computer Security Questions," *New York Times*, 19 Aug. 1995, 31.

[102]Hansell, 31.

helps to defeat password "sniffer" programs that allow criminals to capture passwords as they are transmitted across the network for future use. This may have been how Levin obtained his passwords. He appears to have had access to the network for some time before attempting his crime as he was careful to follow the patterns of routine transactions and kept his individual transfers to below $300,000 to avoid "built-in" security programs that would have highlighted the transaction as abnormal.[103]

While the adoption of the smart card security system and the employment of encryption technology has, Citibank hopes, corrected the security weakness exploited by Levin and his friends, the amount of money lost in this crime is relatively small. The high level of publicity afforded this incident is due to its extranormality, not its dollar value. Each year, according to the American Bankers Association, the following amounts are lost due to crime: Check fraud- $10 *Billion*, Credit Card fraud- $712 Million, ATM fraud- $18 Million, and Online fraud (as in the Citibank case)- $5 Million.[104] While Citibank could use its computers to track and eventually catch Levin, computers and high technology aided in the success of a Vietnamese check fraud ring that operated undetected for seven months. The U.S. Secret Service investigated the crime under the name, "Operation Paper Dragon" and found that the ring took in $25 Million in just over half a year.[105] These high technology

---

[103]John Manson, "Bank's Security Chain's rattled," *Financial Times* (London), 20 September 1995, 20, Nexis.

[104]Kelley Holland, "Bank Fraud, The Old-Fashioned Way," *Business Week,* 4 September 1995, 96, Nexis.

[105]Holland, Nexis.

money making schemes may appeal to terrorist organizations of the future who are unable to secure, or do not desire, state sponsorship. While attractive to terrorists, the security measures put in place by the banking industry to prevent criminals will likely defeat terrorists as well.

(2) Viruses. In an apparent attempt to extort money, the computers of several universities were infected with a virus in an attempt to make them hostages. The virus demanded a ransom for the antidote to the virus.

> Computer users who found the virus were told to send $2,000 to an address in Pakistan to obtain an immunity program that would rid the system of the virus. Investigation showed that the virus was written by two brothers in a computer store in Lahore, Pakistan–they had put their names, and address, and a phone number in the virus! "It's like a fantasy of being a terrorist without the blood," said Eric Corley, editor of a national hacker newsletter, 2600, whose electronic bulletin board was also infected.[106]

The brothers' scheme did not pay well, and the virus was eradicated without their "immunity program." The "fantasy" of being a terrorist without the blood may become reality when an organization uses cyberterror weapons in an attack.

Recently, a virus was used to attack a specific business in Germany. A virus writer, known only as "The Wizard" created then released a virus that he called the "Media Markt advertising virus." Media Markt is a German home-electronics group and was not involved in the virus writing or distribution. Media Markt's lawyer claims that "this is the first time that someone has distributed a virus and tied it to a company that has nothing to do

---

[106]Campbell.

with it."[107] To stave off negative publicity, Media Markt has distributed an anti-virus program to disable the virus on affected computers.

While the true intention of the virus writer may never be known, the principle of indirect attack (attacking the general public to influence a target audience) normally utilized by terrorists was evidenced in these tactics. The virus writer, unleashed an attack on the "innocent" computer users to create negative publicity for Media Markt. In this case, Media Markt was clearly not involved in this activity. However, the anonymous and anarchic nature of cyberspace opens the possibility of creating chaos and making it appear as if someone else is responsible. While it appears that financial gain motivated the Russian hackers in the Citibank case, the possibility exists that terrorists or criminals could perpetrate electronic attacks in the future to weaken the target company, not make money. If a terrorist group could place someone "on the inside" of a software company and infect software with a virus *before* shipment, it may call the integrity of that software company into question. While there are no reported cases of terrorists staging a concerted information warfare attack on a business, the case of Citibank might be a benchmark. Despite news that it had lost more than $10 million, Citibank stock went *up* by ½ a point on the day that the Russian hacker story broke.[108]

---

[107]Matthew May, "Super Snoopers or Plain Bad?" *Times* (London), 18 August 1995, Nexis.

[108]"Wall Street Friday" *AFX News*, 21 August 1995, Nexis.

(3) Personal Attacks. The potential exists for terrorists to single out individuals in cyberspace. In 1994, a hacker logged into a Texas A&M professor's E-mail account and used the account to send out 20,000 racist messages. To those receiving the messages, it appeared that they had come from the professor. As a result, the professor began to receive death threats.[109]

3. The Threat From Hackers Turned Terrorist: Is it real?

Penetration of computer systems is not difficult. The U.S. Defense Information Systems Agency undertook a penetration study of Department of Defense computers. In 1994, the agency attacked 8,932 servers and mainframes. They were able to gain access to 7,860 (88%) of these systems. Only 319 (4%) of these attacks were detected and only 19 (.2%) of the successful attacks were ever reported.[110] The percentages suggest that even organizations that depend on computers to function rarely know when hackers have attacked them. Penetration of DOD systems has also been documented by other than DOD assets, such as the case of Defense computers being attacked by Dutch hackers during the Gulf War. While none of these penetrations were used for terrorist purposes, it is entirely possible that this may occur in the future. Even if the hackers initially do not have terrorist intentions, they remain dangerous. A Government Accounting Office report on the Dutch hacker case states that, "the majority of the hackers' activities appeared to be aimed at gaining access to DOD

---

[109]Rochelle Garner, "The Growing Professional Menace," *Open Computing*, July 1995, 32, Nexis.

[110]Garner.

computer system and then establishing methods for later entry.[111] Should a computer hacker decide to work with terrorists, or be forced to work with terrorists via blackmail, these methods for later entry constitute a serious risk.

The jump from hacker to terrorist is a small one that depends entirely on the hacker's motivation and intent. While these cases prove that hackers can penetrate systems, it does not examine the motivation for the hacker. Several studies of the group dynamics and individual motivations for terrorists have been undertaken to help prevent terrorism. While similar studies on the "computer underground" have been undertaken, an analysis of how a terrorist organization might recruit a hacker would be worthwhile.[112] As the world becomes more dependent on computers, understanding what makes hackers "tick" becomes as important as understanding what motivates terrorists.

4. The Internet Worm

The 1988 Morris Internet Worm incident highlights the incredible disruptive power of information warfare tactics for a cyberterrorist, as well as the limitations inherent in attacking computers.

On November 2, 1988, Robert Tappan Morris, a Cornell University graduate student, released a "worm" onto the Internet. While Morris maintains that it was just an experiment

---

[111]Government Accounting Office, *Hackers Penetrate DOD Computer Systems*, Statement of Jack L. Brock before Senate Subcommittee on Government Information and Regulation, 20 November 1991, 1-4. GAO/T-IMTEC-92-5.

[112]Gordon R. Meyer, "The Social Organization of the Computer Underground" (M.A. thesis, Northern Illinois University, 1989).

that went terribly wrong, the Justice Department decided to prosecute Morris, who was found guilty of a felony and sentenced to three years probation, $10,000 fine and 400 hours of community service. In March of 1991, his appeal to the U.S. Court of Appeals for the second circuit was unsuccessful, In the fall of 1991, the U.S. Supreme Court refused to hear his case.[113]

The worm program, created as an experiment by Morris, was based on three separate security flaws that Morris had discovered in the Berkeley version of the UNIX operating system. The goals of his program were: to infect three computers per network location across the Internet, to avoid slow machines and any network that was in use (to avoid detection by operators), use infected computers to find connections to other uninfected computers, steal the password files of computers and use the passwords to gain access to even more computers.[114]

Computers had fascinated Morris his entire life. Morris' father, Bob Morris, was a computer engineer for Bell Labs, the creators of the UNIX operating system. The area of computer security had been a hobby of Robert Morris throughout his college years. His knowledge of computer systems was so extensive that both the Naval Research Laboratory and the National Security Agency, NSA (where Bob Morris was serving as director of the National Computer Security Center) invited him to speak to the topic of UNIX operating

---

[113]Katie Hafner and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier* (New York: Touchstone/Simon and Schuster, 1991) 345-6.

[114]Hafner and Markoff, 296.

system security. That this was a problem about which the NSA was deeply concerned became apparent during Morris's trial. The presentation to the NSA was videotaped and the prosecution intended to show part of the tape concerning "how not to get caught" to show that Morris had written his program with malicious intent to break into computers. Robert's defense lawyer, Tom Guidoboni, threatened to force Robert's father to testify about the National Security Agency's interest in computer penetration, to include divulging classified material if the tape was shown. Possibly as a result of NSA pressure, the tape was not used in the trial and the NSA was able to protect its secrets.[115]

The knowledge that Robert Morris had obtained in his study of computer security was extensive. He had been aware of two flaws in the UNIX system for over a year before his worm was released. The final flaw, in the FTP, File Transfer Protocol, program (a utility in UNIX that allows individuals on different computers to transfer files back and forth between remote systems) was corrected before Morris could finish his program, so he was forced to adjust and exploit only the remaining two weaknesses. These weaknesses were in the *sendmail* portion of the operating system and in the *finger* utility. It was a combination of these two weaknesses that allowed the worm to spread from computer to computer. The worm was originally designed to limit its growth, with each copy of the program checking to see if other copies were already running on a system before attempting to replicate. If there were other copies running, they would "negotiate" with each other to see which one would

---

[115]Hafner and Markoff, 328-9.

terminate. Unfortunately, the program that agreed to terminate would infect many other computers before it stopped running. Additionally, one in seven of the copies of the worm would not check to see if there were other copies present before infecting a machine. In effect, it refused to die on its own. This "one in seven" system, coupled with the fact that the portion of the program controlling worm to worm communication was improperly written, led to a massive proliferation of worms on thousands of computers on the Internet, causing delays and forcing machines to be taken off the network.

The battle to "beat" the worm was intense. The meeting of Berkeley UNIX experts was fortuitous in that several leading experts, including the creators of the operating system were in the same place and were able to collaborate on finding a solution to the problem. Within 24 hours, the Berkeley team had discovered how the program spread and had corrected the problems in the *sendmail* portion of the operating system. In less than 48 hours, all the weaknesses that the program attempted to exploit were corrected and the "fixes" were sent out to all users on the Internet. The attempt to understand the virus was hampered by its having been encrypted by Morris. Fortunately, the encryption scheme was extremely weak and was quickly broken, allowing the experts to unscramble the code. The next step was to "reverse engineer" the code by decompiling it into source code to study its design and ensure that it did not have "malicious" (data altering/destroying) instructions hidden in the program. Fortunately for the users of the Internet, Morris did not write the worm to destroy data on infected computers, it would merely replicate out of control until the machine became overwhelmed with copies of the worm. Had the worm been written to

destroy data, the recovery time would have been much longer with potentially massive data loss. Despite the rapid response of system experts, the publicity created by the incident was nearly as overwhelming in the media as the worm was to the infected computer systems. The worm caused so much disruption that the *New York Times* carried the story on page one for an entire week. Additionally, both the *Wall Street Journal* and *USA Today* gave it front-page coverage. Television news and talk shows were also filled with discussion on the worm.[116]

This incident, while not malicious, highlights the power of information warfare techniques to cause massive disruption without physical harm to equipment or people. One man created a national computer crisis with a small program that received international attention and was addressed at the highest levels of the U.S. government. While appearing attractive for terrorists, this incident highlights both the positive and the negative aspects of information warfare for terrorism.

5. Positive and Negative Elements for the Cyberterrorist

The ability of one man, in this case Robert T. Morris, to generate such an enormous amount of disruption and publicity with a small 3,000 line computer program might be very appealing to a terrorist organization attempting to achieve its aims with minimum effort and risk. Morris was eventually brought to trial for his worm, mainly because he spoke of its creation to several people. A dedicated cyberterrorist could remain anonymous in the same

---

[116]Peter J. Denning, "The Internet Worm" in *Computers Under Attack: Intruders, Worms, and Viruses* Peter J. Denning ed. (Massachusetts: ACM Press, 1990) 193-4.

manner that the overwhelming majority of virus writers (such as the author of the famous Michelangelo virus - who remains unidentified) escape identification.

The personal equipment and money expenditures required for this incident were minimal as Morris had access to Cornell University's computers. While in the late 80s, Internet access was not widespread, today it is expanding at an exponential rate, with more individuals connecting to the network every day. The number of host computers connected to the Internet rose 30% from 1 July to 1 October 1994.[117] The possible avenues of attack have expanded exponentially, as all that is required for a computer attack is a computer, a modem, and a skilled operator with the requisite information. The increasing number of host computers represent both new targets and new platforms from which to launch an attack.

As the power of computers doubles every 12-18 months, the computing power that was once reserved for major corporations and the government is now available to individuals. Since the "tools" are widely available, it is now the knowledge of how to manipulate those tools that is most important to perpetrate a computer attack. The knowledge that Morris used to attack the Internet came from extensive study of the UNIX operating system. He had known about the flaws for at least a year before writing his program to exploit their weaknesses. The correction of the FTP weakness immediately before Morris completed his worm program highlights the fragility of this information. Had that been the only weakness known to Morris, all of his work would have been for naught. An external attack on a

---

[117]Figures obtained from Internet Society International Host Distribution survey at ftp.isoc.org/isoc/charts2/hosts/hosts.xls. Also see *Internet World*, November 1995.

computer system usually occurs through weaknesses in the software that are unknown to the creators of the software. Those attempting to gain unauthorized access to a system exploit these "bugs" in programs. Once a "bug" is discovered, software developers usually rapidly distribute a "patch" that will correct the error. The flaw that took a hacker several months to find can be corrected in a matter of seconds with the installation of a software patch. The hacker or cyberterrorist is then forced to search for yet another weakness in the system. That flaws in software exist, and are often unknown until exploited, is a double-edged sword for the potential cyberterrorist. If cyberterrorists learn of a weakness in a computer system, every day that they wait to exploit that weakness may allow a legitimate security professional or non-malicious hacker to discover and advertize the weakness, leading to the rapid distribution of a software or hardware fix to the problem. Additionally, if cyberterrorists wish to create massive disruption, they will be forced to "show their hands" and exploit the weakness on a large number of systems or on several high value systems. If they are clever, they may be able to throw system managers off the track for a short period of time.

Additionally, by using publicly available encryption techniques, they can scramble their program so that it will take years to decrypt and examine. This will exacerbate the fear of the unknown, as system managers will be unable to determine the true intent of the program. If malicious, it may require the systems to be completely shut down and all the software reloaded from a "known" clean source. If the rouge program could not be completely understood and then removed without damage, a complete shutdown would be required for all systems that handled critical data or were used to control systems upon which human lives

depend. The disruption would be far greater than that caused by the Morris worm, as it could be controlled, decrypted and safely removed from systems without damaging any of the existing software or negatively affecting the integrity of data on the machines.

The recent controversy over Netscape Corporation's use of encryption to secure Internet transactions highlights the strength and weakness of current encryption schemes. This particular encryption program was designed to allow users to send confidential information (such as credit card numbers) across the Internet securely. A French graduate student in mathematics used two supercomputers and 120 computer workstations to "brute force" decrypt (trying all possible combinations of the "key" in succession until the correct one is found) a message using this encryption program in just less than eight days. This encryption scheme used a 40 bit key (meaning its "key" length was 40 bits- a bit is a single 0 or 1 in binary code) since it was the most powerful scheme that the U.S. government would allow to be exported. The key employed by Netscape within the United States is 128 bits. This 128 bit key, utilizing the same decryption techniques, would take 10^{26} more time to break (about 2.1918×10^{24} *years*).

In less than one month after the brute force decrypting of the 40 bit message, two graduate students at Berkeley discovered a software flaw that would allow them to decode a message encrypted with the 128 bit key in less than one minute. Netscape promptly fixed

the problem and released an updated version of the encryption program within days to re-secure the system.[118]

The ability to create a program or send each other messages that would take law enforcement or government agencies 2.1918×10^{24} years to unscramble is very appealing to cyberterrorists and common criminals. If a law enforcement agency intercepts an encrypted computer message, it is useless until it can be decrypted. This may allow cyberterrorists to move away from using the slow, but relatively secure, face-to-face method of communication for a potentially more secure, worldwide, and nearly instantaneous communication channel offered by encrypted E-mail. The Institute for National Strategic Studies concluded that the communications signals themselves are becoming harder to intercept with the advent of "digital technology, frequency-hopping and spread-spectrum technologies, plus replacement of microwave with optical fiber for long-distance communication." The rise of public key encryption led the Institute to conclude that the capabilities of the codemakers are outpacing those of the codebreakers.[119] The growing ubiquity of encryption, despite several setbacks, as in the Netscape case, has still made it difficult to obtain information that individuals desire to keep secure.

The value of encryption, and the ability of business to drive a response to crime, can be seen in the development of the GSM (Global System for Mobile communications) cellular

---

[118]Aaron Zitner, "Netscape Flaw Seen Setback for Business," *Boston Globe*, 20 September 1995, 33.

[119]*Strategic Assessment 1995* (Washington D.C.: National Institute for Strategic Studies, 1995), 153.

phone standard, which uses encrypted digital signals to prevent eavesdropping and phone fraud. While in the United States, which uses an analog system, AMPS (Advanced Mobile Phone Service), a thief can steal the user ID to a cellular telephone (by intercepting its unencrypted signal) to perpetrate phone fraud. In GSM, this signal is randomly encrypted each time the phone is used, making it useless unless the correct "key" to decrypt the signal is in the possession of the interceptor. While the GSM system cuts down on cellular phone fraud, it also compounds the difficulty of intercepting the communications of known terrorists.

Unlike the physical world, in which a potential aggressor needs time and money to procure or manufacture its weapons, and time to train people to use these weapons, all of which can be observed and defenses readied by the target of aggression, the preparations of "weapons" in cyberspace is often the work of one (or several) individuals and occurs in the relative privacy and security of their own computers. With the explosion of processing power, the computers sitting in homes throughout the world are more powerful than the minicomputers of a decade ago. Unlike conventional terrorism, where the weapons of destruction are outlawed or restricted to use by the state, the weapons in cyberterrorism are available equally to the state and the terrorist organization. For a cyberspace WMD, the critical component becomes knowledge of computer systems, not the ability to procure fissionable material. The state and the terrorists operate on nearly equal footing in cyberspace.

The rapid recovery and complete eradication of the Internet worm, to include defenses against it ever occurring again, are not paralleled in the conventional world. A truck bomb manufactured from fertilizer and diesel fuel will cause damage and terror every time a terrorist parks it in or near a building and detonates it. Despite knowing the damage that car and truck bombs can cause through numerous attacks in the Middle East throughout the 1980s, authorities in the U.S. were unable to prevent the World Trade Center Bombing in New York City or the Murrah Federal Building bombing in Oklahoma City. While improved technology and procedures allow authorities to respond more rapidly to these attacks and take some limited measures to prevent the attacks, they cannot ensure that a "copycat" crime will not occur. In cyberspace, once a vulnerability is noted and a software fix is distributed, a second attack of exactly the same nature will *always* meet with defeat. What was once an open door becomes an impenetrable brick wall. If cyberterrorists were planning to exploit an identified and corrected weakness, all their effort was for naught. Their cyberspace "bomb" simply will not work. They can attempt to take his bomb elsewhere, but only if computer security administrators have shirked their duties and not installed "fixes" will they succeed.

The limited and fragile nature of weaknesses in cyberspace will force cyberterrorists to choose their targets carefully. Since an attack in cyberspace is likely to be a "one shot deal," terrorists must consider the cyberspace target to be of sufficient value to use their one-shot weapon. If a target is not sufficiently valuable, a cyberterrorists may choose to risk waiting until they can penetrate a system that will carry a substantial impact if attacked. A second factor affecting the nature of a cyberterrorist target is the likelihood that the disruption

created will be temporary instead of permanent, as in the case of physical destruction of a target by a conventional or technoterrorist. The temporary nature of the disruption may cause cyberterrorists to string together numerous attacks to create disruption of increased duration.

V. CONCLUSIONS

The vulnerability of U.S. telecommunications and other infrastructure targets led to hearings before Congress, numerous reports and books, and grist for the "technothriller" novel industry. The relative weakness of U.S. 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, technoterrorism, and cyberterrorism. Conventional terrorism will continue to operate exclusively in the physical world. Technoterrorism will operate in the physical world to create a cyberspace disruption and cyberterrorism will operate exclusively in cyberspace. To address the level of threat posed by these 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 of systems as opposed to destruction of property and the killing of citizens. 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 U.S. government 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.

A. SHIFTING DEFINITION OF TERRORISM

1. The Role of Violence in 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 without physical harm to individuals. The violence of the cyberterrorist exists exclusively 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 no casualties, this action will still fulfill the goals of advertizing, 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.

B. IMPACT ON TERRORISM IN 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 as described by J. Bowyer Bell 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.

1. 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 elements. 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.

2. 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 means to support an international terrorist organization are now becoming connected to the world via the Internet and new telecommunications systems. Argentina, Iran, Peru, Egypt and the Philippines had the highest percentage growth in Internet connections from July to October of 1994. Each experienced growth ranging from 419% to 134%.[120] All regions of the world do not match these numbers. Africa has 35 of the world's least developed states in terms of telecommunications, an essential ingredient for connectivity with the rest of the world. Over the last 10 years, Africa has had the lowest growth in teledensity, the number of main telephone lines per 100 inhabitants. It was estimated to be .91 in 1991. States such as Sweden, with an index of 68, Switzerland, Canada, Denmark, Finland, and the United States, all with indexes in the 50s, lead the world in teledensity.[121] 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

---

[120]Internet Society Figures.

[121]William Wresch, "New Lifelines," *Internet World* November 1995, 103.

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.

3. 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, 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. The role of computers and fax machines in the Tiananmen square uprising is well documented. The Zapatista rebel organization in Mexico used the Internet and World Wide Web extensively to promote their cause and get their "message" to sympathetic audiences around the world.

4. Rise of Disruption not Destruction

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 without 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.[122]

In the information age, shifting the definition of terrorism to include violence in cyberspace may be necessary, where electrons, not people 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

---

[122]Arquilla and Ronfeldt, 141.

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.

5. 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 techno and 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.

a. 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.

C. 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 U.S. 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.

1. Government Response to the Problem

The U.S. government, through a variety of agencies is responsible for the vast majority of counter and anti-terrorism activities and policies in the United States.

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 U.S. citizens in the physical world, with force if necessary, it has not made the same sweeping commitment to its citizens in cyberspace. The concept of being an "American" in cyberspace rapidly loses any meaning with the explosion of international connections to the Internet. While a computer may be physically located in the United States, the majority of its users may reside in another country. Should the U.S. government defend the rights of these individuals in cyberspace in the same manner as "official" U.S. citizens?

2. 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, with products such as Netscape offering 128 bit encryption for U.S. transactions 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 in the United States, rather, it only affected about 2% of ATM users. In several years, with the addition of global cellular communications equipment, the paths that data will have from point A to B will be redundant to a point where a terrorist could not disable all of them at once.

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.

3. The Middle Road

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 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 messages 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 (witness the Clipper chip controversy). 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 has 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 it 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.

D. FUTURE RESEARCH

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 terrorist training bases in Libya? 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 the United States are no longer secure. We must recognize the potential threat and adjust our thinking to formulate an effective individual and state response.

APPENDIX A: TERRORISM TYPOLOGY

A. TYPOLOGY

"Conventional" terrorism is important because cyberterrorism will remain, in the near future, subordinate to conventional terrorism. The implications of information warfare tactics and techniques for both terrorism and counterterrorism are summarized in this typology to highlight how terrorism and the response to terrorism may change in the future.

1. From Conventional Terror to Cyberterror

The following chart summarizes the key components of "conventional" terrorism, technoterrorism, and cyberterrorism.

Conventional Terrorism	**Technoterrorism**	**Cyberterrorism**
Targets exist in "real" space •Airlines •Buildings •High Profile individuals •Low Profile individuals	Targets exist in "real" space with cyberspace and "real" space impact •Electric Grids •Computer Networks •Telecommunications	Targets exist exclusively in cyberspace with "real" space impact •Telecommunications •Computer Networks •Control Networks
Creates physical threat	Creates physical and "virtual" threat	Creates "virtual" and physical threat
Weapons: •Explosives •Guns	Weapons: •Explosives •Guns	Weapons: •Malicious Software •EMP Weapons (For data manipulation or destruction)
Techniques: •Bombings •Kidnaping •Assassination	Techniques: •Bombing •Physical Destruction of Key Components	Techniques: •"Virtual" destruction of targets in cyberspace •Disabling of system software •Overwhelming of control systems

Size of Group: •Large Group=large potential impact •Small Group=small potential impact	Size of Group: •Large Group=large potential impact •Small Group=smaller potential impact	Size of Group: •Large Group=large impact •Small Group=large impact
Large amount of money required for large impact	Moderate amount of money required for large impact	Small amount of money required for large impact
Physical risk is high for terrorist	Physical risk is moderate for terrorist	Physical risk is very low for terrorist
Value of state sponsorship: •Money •Equipment •Training •Basing •Intelligence support •Transportation	Value of state sponsorship: •Money •Intelligence •Training •Equipment •Transportation	Value of state sponsorship: •Intelligence
Role of the media: critical	Role of the media: critical	Role of the media: moderate
Laws are clear	Laws are clear	Laws are nebulous
Intel/Info requirements for success are low	Intel/Info requirements for success are moderate	Intel/Info requirements for success are vitally important
Communications vital for success and a vulnerability	Communications vital for success and a vulnerability	Communications vital for success and normally secure. (encryption-global connectivity)
Disruption potential is moderate •Coordinated/distributed attacks hard	Disruption potential is large •Coordinated/distributed attacks difficult	Disruption potential is immense •Coordinated/distributed attacks relatively easy
Type of Groups: •Nationalist-separatist-irredentist •Issue •Ideological •Exile •State/State-sponsored •Religious fanaticism	Type of Groups: •Nationalist-separatist-irredentist •Issue •Ideological •Exile •State/State-sponsored	Type of Groups: •Nationalist-separatist-irredentist •Issue •Ideological •Exile •State/State-sponsored
Physical presence required for attack to be successful •Borders matter	Physical presence required for attack to be successful •Borders matter	Physical presence NOT required for attack to be successful •Borders nonexistent
Attack has focused effects	Attack has diffuse effects	Attack can have either focused or diffuse effects

Prevention/Response Measures

Conventional Terrorism	**Technoterrorism**	**Cyberterrorism**
Deter •Sponsoring State Military response Economic response •Legal mechanisms	Deter •Sponsoring State Military response Economic response •Legal mechanisms	Deter Who? How?
Defend •Physically "harden" targets (buildings) •Prevent access to targets (airport security) •Increase intelligence gathering	Defend •Physically "harden" targets (buildings/transformers/ pipelines) •Increase intelligence on potential targets	Defend •"harden" computer systems •increased training in security •Increase intelligence gathering
Disrupt •Infiltrate groups •Discredit leadership •Communications links	Disrupt •Infiltrate groups (harder) •Discredit leadership (if identifiable)	Disrupt •Take away comm channels •Prevent repeated access attempts
Preempt •Strike groups before attacks	Preempt •Strike groups before attacks	Preempt •strike computers with IW weapons •Physically destroy computers or attack group members

APPENDIX B: SAMPLE TERRORISM DEFINITIONS

The official definition of terrorism contained in Title 22 of the United States Code, Section 2656f(d) is as follows:

> The term "terrorism" means premeditated, politically motivated violence perpetuated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience.

Components of this government definition are seen throughout the academic literature on the subject of terrorism. These definitions range from the limited to the all inclusive. In a questionnaire sent out to leading terrorism scholars by Alex Schmid, the following responses were given to the question "Whose definition of terrorism do you find adequate for your purpose?"

Authors Mentioned	Number of Citations
There is no adequate definition	10
My own definition is adequate	9
No answer	5
Walter	4
Thornton	3
Crenshaw (Hutchinson)	3
Wilkinson	3
Jenkins (& Johnson)	3
U.S. National Advisory Committee on Criminal Justice	3
Paust	2

Table 1[123]

[123]Alex P. Schmid, *Political Terrorism* (New Brunswick: Transaction Books, 1983), 73.

Several of the more popular definitions of terrorism are quoted below in order to show the common threads of violence and political intent in the academic definitions of terrorism:

> Terror is a symbolic act designed to influence political behavior by extranormal means, entailing the use or threat of violence.[124]

> . . . the use or threat of use, of anxiety-inducing extranormal violence for political purposes by any individual or group, whether acting for or in opposition to established governmental authority, when such action is intended to influence the attitudes and behavior of a target group wider than the immediate victims and when, through the nationality or foreign ties of its perpetrators, its location, the nature of its institutional or human victims, or the mechanism of its resolution, its ramifications transcend national boundaries.[125]

> . . .terrorism- the attack on an individual to frighten and coerce a large number of others- is as old as civilization itself. It is the recourse of a minority or even of a single dissident frustrated by the inability to make society shift in the desired direction by what that society regards as 'legitimate' means. It is primarily an attack on the rule of law, aimed either to destroy it or (as in more recent times) to change it radically to conform to the terrorist's idea of society. (. . .) Terrorism is not precisely the same as violence. Terrorism aims, by the use of violence or the threat of violence, to coerce governments, authorities or populations by inducing fear. Television has enormously expanded their ability to do so.[126]

---

[124]Thomas Perry Thornton, "Terror as a Weapon of Political Agitation," *Internal War: Problems and Approaches*, ed. Harry Eckstein (New York: Free Press of Glencoe, 1964), 73.

[125]E.F. Mickolus, *Transnational Terrorism: A Chronology of Events, 1968-1979* (London: Aldwych Press, 1980), XIII-XIV as quoted in Schmid *Political Terrorism*.

[126]R. Clutterbuck *Guerrillas and Terrorists* (London: Faber and Faber, 1977), 11,21 as quoted in Schmid *Political Terrorism*.

Terrorism is a method of combat in which random or symbolic victims serve as instrumental targets of violence. These instrumental victims share group or class characteristics which form the basis for their selection for victimization. Through previous use of violence or the credible threat of violence other members of that group or class are put in a state of chronic fear (terror) . This group or class, whose members' sense of security is purposively undermined, is the target of terror. The victimization of the target of violence is considered extranormal by most observers from the witnessing audience on the basis of its atrocity; the time (e.g. peacetime) or place (not a battlefield) of victimization or the disregard for rules of combat accepted in conventional warfare. The norm violation creates an attentive audience beyond the target of terror; sectors of this audience might in turn form the main object of manipulation. The purpose of this indirect method of combat is either to immobilize the target of terror in order to produce disorientation and/or compliance, or to mobilize secondary targets of demands (e.g. a government) or targets of attention (e.g. public opinion) to changes of attitude or behavior favoring the short or long-term interests of the users of this method of combat.[127]

[127]Schmid, 111.

BIBLIOGRAPHY

Alexander, Yonah and Charles Ebinger, eds. *Political Terrorism and Energy: The Threat and Response*. New York: Praeger, 1982.

Alexander, Yonah, David Carlton, and Paul Wilkinson. *Terrorism: Theory and Practice*. Boulder CO: Westview Press, 1979.

Bell, J. Bower. *A Time of Terror*. New York: Basic Books, 1978.

Blitzer, Wolf. *Territory of Lies*. New York: Harper and Row, 1989.

Chairman of the Joint Chiefs of Staff. *Memorandum of Policy Number 30*. Washington, D.C., 8 March 1993.

Clark, Richard C. *Technological Terrorism*. Old Greenwich CT: Devin-Adair, 1980.

Clutterbuck, Richard. *Terrorism and Guerrilla Warfare*. New York: Routledge, 1990.

Coakley, Thomas P. *Command and Control for War and Peace*. Washington, D.C.: National Defense University, 1991.

Cohen, Frederick B. *Protection and Security on the Information Superhighway*. New York: John Wiley and Sons, 1995.

Cooper, James A. *Computer and Communications Security*. New York: Intertext, 1989.

Denning, Peter J., ed. *Computers Under Attack*. Reading MA: ACM Press, 1990.

Eckstein, Harry, ed. *Internal War: Problems and Approaches*. London: Free Press of Glencoe, 1964.

Ederington, L. Benjamin, and Michael Mazarr, eds. *Turning Point: The Gulf War and U.S. Military Strategy*. Boulder: Westview Press, 1994.

Gutteridge, William F. *Contemporary Terrorism*. New York: Facts on File Publications, 1986.

Hafner, Katie and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon and Shuster, 1991.

Handel, Michael I. *Masters of War: Sun Tzu, Clausewitz and Jomini*. Portland: Frank Cass c/o International Specialized Book Services, Inc., 1992.

Hoffman, Bruce. *Recent Trends and Future Prospects of Terrorism in the United States*. Santa Monica CA: Rand Corporation, 1988.

Hoffman, Bruce. *Responding to Terrorism Across the Technological Spectrum*. Santa Monica CA: Rand Corporation, 1994.

Kurz, Anat, ed. *Contemporary Trends in World Terrorism*. New York: Praeger, 1987.

Laqueur, Walter. *The Age of Terrorism*. Boston: Little, Brown and Co., 1987.

Libicki, Martin, C. *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*. Washington, D.C.: National Defense University, 1994.

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

Netanyahu, Benjamin, ed. *Terrorism: How the West Can Win*. New York: Farrar, Straus, Giroux, 1986.

Planning Considerations for Defensive Information Warfare: Information Assurance. Report prepared for Defense Information Systems Agency, Joint Interoperability and Engineering Organization, and Center for Information Systems Security by SAIC under Task order 90-SAIC-019, 16 December 1993.

Power, Richard. *Information Warfare: A CSI Special Report*. San Francisco: Computer Security Institute, 1995.

Reich, Walter, ed. *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*. New York: Cambridge University Press, 1990.

Rowe, Wayne, J. *Information Warfare: A Primer for Navy Personnel*. Newport RI: Naval War College, Center for Naval Warfare Studies, 1995.

Schmid, Alex P. *Political Terrorism*. New Brunswick: Transaction Books, 1983.

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

Schweizer, Peter. *Friendly Spies*. New York: Atlantic Monthly Press, 1993.

Simon, Jeffrey D. *The Terrorist Trap*. Indianapolis: Indiana University Press, 1994.

Slater, Robert O. and Michael Stohl, eds. *Current Perspectives on International Terrorism*. New York: St. Martin's Press, 1988.

Sloan, Stephen. *Beating International Terrorism: An Action Strategy for Preemption and Punishment*. Maxwell AFB, Alabama: Air University Press, 1986.

Smith, G. Davidson. *Combating Terrorism*. New York: Routledge, 1990.

Sterling, Claire. *The Terror Network*. New York: Berkeley, 1982.

Stoll, Clifford. *The Cuckoo's Egg*. New York: Doubleday, 1989.

Toffler, Alvin. *The Third Wave*. New York: William Morrow, 1985.

Toffler, Alvin. *Powershift*. New York: Bantam, 1990.

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

U.S. General Accounting Office. *Hackers Penetrate DOD Computer Systems*, testimony of Jack L. Brock before Senate Subcommittee on Government Information and Regulation, Committee of Governmental Affairs, GAO/T-IMTEC-92-5, 20 November 1991.

U.S. Congress. Senate. Committee on Governmental Affairs. *Vulnerability of Telecommunications and Energy Resources to Terrorism*. 101st Cong., 1st Sess., 7-8 February 1989.

U.S. Congress. House. Science, Space and Technology Committee. *Computer Security*. 101st Cong., 2nd Sess., 10 July 1990.

U.S. Congress, Office of Technology Assessment. *Technology Against Terrorism: Structuring Security*, OTA-ISC-511. Washington, D.C.: U.S. Government Printing Office, January 1992.

U.S. Congress. Senate. Committee on Governmental Affairs. *Vulnerability of the Nation's Electric System to Multi-Site Terrorist Attack*. 101st Cong., 2nd Sess., 28 June 1990.

Van Creveld, Martin. *Command in War*. Cambridge MA: Harvard University Press, 1985.

Van Creveld, Martin. *Technology and War*. New York: Free Press, 1989.

Van Creveld, Martin. *The Transformation of War*. New York: The Free Press, 1991.

Wardlaw, Grant. *Political Terrorism: Theory, Tactics, and Counter-measures*. New York: Cambridge University Press, 1982.

Wilkinson, Paul. *Terrorism and the Liberal State*. New York: NYU Press, 1986.

ARTICLES

Ager, Susan. "Byline." *Associated Press*, 17 March 1978.

Anthes, Gary. "Info-terrorist Threat Growing." *Computerworld*, 30 January 1995, 1.

Anthes, Gary. "Info Warfare Risk Growing." *Computerworld*, 22 May 1995, 1.

Arquilla, John, and Ronfeldt, David. "Cyberwar is Coming!" *Comparative Strategy*, 12 (1993): 141-165.

Arquilla, John. "The Strategic Implications of Information Dominance." *Strategic Review* (Summer 1994): 24-30.

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

Benesh, Peter. "Amateurs; Deadly New Menace." *Pittsburgh Post-Gazette*, 28 September 1995, A1.

Bloombecker, Buck. "Of Systems, Solidarity, and Struggle." *Datamation*, 1 November 1987, 47.

Bournellis, Cynthia. "Internet '95." *Internet World*, November 1995, 47.

Bowman, Stephen. "U.S. Still Ripe for Terror." *Denver Post*, 28 May 1995, A2.

Bowman, Stephen. "Lights out: Electrical Systems an Easy Target for Terrorists." *Denver Post*, 29 May 1995, A2.

Campbell, Douglas, E. "The Intelligent Threat." *Security Management*, March 1989, 19A.

Cetron, Marvin J. "The Growing Threat of Terrorism." *The Futurist* 23-4 (July 1989): 4.

Cetron, Mervin J. and Owen Davies. "The Future Face of Terrorism." *The Futurist* 28-6 (November 1994): 10.

Cooper, Pat. "In Cyberspace, U.S. Confronts and Illusive Foe." *Defense News*, 13 February 1995, 1.

Crabbe, Robert. "Mideast War: California Moves to Protect Big Dams." *United Press International*, 25 January 1991.

Diringer, Elliot. "Environmental Demonstrations Take Violent Turn." *San Francisco Chronicle*, 24 April 1990, A3.

Dowell, William. "French Terrorists Attract Outside Aid." *Christian Science Monitor*, 17 July 1980, 4.

Eddington, Mark. "Taking the Offensive; Against Terrorism." *The Atlantic* 269-6 (June 1992): 40.

Elliott, Ronald. "Information Security is Crucial." *Defense News*, 13 January 1992, 20.

Evers, Stacey, "IW Poses Infinite Questions, Few Answers." *Aerospace Daily*, 23 June 1995, 472.

Garner, Rochelle. "The Growing Professional Menace." *Open Computing*, July 1995, 32.

Gertz, Bill. "Spies on the Information Superhighway." *The Washington Times*, 17 Nov. 1994.

Graham, Rusty. "Storm, Bombing Work 1-2 Punch on Local ATMs." *Temple Daily Telegram*, 18 March 1993.

Grier, Peter. "Information Warfare." *Air Force Magazine*, March 1995, 34.

Hansell, Saul. "Citibank Fraud Case Raises Computer Security Questions." *New York Times*, 19 August 1995, 1-31.

Hoffman, Lance, Faraz Ali, Steven Heckler, Ann Huybrechts. "Cryptography Policy." *Communications of the ACM* 37-9 (September 1994): 109.

Holland, Kelley. "Bank Fraud, The Old-Fashioned Way." *Business Week*, 4 September 1995.

Keating, Stephen. "Global Intrigue on Info Highway." *Denver Post,* 24 April 1994, A1.

Knutson, Jeanne N. "The Terrorist's Dilemmas: Some Implicit Rules of the Game." *Terrorism: An International Journal,* 4 (1980): 195-222.

Lamb, John and James Etheridge. "DP: The Target of Terror." *Datamation*, 1 February 1986, 44.

Leach, Norman. "Terrorism in Your Own Backyard." *Security Management* 33-5 (May 1989): 56.

Madsen, Wayne. "Retired KGB Officers Refuse Comment on Russian Computer Espionage." *Computer Fraud and Security Bulletin,* January 1994.

Madsen, Wayne. "Intelligence Agency Threats to Computer Security." *International Journal of Intelligence and Counterintelligence* 6-4 (Winter 1993): 413-487.

Maney, Kevin and Robyn Meredith. "Risky Business on the Internet." *USA Today*, 20 September 1995, 1B.

Mannix, Margaret. "Can Hackers Break into Netscape?" *U.S. News and World Report*, 2 October 1995, 84.

Markoff, John. "Feared Computer Plague Passes With Very Few Infections." *New York Times*, 7 March 1992, 1-8.

Mason, John. "Banks' Security Chains Rattled." *Financial Times*, 20 September 1995, 20.

May, Matthew. "Super Snoopers or Plain Bad?" *Times* (London), 18 August 1995.

Moffett, George D. "High-tech Terrorism in the Future." *Christian Science Monitor*, 27 June 1986, 4.

Mokrzycki, Mike. "Battleground of Bits and Bytes." *Jerusalem Post*, 19 April 1995, 5.

Munro, Neil. "The Pentagon's New Nightmare: An Electronic Pearl Harbor." *Washington Post*, 16 July 1995, C3.

Ognibene, Peter J. "Perspective on Gulf Crisis; America, The Vulnerable." *Los Angeles Times*, 16 January 1991, B7.

Peterzell, Jay. "Spying and Sabotage by Computer." *Time* 20 March 1989, 25.

Radigan, Joseph. "Info Highway Robbers Try Cracking the Vault." *U.S. Banker*, May 1995, 67.

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

Richardson, Valerie. "Ecoterrorists put 92,000 Homes in Dark." *Washington Times*, 24 April 1990, A4.

Sakkas, Peter E. "Espionage and Sabotage in the Computer World." *International Journal of Intelligence and Counterintelligence* 5-2 (Spring 1992): 155-202.

Segal, Gerald. "Asians in Cyberia." *Washington Quarterly* 18-3 (Summer 1995): 3.

Sitomer, Curtis J. "Crooks find Computers Useful; Terrorist see Vulnerable Targets." *Christian Science Monitor*, 5 December 1986, 6.

Stern, Chester. "Chaos by Computer." *Mail on Sunday* (Associated Newspapers), 14 February 1993, 8.

Tomkins, Richard, "Techno-terror Makes Debut, Repeat Performances Likely." *Deutsche Presse-Agentur*, 24 March 1995.

Wade, Nicholas. "Method and Madness: Bytes Make Might." *New York Times*, 12 March 1995, 6-28.

Wald, Matthew. "The Nation; How Does the World Look Through the Eyes of Aspiring Terrorists?" *New York Times*, 6 March 1994, 4-3.

Wilder, Clinton. "Netscape Encryption Codes Cracked." *InformationWeek*, 2 October 1995, 32.

Wresch, William. "New Lifelines: The Internet in Africa." *Internet World*, November 1995. 102.

Zitner, Aaron. "Netscape Flaw Seen as Setback for Business." *Boston Globe*, 20 September 1995, 33.

"A War on French Computers." *Newsweek*, 28 April 1980, 56.

"France; Terror by Technology." *Economist*, 19 April 1980, 44.

"German Retailer Warns on Computer Virus." *Reuter European Business Report*, 10 August 1995.

"Police Say Radicals Used Radio Transmitters in Rail Sabotage." *Associated Press*, 1 December 1985, AM Cycle.

"Radical Guerrilla Assaults Stop JNR Train Runs." *Japan Economic Newswire*, 29 November 1985.

"Soviet Attaché Expelled as 'Computer Spy'." *Jane's Defence Weekly* 11-11(18 March 1989).

"Suspicions Surface About Bugged Swiss Encryption Units." *Computer Fraud and Security Bulletin,* October 1994.

"Techno-Terrorists Might Cripple Computerized Society." *Associated Press*, 11 April 1986.

"The Softwar Revolution; The Ties that Bind." *The Economist*, 10 June 1995, 18.

PROCEEDINGS

Kelchner, T. and Graham, K., eds. *InfoWarCon'95 Conference Proceedings, September 7-8, 1995*, by National Computer Security Association. Carlisle PA: National Computer Security Association, 1995.

THESES

Meyer, Gordon, R. "The Social Organization of the Computer Underground." M.A. Thesis, Northern Illinois University, 1989.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center 8725 John J. Kingman Rd., STE 0944 Ft. Belvoir, VA 22060-6218	2
2.	Library, Code 13 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Dr. Frank Teti Chairman, National Security Affairs (NS/Te) Naval Postgraduate School Monterey, CA 93943	1
4.	Professor Gordon H. McCormick (Code NS/Mc) Naval Postgraduate School Monterey, CA 93943-5000	1
5.	Professor John Arquilla (Code NS/Aq) Naval Postgraduate School Monterey, CA 93943-5000	5
6.	Professor James Wirtz (Code NS/Wz) Naval Postgraduate School Monterey, CA 93943-5000	5
7.	Professor Maria Moyano (Code NS/Mm) Naval Postgraduate School Monterey, CA 93943-5000	1
8.	Jennifer Duncan Center for the Study of Political Violence Naval Postgraduate School Monterey, CA 93943-5000	5

9. The Honorable Emmett Paige, Jr. 1
Assistant Secretary of Defense for C3I
The Pentagon, RM 3E172
Washington, DC 20301-6000

10. The Honorable H. Allen Holmes 1
Assistant Secretary of Defense for SO/LIC
The Pentagon, RM 2E258
Washington, DC 20301-2500

11. GEN Wayne A. Downing, USA 1
Commander in Chief
US Special Operations Command
MacDill AFB, FL 33608-6001

12. Commander, Naval Special Warfare Command 1
NAB Coronado
San Diego, CA 92155

13. Commander Naval Special Warfare Development Group 1
FCTCL Dam Neck
Virginia Beach, VA 23461-5200

14. Commander, Naval Special Warfare Group One 1
NAB Coronado
San Diego, CA 92155

15. Commander, Naval Special Warfare Group Two 1
NAB Little Creek
Norfolk, VA 23521

16. Commander 1
Naval Information Warfare Command
9800 Savage Road
Fort G. Meade, MD 20755-6000

17. Commander 1
Joint Special Operations Command
ATTN: J-3
P.O. Box 70239
Ft. Bragg, NC 28307-6001

18. Mr. Andrew Marshall — 1
Director of Net Assessment
OSD/NA
The Pentagon, RM 3A930
Washington, DC 20301

19. The JCS Staff — 1
J-3 Special Operations Division
Washington, DC 20318-3000

20. Strategic Studies Group (SSG) — 1
Naval War College
Newport, RI 02840

21. Library — 1
Naval War College
Newport, RI 02840

22. Library — 1
Air War College
Maxwell AFB, AL36112-6428

23. United States Special Operations Command — 1
Joint Special Operations Forces Institute
Fort Bragg, NC 28307-5000

24. Department of Military Strategy — 1
National War College (NWMS)
Ft. Leslie J. McNair
Washington, DC 20319-6111

25. US Army Command & General Staff College — 1
Concepts and Doctrine Directorate
ATTN: Mr. John B. Hunt
Ft. Leavenworth, KS 66027-6900

26. Harvard University — 1
JFK School of Government
Cambridge, MA 02138

27. US Army Center for Military History — 1
1099 14th St NW
Washington, DC 20005-3402

28. US Military Academy — 1
ATTN: Department of Military History
West Point, NY 10996

29. Marquat Memorial Library — 1
US Army John F Kennedy Special Warfare Center & School
Rm. C287, Bldg 3915
ATTN: Mr Fred Fuller
Ft Bragg, NC 28307-5000

30. Harvard University — 1
JFK School of Government
Cambridge, MA 02138

31. Hoover Institution for War, Revolution and Peace — 1
Palo Alto, CA 94306

32. Hurlburt Base Library — 1
16SVS/SVRL
ATTN: Susan Whitson
410 Cody Ave
Hurlburt Fld, FL 32544-5417

33. USASOC — 2
Directorate of History and Museums
ATTN: AOHS-Dr Stewart
Ft Bragg, NC 28307-5200

34. Defense and Arms Control Studies Program — 1
Massachusetts Institute of Technology
292 Main Street (E38-603)
Cambridge, MA 02139

35. RADM Preston A. Littleton, Jr., USPHS (Ret.) — 2
11907 Whistler Ct.
Potomac, MD 20854

36. Captain Richard O'Neill, USN — 1
ASD/C3I
The Pentagon, RM 3D200
Washington, DC 20301-6000

37. LCDR Dean Rich, USN — 1
Fleet Information Warfare Center
2555 Amphibious Dr.
Norfolk, VA 23521-3225

38. Major John Viehe — 1
U.S. Special Operations Command
ATTN: AOFI-ST
Fort Bragg, NC 28307-5200

39. Lt. Matthew J. Littleton, USN — 1
Navy/Marine Corps Intelligence Training Center-Dam Neck
2088 Regulus Avenue
Virginia Beach, VA 23461-2099

40. LT Matthew Knapp, USN — 1
Code 39
Naval Postgraduate School
Monterey, CA 93943-5000