STRATEGY RESEARCH PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

CYBER-TERRORISM: MODEM MAYHEM

BY

COLONEL KENNETH C. WHITE
United States Army

19980605 068

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

DTIC QUALITY INSPECTED 4

USAWC STRATEGY RESEARCH PROJECT

Cyber-Terrorism: Modem Mayhem

by

COL Kenneth C. White

Robert D. Johnson
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

ABSTRACT

AUTHOR: **Kenneth C. White (COL), USA**

TITLE: **Cyber-Terrorism: Modem Mayhem**

FORMAT: **Strategy Research Project**

DATE: **14 April 1998** PAGES: **38** CLASSIFICATION: **Unclassified**

America can no longer rely on broad oceans and a strong military to protect its homefront. The arrival of the information age has created a new menace--cyber-terrorism. This threat recognizes no boundaries, requires minimal resources to mount an attack, and leaves no human footprint at ground zero.

This study addresses technology, identification procedures, and legal ambiguity as major issues, for countering cyber-terrorism as an emerging challenge to U.S. national security. As America's reliance on computer technology increases, so does its vulnerability to cyber attacks.

TABLE OF CONTENTS

ABSTRACT iii

INTRODUCTION 1

BACKGROUND 4

EVOLUTION IN REVOLUTION 4

CHALLENGES 9

TECHNOLOGY 9

IDENTIFICATION 14

AMBIGUITY 17

RECOMMENDATIONS 21

CONCLUSION 23

ENDNOTES 25

BIBLIOGRAPHY 31

> U.S. vulnerability to [cyber-terrorism is] the major security challenge of this decade and possibly the next century.[1]
>
> — Joint Security Commission

For more than 200 years, America's homeland has enjoyed protection from attacks because of broad surrounding oceans and a strong military force. However, the arrival of the information age[2] has dramatically changed America's defense posture: How can we protect our recently developed critical information infrastructure? According to the Presidential Commission on Critical Infrastructure Protection, "as networked computers expand their control over the nation's energy, power, water, finance, communications, and emergency systems, the possibility of electronic attack and catastrophic terrorism becomes increasingly possible."[3]

Yearly, commercial businesses and government organizations lose valuable data, time, and money because computer systems are compromised. Annually, some 250,000 attempts to penetrate U.S. Department of Defense (DoD) computer systems are recorded. Sixty-five percent of these attempts are successful.[4] For example, in February 1998, as the U.S. was stepping up deployments of troops and equipment to the Persian Gulf, 11 U.S. military computer systems were comprised--seven Air Force systems, four Navy systems. Those compromised contained logistical, administrative, and pay records data. Such intrusions potentially cause widespread confusion and disruption

of military operations. They certainly call into question the integrity of security for our DoD computer systems. Investigating authorities have stated that recent breaches of military computers are the most organized and systematic attacks on U.S. defense networks to date. Sources of these attacks have not been identified.[5]

Other compromises of national critical infrastructure network components include an October 1997 compromise of the Pacific & Electric Company's network, which caused widespread power outages in San Francisco, California. Also switchboards in Florida were jammed intermittently for months in 1996, which prompted a global hunt for the attacker by the Federal Bureau of Investigations. Likewise, another high profile hacker (a person who attempts to penetrate security systems on remote computers as a challenge) intrusion occurred during the summer of 1995, when several military and university computer systems containing important and sensitive information about satellites, radiation and energy were compromised.[6] These cases involve hacker break-ins to computer systems, not cyber-terrorists attacks. However, hackers and cyber-terrorists differ only in their intentions: Hackers may be only criminally destructive adventurers, whereas cyber-terrorists are advanced enemies of a nation state.

"The information age promises an explosion in economic growth, technological innovation and educational opportunities that could improve the standard of living and quality of life

around the world."[7] However, an unintended consequence of information age triumphs is the creation of a new problem--cyber-terrorism. Barry Collins, an analyst for the Institute for Security and Intelligence, coined the term "cyber-terrorism" a decade ago. He identifies cyber-terrorism as "the intentional abuse of a digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action."[8] Current corporate and government practices to computerize more and more tasks and processes plays into the hands of the cyber-terrorist.

Documented evidence indicates several terrorist organizations have incorporated information age technology into their terroristic strategies. For example, the Italian Red Brigade's manifesto specifies attacking computer systems as an objective for striking a state's center of gravity. Law enforcement and intelligence officials say various terrorist organizations operating in the U.S. are making full use of technology to link their World Wide Web sites, to solicit funds, to transfer funds to anonymous off-shore bank accounts, and to stage attacks.

John Deutch, then Central Intelligence Agency Director, in testimony before Congress in June of 1996, warned that "the ability to launch an attack on the U.S. infrastructure via computer-generated terrorism, the ultimate precision-guided

weapon, is already in the hands of terrorist organizations".[9] Indeed, "modem mayhem[10]" is plausible.

This study addresses several issues that characterize cyber-terrorism as an emerging challenge to U.S. national security. The background establishes a frame of reference for understanding cyber-terrorism. Secondly, the challenges are analyzed in terms of major issues related to cyber-terrorism: technology, identification procedures, and legal ambiguity. This study concludes with recommendations for limiting vulnerabilities of critical U.S. infrastructure computer networks to cyber-terrorism.

BACKGROUND: Evolution in Revolution

> I am a computer revolutionary. If a revolutionary is a terrorist, then a computer revolutionary is a computer terrorist and therefore, I am a computer terrorist.[11]
>
> — Rop
> European Hacker

U.S. national security experts list terrorism as one of the top current menaces. However, terrorists have recently implemented new strategies utilizing information age tools. Given the minimal requirement of a personal computer, modem, telephone connection, and a few well placed key strokes to orchestrate an attack on a nation's electronic infrastructure, a new terrorist species has evolved, the cyber-terrorist. The cyber-terrorist practices cyber-terrorism, a new breed of terrorism.[12] Just as nations have exploited technology in their national interest, cyber-terrorists have also leveraged

technology in pursuit of exploiting the power of information tools in their interests.

Historically, the form of terrorism dominant during the Cold War was ideological terrorism, and could be categorized as either Marxist or nationalist. For example, the Italian-based Marxist Red Brigade, very active in the 1980s, seeks to create his own revolutionary state through armed struggle and to separate Italy from the Western Alliance. This group concentrated on assassination and kidnapping of Italian government officials and influential, private sector leaders. However, Americans were also targeted. U.S. Army Brigadier General James Dozier was kidnapped in 1981 and Leamon Hunt, U.S. Chief of the Sinai Multinational Force and Observer Group, was murdered in 1984 by the Red Brigade to protest U.S. and NATO forces presence in Italy, as well as their foreign policies.[13]

In the wake of the Cold War, ethno-religious and single-issue terrorism was most prevalent. Ethno-religious terrorism was responsible for the 1993 World Trade Center bombing in New York City by militant Islamic radicals who view the U.S. as the "Great Satan", an enemy of Islam that must be punished. The 1995 bombing of Oklahoma City's Alfred P. Murrah Federal Building was an example of single-issue terrorism. Prosecutors contend that the conspirators responsible for the bombing sought retaliation for the federal government's 1993 siege of and attack on the Branch Davidian compound at Waco, Texas. Some terrorist experts,

supported by their research, contend that single-issue terrorism has the potential to be the most prevalent terrorism form to occur domestically.

Some of the organizations, groups, and individuals who have shown an inclination to implement single-issue terrorism include radical environmentalists, pro-life movement extremists, animal rights extremists, separatist groups, millenium watchers, cultists, survivalists, neo-fascists, drug and other criminal cartels, as well as disgruntled employees. Representatives of all these groups reside and are active in the U.S.

Who or what do these terrorist groups target? The President's Commission on Critical Infrastructure Protection has identified eight critical U.S. infrastructures at risk: telecommunications; transportation (aviation, shipping, trucking and rail industries); electrical power systems; water supply systems; gas and oil storage and transportation; emergency services; banking and finance; and continuity of government services.[14] Not all of these systems are networked, but all are becoming so. Even systems in a "stand alone" mode are vulnerable to several kinds of attacks. One vulnerability can be exploited through a modem and social engineering. The terrorist pose as a new employee in need of assistance to access company computers in order to acquire data on internal security, passwords, and system configurations. Similarly, "Trusted Insiders" use their direct access to destroy or manipulate the data or computer networks

from within. Sometimes they insert a malicious code during outside service calls, contractor network upgrades, or through loading unsolicited software. Even software received anonymously in the mail may carry out such insidious disruption; it may indeed be innocently introduced to a targeted system.

What objectives cyber-terrorists achieve through such relatively easy intrusions? The cyber-terrorist has three potential objectives: destruction, alteration, or acquisition and retransmission of data/commands. Achievement of any of these objectives could have a potentially devastating impact on the intended target.

What are cyber-terrorists' weapons? Weapons of choice are electronic in nature. They require only time to create a list of instructions for the computer to follow and a few key strokes to deliver those instructions. Computer viruses are the oldest and best-known software weapons. They invade computer systems and reproduce themselves, destroying data and/or hardware. Most viruses use the hitchhiker approach to enter a computer system. Like biological viruses, the computer virus is silent and invisible; it does not show itself until the targeted system is already infected.[15]

Another weapon is the worm. "Worms are breeder programs, reproducing themselves endlessly to fill up memory and hard disks. Worms are often designed to send themselves throughout a network, making their spread active and deliberate."[16]

A third weapon is the logic bomb, which is difficult to locate. The logic bomb is a set of destructive instructions that detonate on a predetermined date. It may also detonate when a specific set of instructions is executed, causing damage within the computer or throughout a network.

Bots are a fourth weapon of the cyber-terrorist. The bot is derived from robot; it is code-designed to recon the Internet and carry out designated tasks. For instance, it may retrieve or destroy specified data. The SYN attack is a similar bot weapon. It floods a host server and causes a bottle-neck or traffic jam. Server access slows to a crawl or is disabled.

Finally, extortion can be used just as effectively as one of the weapons listed above. Recent reports indicate that banks have paid hackers upwards to six figures to prevent them from using the banks' compromised security codes. Also, in the past year, corporations have lost in excess of $800 million as a result of computer break-ins.[17]

The above list of cyber-terrorist weapons is by no means exhaustive. It is merely a representative sampling of tools in the hands of John Q. Cyber-Terrorist. A radical European computer hacker proclaimed, "You see, computers are to be used as a tool for the revolution. It is up to us to stir up the social system. It's not working. We have to make the waves."[18] As America's dependence on computers continues to flourish, John Q. Cyber-Terrorist no doubt looks at the U.S. as a target rich

environment. His new maxim may be, "So many new targets...so little time".[19]

CHALLENGES: TECHNOLOGY

> In the future, factories will have only two employees, a man and a dog. The man to feed the dog and the dog to keep the man away from the computers.[20]
>
> — Anonymous

Technology enables cyber-terrorists to maintain anonymity. "No airport checkpoints to pass through. No fingerprints left on the steering wheels or bomb fragments. No human presence at ground zero."[21]

Since information system knowledge doubles every twelve months and since this growth continues to accelerate, security procedures cannot keep pace with technology improvements. By the time the full impact or significance of a technological improvement is known, new advancements are already on the market.[22] As technology becomes more cost effective, cyber-terrorists become more technologically oriented in their tactics and strategies.

Technology has linked America's critical infrastructure systems together so tightly that an attack on any link could very well have cascading impacts, eventually affecting several or all systems. Unfortunately, the U.S. is the leading, worldwide consumer of digitization; the nation has become enthralled with the plethora of data available at the users' fingertips. Americans expect their computers to work all the time, exactly

when they want them to. If such expectations are not fulfilled, this dependence forces a virtual productivity shutdown.

Sophisticated cyber-terrorists recognize that a disruption of America's computer network will have cascading negative impacts. Frequent disruptions will initiate the desired effects of fear, panic, and a loss of confidence in the nation's leadership to prevent future disruptions. Imagine the havoc created if only a region of America's financial network was successfully attacked: No stock or credit card transactions, personal and corporate banking accounts deleted, and automatic telemachines being rendered inoperative. No doubt, mass hysteria would result. The most frightening aspect of the above scenario is that the tools and techniques for creating such havoc are readily available today. A few select commands to key power grids could cause a massive power outage for days, possibly for weeks--especially if the main computer, as well as the backup software, were corrupted as a result of a cyber attack.

Technological advances in hardware, software, and the Internet are enabling private citizens, businesses, government, and DoD to obtain sensitive data for legitimate purposes. But these advancements also assist cyber-terrorists in the conduct of illegitimate activities.[23] A cyber-terrorist's primary tools are the personal computer (PC), the modem, and a telecommunications line. Approximately every twelve months, the PC is enhanced by increased processing speed, increased CD ROM speed, increased

data storage capacity, improved reliability, improved mobility, and greater acceptance because of lower prices and ease of operation.

The second hardware tool is the modem. It is also enhanced on an ongoing basis to increase data transmission speed and reliability. These enhancements likewise enable the cyber-terrorist to transmit his destructive commands faster and more accurately.

The cyber-terrorist also has easy access to the telecommunication line. Recent improvements have removed old wiring, which carried only one call per strand. It has been replaced by fiber optic cable, which can carry thousands of communication exchanges on one line smaller than a human hair. The fiber optic cable facilitates telecommunications transmission of video, data, voice, word, and images which can be transmitted one at a time or simultaneously. Fiber optic cable also easily encrypts data for security purposes.[24] Although legitimate users enjoy the many advantages of fiber optic cable use, the same advantages also enhance the cyber-terrorist's capability to attack and disrupt systems.

With one or more of these accessible tools of terror, the cyber-terrorist is almost ready to launch an attack. All he lacks is a set of programming instructions, the software. Some of the hacker software programs now available are SATAN, an infiltration program designed to automatically scan networks for

documented security holes; PC Track, a program that tracks satellites orbiting the earth; and Virus Creation Lab, a combination of software codes that may be mixed and matched to create malicious virus programs.[25] Using this software, the cyber-terrorist, assisted by the PC, modem, and a telecommunications line, can rapidly access, destroy, alter, copy, or retransmit selected data.

He can also use the software advancement in cryptography, which is the science of code making and code breaking. Cryptography is no longer used primarily by the diplomatic and military establishments. Law-abiding private citizens, businesses, and government organizations are employing cryptography software to share information securely. Once again, cyber-terrorists now utilize cryptography software to carry-on illegal activities such as encrypting their message traffic from the prying eyes of law-enforcement agencies.[26]

Last but not least is the cyber-terrorist's ready access to the Internet. Some technical writers have proclaimed the Internet as the foundation for planetary connection and the ultimate pathway to democracy. However, like many powerful tools, the Internet can be abused. "The Internet, which was created in 1969 as a network for the U.S. Department of Defense, essentially is a network of networks (a large group of computers interlinked and capable of sharing information)."[27] The exponential growth of the Internet is based on its service to

commercial activities. Business uses of the Internet range from internal and external communications to advertising and selling products.[28]

Americans are increasingly using the Internet, both for business, and for recreational and educational purposes. The Internet has far transcended its original purpose of enabling scientists to share information and resources with their colleagues across long distances and to provide an assured means of communicating with selected governmental proponents in the event of a nuclear war.[29] Today it provides multiple points of entry into computer systems connected to it. As the Internet grows, so do vulnerabilities, because computer systems linked through the Internet are less and less physically isolated and controlled. Instead, connections are more indiscriminate, access is less monitored and controlled. The Internet today consists of layers of systems distributed across many other systems which utilize network and application software too complex for a single individual to understand completely.[30]

In summary, technology employed by cyber-terrorists is readily available and cost effective. Access to it requires no state sponsorship. Technology provides a comfortable degree of anonymity and offers a multitude of points of entry to attack America's critical infrastructure systems remotely. Misuse of technology will continue to place America's critical networks at risk because of the constant improvements in technological

capabilities and the cyber-terrorist's ability to quickly and relatively easily exploit these improvements.

IDENTIFICATION

Emerging technology has undoubtedly enhanced the cyber-terrorist's weapons arsenal. To compound the problem of countering cyber-terrorists, this technology has also diminished capabilities to identify perpetrators. As hardware (computers and modems) continues to shrink, cyber-terrorists' mobility increases. As the hardware's processing speed increases, the cyber-terrorists' on-line time to issue destructive commands or to communicate with compatriots likewise decreases, limiting defenders' chances of "catching them red-handed". As hardware prices fall, cyber-terrorists are ensured of ready access to state-of-the-art equipment. And as software enhancements are implemented, the cyber-terrorist's efficiency likewise increases. All told, computer systems security managers face a Herculean challenge to identify, with certainty, the cyber-terrorist.

Another technological innovation that hampers the identification of cyber-terrorists is the anonymous server. It sends message traffic through several electronic remailers. As the intruder's destructive signals traverse several anonymous servers located in far-flung parts of the world, their true origin is almost certainly masked.[31]

Likewise, the identification of state sponsored cyber-terrorism is definitely not a cut-and-dried proposition. The

distinction between legitimate rational states and rogue states is blurred. "If a government could choose between perpetrating an attack through its own organs or contracting out, most would take the latter option quite seriously."[32] Why? Nations can always use the deniability screen provided by technology to proclaim their innocence. Even if the perpetrators are caught, identifying them as agents of a particular government is hardly guaranteed. Cyber-terrorists neither wear uniforms nor require special equipment available through sponsorship, such as tanks, planes, or submarines that may be traced.

Responding to a cyber-terrorist attack is a risky endeavor, especially if the attacker has not been positively identified. An offensive response triggering a retaliatory strike requires clear and positive identity of the attackers. But many questions must be answered prior to retaliation: How should the U.S. respond, through the use of military force, diplomatic channels, federal law enforcement, or a combination of the above? What are the criteria for responding? Depending on the nature and extent of the attack, should the response be through an alliance with a coalition of other nations or as a unilateral action? If such questions are not addressed, surely the situation could escalate beyond cyberspace, that virtual world where humans and computers co-exist, to a full scale conventional war.

Last but certainly not least in the identification arena is the owner-operators' inability to discern when a system is under

attack. Only five percent of all victims know their networks are under attack. Of those who know of or suspect an attack, only two percent report it.[33] Unfortunately, owner-operators cannot distinguish an accidental outage or maintenance problem from a cyber-terrorist attack. The new breed of terrorists increasingly choose to remain anonymous after they have attacked, instead of identifying themselves as they have done in the past. The actual attack thus becomes an end unto itself according to several terrorism experts. Additionally, this lack of acknowledgement increases anxiety, tension, and uncertainty regarding follow-on attacks.

Given the low probability that a cyber-terrorist will be identified, thoroughly resourced attacks can be implemented at the time and place of the attackers' choosing. The President's Commission on Critical Infrastructure Protection concluded that cyber-terrorists are able to conceive, plan, and implement an attack with no detectable logistical preparations. "The target can be invisibly reconnoitered, the sequence of events clandestinely rehearsed, and an attack launched without revealing the identity of the intruder."[34]

AMBIGUITY

> Criminals [are] moving increasingly into cyberspace and without new laws, drug dealers, arms dealers, terrorists and spies will have immunity like no other.[35]
>
> — Louis Freeh
> FBI Director

In an era of global markets and global competition, the technologies to create, manipulate, manage, use, and protect critical infrastructure networks are of strategic importance to the U.S. However, the global information age challenges U.S. law and necessitates the creation of consistent multinational legal standards. How can the national security establishment better discern what is a politically motivated computer crime as opposed to a teenage computer prank? Criminal law has applied the so-called "rule of lenity" and imposed the burden of proof and persuasion on the prosecution. Thus, in order to impose criminal sanctions, laws protecting the informational infrastructure must clearly and unambiguously define which activities are permitted and which are proscribed.

Further, any doubts concerning the application of the law should be resolved in favor of the accused. If the law is too ambiguous to be assuredly applied or if it fails to define the nature of the proscribed conduct, the entire statutory scheme may be struck down as "void for vagueness."[36] The bottom line is that currently the prosecutor has the burden of proving beyond a reasonable doubt that the accused is guilty. Also, computer-related offenses without eyewitness testimony and physical

evidence pose a major problem for law enforcement authorities. All too frequently, they cannot gather sufficient evidence to support a conviction of known culprits.

In fact, we have no generally accepted definition of what constitutes a computer crime, wherein terrorism has only a small part. Although the term "cyber-terrorism" was coined a decade ago, there is no indication that the State Department has adapted a useful definition of the term. The State Department's Anti-terrorism unit narrowly defines terrorism as only politically-motivated physical attacks. Thus computer network attacks generally do not conform to their definition of terrorism.[37] Ego-driven intrusions into a system to erase files or stealing information with the sole intent to blackmail is nothing more than simple theft, fraud, or extortion. Such intrusions do not constitute an attack on the government.[38] However, Ambassador Philip C. Wilcox, Jr., the State Department's coordinator for counter-terrorism, did address cyber-terrorism in his remarks to the 15th Annual Government/Industry Conference on Terrorism, Political Instability, and International Crime on 28 February 1997 in Washington, D.C.

Since cyber-terrorism respects neither national borders nor legal constraints, the challenge of international cooperation and coordination of investigations, coupled with diverse, overlapping and sometimes contradictory computer crime laws, regulations and criminal procedures, makes enforcement of criminal statutes even

more difficult.[39] Understandably, sovereign nations are reluctant to release control over domestic issues or to allow foreign governments to impose laws on their citizens.

"It is commonplace to observe that states participate in international arrangements when it is in their best interest to do so, or when those arrangements can be molded to conform with states' perceived self-interests."[40] Governments around the world must acknowledge that their individual and collective self-interest lies in compatible legal procedures, workable international standards, and global cooperation.

Computer criminals are becoming increasingly sophisticated and knowledgeable. Some legal experts accordingly despair that cyberlaws (rules and regulations regarding behavior in the virtual computer world), like many other statutes "become obsolete as soon as they are passed with changes in behavior out stripping changes in the law."[41] Cyberlaw is currently only graduating from kindergarten. Lamentably, there is little consensus on how to proceed legislatively and judicially.[42]

A convincing argument can be made that it is in America's interest to take the lead in seeking global cooperation to establish compatible legal procedures and international standards. After all, America is the world's largest consumer of automation, even though it has only five percent of the world's population. The security of the nation's electronic infrastructure is too important for America not to seek more

protective measures. Some defense and intelligence officials warn, that "as the United States becomes more dependent on computerized information systems, and links between these networks grow, so does the vulnerability to an electronic assault that could paralyze the country."[43]

DoD must assume a significant role in addressing cyber-terrorist attacks. But this emerging role, like laws governing computer crime, is currently ambiguous and uncertain. Of concern in some quarters is DoD's lack of authority to provide guidance on securing America's infrastructure networks, although the transmission of the majority of DoD's unclassified data utilizes public-switched networks. In view of DoD's broad mission to maintain the leading edge in warfighting capability and its current and historical role in the deployment and use of computers and computer networks, it is reasonable to assume DoD will be a key player during the formulation and implementation of a strategy to address cyber-terrorism. DoD possesses unique technical expertise, equipment, and experiences that are ideally suited to confront threats to America's critical computer networks.

Since cyber-terrorism knows no national boundaries and does not have to present a passport at borders, it will continue to flourish. Cyber-terrorists can ply their destructive trade far from the scene of the attack. Cyber-terrorists can stay at home and remotely perpetrate their misdeeds. Without cutting-edge

standardized laws and international cooperation, cyber-terrorists remain mostly free to attack targets of their choice, when they choose. Until DoD's role in combating cyber-terrorism is defined, its potential assistance in defending critical infrastructure networks is limited.

RECOMMENDATIONS

> We should attend to our critical foundations before the storm arrives, not after: Waiting for disaster will prove as expensive as it is irresponsible.[44]
>
> — President's Commission on Critical Infrastructure Protection

Cyber-terrorism is constantly evolving. Effectively countering it requires adapting to a changing culture. Many procedures are available to challenge cyber-terrorism; however, network vulnerabilities cannot be eliminated through the use of any single procedure. In fact, all the holes will never be plugged because the challenge is dynamic and the cost of security is very high indeed. Although the federal government's budget for research and development of infrastructure protection is $250M annually, recommendations have been made to quadruple this figure over the next five years.[45] The following recommendations for public and private sector action are introduced as positive steps in limiting the cyber threat to America's critical infrastructure networks.

First, implement training programs in the public and private sectors to alert and inform users and operators of network vulnerabilities and procedures to reduce them. Prescribing a "PC

lite" diet to America would not be an effective action plan. However, a widespread educational program to increase awareness of the problem holds considerable promise.

Second, we should leverage technology to limit computer network vulnerabilities. Such technologies as encryption, clipper chip,[46] and biometrics[47] are front runners in this area. Although the commercial sector does not endorse the clipper chip due to potential law enforcement monitoring of commercial dealings, such issues must be re-addressed so that necessary compromises lead to effective actions. The clipper chip encryption device should be designated as standard protection against network security breaches in both the commercial and government sectors. The degree of privacy that may be lost is miniscule compared to the degree of havoc that can be wreaked upon the nation's critical computer networks, to say nothing of the second and third order effects to follow. The U.S. should also take the lead in standardizing commercial encryption tools used internationally.

Third, rewrite and continuously update legislation to ensure it is unambiguous regarding what constitutes a computer crime. Agreements must be implemented to clarify legal proceedings within the U.S. and internationally. Laws, however, must be expansive enough to deter unlawful activities, but narrow enough to recognize the many legitimate uses of computers and computer networks.

Finally, we should create a coalition between private and public sector participants. Responsibility for the protection of the nation's critical computer networks crosses public and private sector boundaries. The coalition must clearly delineate the roles and missions of combatants of cyber-terrorism. From a military perspective, DoD's role in combating cyber-terrorism must be clearly specified to take full advantage of the unique skills and experiences that DoD possesses.

CONCLUSION

> Tomorrow's terrorists may be able to do more damage with a keyboard than with a bomb.[48]
>
> — National Research Council

In the past, America's homefront has been protected by large surrounding oceans and a strong military. However, the importance of those oceans and of military force has been decreased, thanks to wholesale acceptance of information age innovations. America's national security is currently challenged by a new menace, cyber-terrorism. Documented evidence, such as the Italian Red Brigade's manifesto, reveals that cyber-terrorism has been incorporated into some terrorists' campaign strategy. Unfortunately, the tools to orchestrate a computer-generated attack on critical U.S. infrastructure networks are readily available today.

Cyber-terrorists have leveraged technology to exploit the power of information age tools to the maximum extent possible. They have demonstrated their capabilities to use advanced

technology, to travel and communicate undetected, and to circumvent the letter and spirit of the law. Computer networks that control the nation's critical infrastructure systems have already been infiltrated on many occasions, at many different sites.

Cyber-terrorism is dynamic. But its impact can be lessened through vigilance, cooperation, and a clear delineation of roles and missions for business, government, and DoD to combat cyber attacks. Although a devastating computer network attack has not yet occurred, known compromises of U.S. computer systems should serve as a warning sign of impending danger. As Senator Richard Lugar of Indiana observed, "People don't understand the enormity of the national security threats out there; we need to be vigilant. This is not a time to go to sleep at the switch."[49] Now is the time to establish procedures to address the emerging challenge of modem mayhem to national security.

Word Count=5,231

ENDNOTES

[1] Joint Security Commission, "Technology Report on Cyber-terrorism," 1994 p.1; available from: <http://www.mvhs.srusd.k12.ca.us/~kwade/techreport.html>; Internet; accessed 28 March 1998.

[2] Information Age - An era of a globally, computer interconnected society where information and economic value are nearly synonymous. Winn Schwartau. Information Warfare, (New York: Thunder's Mouth Press, 1996), 28.

[3] David Phinney, "Electronic Plan of Attack." 20 Oct 1997, p. 1. available from: <http://www.abcnews.aol.com/sections/us/cyberterror1020/index.html>; Internet; accessed 28 March 1998.

[4] Reid Kanaley, from the article "Analyst Finds U.S. Treasury, Military Computers Vulnerable to Infowar," available from: <wysiwyg://184/http://www.infowar.com/civil_de/civil_i.html-ssi>; Internet; accessed 27 March 1998.

[5] Bradley Graham, "11 U.S. Military Computer Systems Breached by Hackers This Month," 26 Feb 98, p. 1, available from: <http://www.infowar.com/hacker/hack 030498a j.html-ssi>; Internet; accessed 16 November 1997.

[6] "Cyber Threats," available from: <http://www.infowar.com/hackers/hack.html>; Internet; accessed 26 March 1998.

[7] "Perspectives on Security in the Info Age," which outlines breaches of confidentiality, disruption of operations, and destruction of cyber property. Available from: <http://www.cspp.org/reports/report1-96.html>; Internet; accessed 16 November 1997.

[8] Matthew G. Devost, Brian K. Houghton, Neal A. Pollard, "Information Terrorism: Can You Trust Your Toaster,"available from: <http://www.terrorism.com/terrorism/itpaper.html>; Internet; accessed 16 November 1997.

[9] "New Security Threats Rest in Cyber Terrorism", 3 Feb 1997, available from: <http://www.infowar.com/civil_de/civil_c.html-ssi>; Internet; accessed 16 November 1997.

[10] Modem (Modulate - Demodulate): "A form of computer hardware that allows a computer to communicate with other computers…through telephone lines". Garry S. Howard, Introduction to Internet Security from Basics to Beyond, (Rocklin, CA: Prima Publishing, 1995), 354.

[11] Schwartau, p.357.

[12] Terrorism is "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." Douglas Platzer, "The Future of Terrorism," March 1997. Available from: <http://www.terrorism.com /terrorism>; Internet; accessed 29 November 1997.

[13] George Goncalves, "Terrorist Group Profiles: Red Brigade," Last Update, 2 Mar 97. Available from: <http://www.milnet.com/ milnet/tgp/data/br.htm>; Internet; accessed 27 March 1998.

[14] Summary of the President's Commission on Critical Infrastructure Protection Survey conducted in 1996. The results will be used to "develop recommendations for research and development programs to address technology shortfalls and formulate critical infrastructure protection strategies." Available from: The Texas Transportation Institute's Information and Technology Exchange Center, <http://www.tti.tamu.edu/pccip>; Internet; accessed 29 November 1997.

[15] Schwartau, p. 156.

[16] "Net Apocalypse! - War: Cyber-terrorism," CNET, available from: <http://zeppo.cnet.com/Content/features/Dlife/apocalypse / ss02a.html>; Internet; accessed 12 February 1998.

[17] Ibid.

[18] Schwartau, p. 356.

[19] Sloan, p.4.

[20] Anonymous

[21] "Apocalypse Explained," CNET, 1997, available from: <http://zeppo.cnet.com/content/features/dlife/apocalypse/ss02a.ht ml>; Internet; accessed 9 October 1997.

[22] James W. McLennan, "Battlefield of the Future." available from: <http://www.cdsar.af.mil/battle/chp7.html>; Internet; accessed 29 November 1997.

[23] Richard L. Field, "Electronic Banking: Banking Has Important Stake in Unfolding Cryptography Regulations." available from: <http://www.ctr.columbia.edu/vii/crypto/rlf2.htm>; Internet; accessed 29 November 1997.

[24] Kornel Terplan, Communication Networks Management, (Englewood Cliffs, NJ: Prentice Hall, 1992), 52.

[25] "Technology Report on Cyberterrorism," p.3, see endnote 1.

[26] Michael Alexander, Net Security: Your Digital Doberman (NC: Ventana Communications, 1997),73.

[27] Elizabeth Panska, PC Novice Guide to the Web, (Lincoln, NE: Peed Corporation, 1996),6.

[28] William Stallings, Internet Security Handbook, (Westport, CT: IDG Books Worldwide, 1995),185.

[29] Ibid.

[30] Kent Anderson, "Criminal threats to Business on the Internet," 23 Jun 97, p. 2; available from: <http://www.aranet.com/~kea/papers/white paper.shtml>; Internet; accessed 5 January 1998.

[31] Jean Guisnel, Cyberwars: Espionage on the Internet, (New York, NY: Plenum Trade, 1997), 132.

[32] Ibid., p.50.

[33] Ibid., p. 24.

[34] "The President's Commission on Critical Infrastructure Protection, Report Summary," Oct 97; available from: <http://www.pccip.gov/sumarry.html>; Internet; accessed 20 November 1997.

[35] REUTERS, "FBI Chief Calls for Computer Crime Crackdown," 28 Oct 97; available from: <wysiwyg://65/http://www.infowar.com/class_2103097b.html-ssi>; Internet; accessed 20 November 1997.

[36] Mark D Rasch, "Criminal Law and the Internet," in The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues, (The Computer Law Association, 1996), 1.

[37] Richard W. Aldrich, "The International Legal Implications of Information Warfare," Apr 96, available from: <http://www.usafa.af.mil/inss/ocp9.htm>; Internet; accessed 5 January 1998.

[38] Matthew G. Devost, Brian K. Houghton, Neal A. Pollard, "Information Terrorism: Political Violence in the Information Age," available from: <http://www.terrorism.com/denning.html>; Internet; accessed 11 January 1998.

[39] Rash, p. 1.

[40] Fred H. Cate, "Global Information Policymaking and Domestic Law," available from: <http://www.law.indiana.edu/glsj/vol1/cate.html>; Internet; accessed 11 January 1998.

[41] Rash, p. 1.

[42] Stallings, William, p. xxi.

[43] Graham, Bradley, p. 1.

[44] "The President's Commission on Critical Infrastructure Protection," Oct 97, available from: <http://www.pccip.gov/sumarry.html>; Internet; accessed 20 January 1998.

[45] Ibid., p. 89.

[46] Clipper Chip is a hardware product of the National Security Agency. It is a computer chip that encodes voice and data communications (i.e. telephones, fax machines, and modems). The difference in clipper chip and other encryption devices "is that the chip has a trap door that [law enforcement, with a search warrant] can open to wiretap clipper equipped devices." Stallings, p. 213.

[47] Biometrics is a type of authentication using fingerprints, voiceprints, palm prints, retinal scans, and other physical/biological signatures of an individual. Howard, Garry S., Introduction to Internet Security from Basics to Beyond. Rocklin, CA: Prima Publishing, 1995, p.125.

[48] Statement by the National Research Council on computer security, "Computers at Risk: Safe Computing in the Information Age," (National Academy Press, 1991), 7.

[49] "National Nightmares," available from: <http://www.infowar.com/class 3/class3 081897.html>; Internet; accessed 4 December 1997.

BIBLIOGRAPHY

Aldrich, Richard W., "The International Legal Implications of Information Warfare," Apr 96. Available from <http://www.usafa.af.mil/inss/ocp9.htm>. Internet. Accessed 5 January 1998.

Alexander, Michael. Net Security: Your Digital Doberman. NC: Ventana Communications, 1997, p. 73.

Anderson, Kent, "Criminal Threats to Business on the Internet," 23 Jun 97, p. 2. Available from <http://www.aranet.com/~kea/papers/whitepaper.shtml>. Internet. Accessed 5 January 1998.

"Apocalypse Explained," CNET, 1997. Available from <http://zeppo.cnet.com/Content/features/Dlife/apocalypse/ss02a.html>. Internet. Accessed 9 October 1997.

Basken, Paul, "Wide Effort Urged to Protect Computers," 9 Oct 97, Washington, D.C. Available from <http://www.infowar.com/civil De/civil 101397.html-ssi>. Internet. Accessed 12 December 1997.

"Cyber Threats." Available from <http://www.infowar.com/hackers/hack.html>. Internet. Accessed 26 march 1998.

Devost, Matthew G., Houghton, Brian K., Pollard, Neal A., members of The Terrorism Research Center. From the article "Information Terrorism: Can You Trust Your Toaster." Available from <http://www.terrorism.com/Terrorism/itpaper.html>. Internet. Accessed 16 November 1997.

Devost, Matthew G., Houghton, Brian K., Pollard, Neal A., "Information Terrorism: Political Violence in the Information Age." Available from <http://www.terrorism.Com/denning.html>. Internet. Accessed 11 January 1998.

From e-mail message entitled, "A Quote for the Ages," 4 September 1997. Available from <wysiwyg://125/http://www.infowar.com/hacker/hack_090897.html-ssi>. Internet. Accessed 23 November 1997.

Field, Richard L. "Electronic Banking: Banking Has Important Stake in Unfolding Cryptography Regulations."

Available from <http:www.ctr.columbia.edu/vii/crypto/Rlf2.htm>. Internet. Accessed 12 December 1997.

Goncalves, George, "Terrorist Group Profiles: Red Brigade," Last Update, 2 Mar 97. Available from <http://www.milnet com/milnet/tgp/data/br.htm>. Internet. Accessed 27 March 1998.

Howard, Garry S. Introduction to Internet Security From Basics to Beyond. Rocklin, CA: Prima Publishing, 1995, p. 249.

Joint Security Commission, "Technology Report on Cyber-terrorism." 1994 p.1. Available from <http://www.mvhs .srusd.k12.ca.us/~kwade/techreport.html>. Internet. Accessed 11 January 1998.

Kanaley, Reid, from the article "Analyst Finds U.S. Treasury, Military Computers Vulnerable to Infowar." Available from <wysiwyg://184/http://www.infowar.com/Civil_de/civil_i.html-ssi>. Internet. Accessed 27 March 1998.

McLennan, James W. "Battlefield of the Future." Available From <http://www.cdsar.af.mil/battle/chp7.html>. Internet. Accessed 16 November 1998.

Howard, Garry S., Introduction to Internet Security from Basics to Beyond. Rocklin, CA: Prima Publishing, 1995, p.354.

"National Nightmares." Available from <http://www.infowar .com/class_3/class3_081897.html>. Internet. Accessed 12 December 1997.

"New Security Threats Rest in Cyber Terrorism," 3 Feb 1997. Available from <http://www.infowar.com/civil_de/civil_c.html-ssi>. Internet. Accessed 18 December 1997.

Panska, Elizabeth. PC Novice Guide to the Web. Lincoln, NE: Peed Corporation, 1996, p. 6.

Phinney, David, "Electronic Plan of Attack." 20 Oct 1997, p.1. Available from <http://www.abcnews.aol.com/sections

/us/cyberterror1020/index.html>. Internet. Accessed 28 March 1998.

Platzer, Douglas. "The Future of Terrorism," March 1997. Available from <http://www.terrorism.com/terrorism>. Internet. Accessed 20 January 1998.

"The President's Commission on Critical Infrastructure Protection, Report Summary." Oct 97. Available from <http://www.pccip.gov/sumarry.html>. Internet. Accessed 20 November 1997.

Rasch, Mark D. The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues, Chapter 11, "Criminal Law and the Internet." The Computer Law Association, 1996, p.1.

REUTERS, "FBI Chief Calls for Computer Crime Crackdown." 28 Oct 97. Available from <wysiwyg://65/http://www.infowar.com/class_2103097b.html-ssi>. Internet. Accessed 20 November 1997.

Sloan, Steven. "Terrorism: How Vulnerable is the United States." Paper. "Terrorism: National Security Policy and the Home Front, edited by Stephen Pelletiere. The Strategic Studies Institute, U.S. Army War College, May 1995. Available from <http://www.terrorism.com/terrorism/sloan.html>. Accessed 20 November 1997.

Stallings, William. Internet Security Handbook. Westport, CT: IDG Books Worldwide, 1995, p.