AIR WAR COLLEGE

AIR UNIVERSITY

ANATOMY OF CYBERTERRORISM: IS AMERICA VULNERABLE?

by

Bradley K. Ashley, Lt Col, USAF
Seminar 10

A Research Paper Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Col Kent Williams

Maxwell AFB, AL

27 February 2003

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
27 FEB 2003	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Anatomy of Cyberterrorism: Is America Vulnerable?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University Press Maxwell AFB, AL 36112-6615**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**45**	

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U. S. government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

List of Illustrations

Page

Abstract

The United States is vulnerable to attacks from cyberterrorists. A "Digital World Trade Center Attack", possibly killing thousands and causing billions of dollars in damage. This paper will provide fundamental background information on what cyberterror is and what it means. It also presents a model to understand the anatomy of cyberterrorism, describing some real-world cyber events, assesses cyberterrorist capabilities, and finally makes specific recommendations for improvement in cyber security.

This paper begins with a chilling scenario of cyberterror illustrating many aspects of potential future actions. The scenario is based 100% on real-world events that occurred within the past few years. The cyberterrorism model describes the anatomy of cyberterror and its components. It is a descriptive model and not a prescriptive model. In order to fully understand cyberterror, one must first understand the cyberspace environment and its unique attributes. Then by analyzing the various components of the cyberterror anatomy, we can grasp the answers to basic questions: who, what how, where, why, and when. Only after one understands these basic pillars, can one fully understand the whole of cyberterrorism.

The events of 9/11 caught us by surprise. We were unprepared and we now must broaden our expanded defense to include the cyber threat. Unless we take the appropriate steps to protect ourselves against cyber attacks now, America will surely suffer tragic cyberterrorist attacks that will have devastating impacts on our economy and will include loss of life.

Chapter 1

Introduction

There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things.

—Machiavelli

Scenario

The global media is buzzing with reports of American military systems under relentless electronic assault from computers in the Middle East. The latest media buzz term is "cyberterrorist". An unknown adversary controls logistics, transportation, administration, and accounting systems essential to deploying troops just as troops begin to flow to the Persian Gulf to enforce Iraqi compliance with United Nations inspections. The Department of Defense (DoD) debates the pros and cons of removing all its Internet connections. Many of America's largest commercial websites are flooded with connection requests rendering them inoperative and paralyzing significant portions of the Internet. Deadly viruses begin to infect computers and data around the globe including many military systems. Both government and private sector networks are destroyed. Over 60 million computers are affected costing billions of dollars in lost productivity, cleaning costs, and network/data restoration.[1] The timing of the cyber attacks is so

accurate, the attacks are interpreted as a first wave of subsequent attacks by a hostile nation or group.

Websites spring up like weeds calling for an electronic war and providing training on nuclear, chemical, biological, cyber attacks, and explosives. People around the globe are invited to join in electronic attacks simply by clicking on a website button to begin a flooding campaign. Osama bin Laden calls for a cyber Jihad on an Afghanistan hosted website. Computers at American infrastructure sites like airports and dams are infiltrated. Over one million liters of raw sewage are released into rivers and coastal waters. Agents tied to Al Qaeda buy useful information to penetrate Department of Defense computer networks. Power grids in California are infiltrated and held captive for weeks. Vigilante American hackers strike back at government computers of several suspected countries in the Middle East who may have initiated the original attacks. Cyber security experts testify before Congress that there is a high probability of further cyberterror attacks. The stock market is closed early due to computer problems after a record setting one week loss. Americans are alarmed at the devastation, cost, and results of these cyber attacks coming on the heels of the World Trade Center tragedy. The competitive media help spread the panic throughout the nation.

Does this scenario sound like science fiction? Is this a realistic scenario or panic filled rhetoric and hype? I assure you that it is 100% plausible because each one of the events described above has already occurred. Fortunately for us, these events took place at different times over the past several years. But could they happen in an orchestrated fashion in a short timeframe in the future?

This paper provides some fundamental background information on cyberterror, presents a model to understand the anatomy of cyberterrorism, describes some real-world cyber events, assesses cyberterrorist capabilities, and makes some recommendations. The United States is vulnerable to attacks from cyberterrorists today. A digital equivalent to the World Trade Center attack is quite plausible. The results could be the deaths of hundreds or thousands and could cost us billions of dollars.

Notes

[1] "National Strategy to Secure Cyberspace", draft, September 2002

Chapter 2

Background

All warfare is based on deception…know your enemy and know yourself and you can fight a hundred battles without disaster.

—Sun Tzu

Definitions of Basic Terms

Information Operations

The process of attacking and defending information is Information Operations (IO). The DoD defines Information Operations as "action taken to affect adversary information and information systems while defending one's own information and information systems."[2,3] This definition communicates that there is more to IO than simply attacking computer systems. IO consists of technology, processes, and human factors impacting the mind of the decision maker. IO can be targeted against leaders or key decision makers, but can also affect every echelon of the military, government, industry, and even the general population.

Defensive Information Operations "ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes."[4] Defensive IO are conducted through Information Assurance (IA), Operational Security (OPSEC), physical security, counter

deception, counter psychological operations, counter intelligence, electronic warfare, and special information operations.[5] IA is vital because of the continuing technological advances in systems (particularly in the speed, processing power, and miniaturization of computers) that advance the ongoing information revolution.

Information Assurance

Information Assurance is defined as "information operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."[6] The Information Assurance process ensures that: authorized users have guaranteed access to appropriate friendly information systems (availability;) friendly information systems are protected from unauthorized change or tampering (integrity;) authorized users are verified (authentication;) the information within the system is protected from unauthorized disclosure (confidentiality;) and friendly information systems provide an undeniable record of proof of user participation and transactions (non-repudiation.) Any information system or process that lacks any of the above information assurance components is vulnerable to adversary disruption or exploitation and must be considered unreliable.

Computer Network Attack

Computer Network Attack (CNA) are operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic Attack (EA) can be used against a computer, but it is not

CNA. CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA.[7]

Terrorism

The National Strategy for Homeland Security defines terrorism as any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments.[8] Terrorism is the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.[9]

Cyberterror

Cyberterror is a relatively new term. The Federal Bureau of Investigation (FBI) defines cyberterror as "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…through the exploitation of systems deployed by the target."[10] Interestingly enough, there is no DoD definition for cyberterror or information terror - yet.[11]

Infrastructure

Infrastructure covers a wide variety of systems from oil, rail, highway, banking, telecommunications, and emergency services, to the Internet. The DoD infrastructure

consists of over 2.1 million computers, 10,000 local area networks, and 1000 long distance networks. Over 95% of DoD's systems utilize public communications networks available to the general public. These networks are categorized as the global, national, and defense information infrastructures (GII, NII, and DII). Although these names imply independence, they all use interconnected transport medium linked to public switches that route data between geographically separated systems. The multitude of automated systems allows DoD to command, control, protect, pay, supply, and inform the force. As dependence on increasingly interconnected information systems grows, so do DoD vulnerabilities.

Notes

[2] DoD Directive 3600.1, "Information Operations", December 9, 1996.

[3] "DoD Dictionary" at http://www.dtic.mil/doctrine/jel/doddict/data/i/02581.html, October 22, 2002.

[4] Draft Joint Publication 3-13, "Joint Doctrine for Information Operations", January 28, 1998.

[5] CJCS Instruction 6510.01B, "Defensive Information Operations Implementation", June 30, 1997.

[6] Ibid.

[7] "DoD Dictionary" at http://www.dtic.mil/doctrine/jel/doddict/data/c/01168.html, October 22, 2002.

[8] "National Strategy for Homeland Security", White House, Office of Homeland Security, July 2002.

[9] "DoD Dictionary" at http://www.dtic.mil/doctrine/jel/doddict/data/t/05290.html, October 22, 2002.

[10] "Overview of Cyber-Terrorism," at www.cybercrimes.net/Terrorism/overview/page1.html, September 21, 2002.

[11] "DoD Dictionary" at http://www.dtic.mil/doctrine/jel/doddict/index.html, October 22, 2002.

Chapter 3

Ashley's Cyberterrorism Model

First I shall proceed from the simple to the complex. But in war more than in any other subject we must begin by looking at the nature of the whole; for here more than elsewhere the part and the whole must always be thought of together.

—Carl von Clausewitz

Figure 1. Ashley's Cyberterrorism Model

My model describes the anatomy of cyberterrorism. It is descriptive and should not be confused as a prescriptive model. In order to fully understand cyberterror, one must first understand the cyberspace environment and its unique attributes. Then by analyzing the various components of the cyberterror anatomy, we can grasp the answers to basic questions: who, what how, where, why, and when. Only after one understands these basic pillars, can one fully understand the whole of cyberterrorism.

Cyberspace Environment

Cyberspace is a very unique environment. It is ageographic (borderless), anonymous, asymmetric, and can be clandestine. It has virtually unlimited range and speed. Massive results can be achieved without "mass". It is fast, easy, and relatively inexpensive. Many regional conflicts have cyber dimensions where battles are fought by hackers on both sides with their own rules of engagement. We saw this in Bosnia, Kosovo, Kashmir, and the Middle East conflict. "Cyberspace security is an international challenge that is not bounded by any physical national boundary. The operations of multiple sectors cross international boundaries."[12]

Cyberterror Actors – Who?

The diversity of information operation adversaries ranges from individuals to nation-states. Their motivations include innocent curiosity, challenge, bravado, revenge, embarrassment, greed, idealistic activism, and national security interests. Adversaries of the United States are conducting information operations against us daily. Hackers are probing while well-organized and resourced foreign intelligence collection efforts are

performing an intelligence preparation of the cyber battlefield to gain unauthorized knowledge and access to DoD systems.

There are many actors in cyberspace that may resort to cyberterror: state sponsored, non-state supported, sub-state actors, hackers, and insiders.

State Supported

Several nations openly engage in defensive and even offensive information operations. These activities include: doctrine, education, training, organizations, resources, labs, and personnel.

Non-State Supported

Many nations are suspected of having information operations programs but do not reveal their capabilities. Institutions and organizations within the state could also conduct cyberterror.

Sub-State Actor

Terrorist groups, religious groups and political parties fit into this category. This group, along with hackers, has the highest probability of using cyberterror tactics. Subnational groups or terrorist organizations with political agendas not aligned with U.S. interests pose a more persistent threat than all but nation-state supported intruders. They may cheaply and anonymously gather information to embarrass or target DoD vulnerabilities.

Hacker

Virus writers, worm developers, and hackers fit into this category.

Insiders

An internal threat from disaffected employees with authorized access to information systems comprises another large pool of potential information adversaries. The damage such individuals are capable of today is exponentially higher than was possible before reliance on computerized information systems. Forty-four percent of respondents to the 1998 FBI Computer Crime and Security Survey reported unauthorized access by employees. This figure exceeded all other reported intrusions and continues to be DoD's number one threat.[13] Also, insiders are prime candidates to be "hired" by potential adversaries. Insiders that are sympathetic to the causes of the terrorist group make excellent potential recruits.

The typical "innocent juvenile hacker" who intrudes on systems for sport is nonetheless a potential threat to national security. The danger in attributing most detected intrusions to harmless hackers is to minimize the seriousness of the potential consequences. Hackers often use their age or status as a screen when, in fact, they may be "coached", persuaded or even hired for financial gain by anonymous agents that have more sinister motives. Computer vandals are more destructive and their motivations are simply to break into computers to wreak havoc and cause damage.

Tools and Techniques - What?

It Is Getting Easier

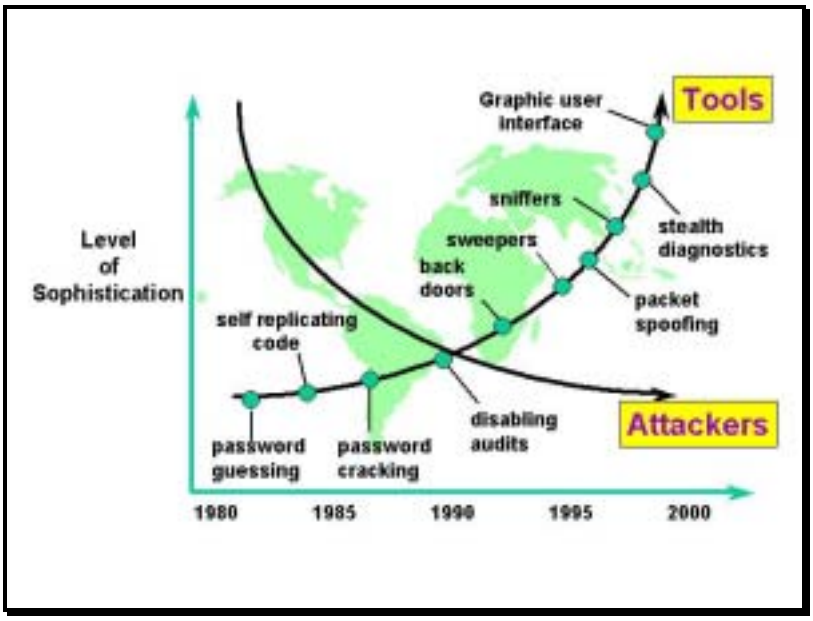

Figure 2. Level of Sophistication Over Time

Over time, the level of sophistication required to hack into an information system has dramatically decreased. At the same time, the quality, quantity, and availability of hacking tools has dramatically increased. This creates an environment where teenagers successfully infiltrate DoD and U. S. government systems. This creates a very dangerous target-rich and low-risk combination. Statistics show cyber attacks are on a dramatic rise.

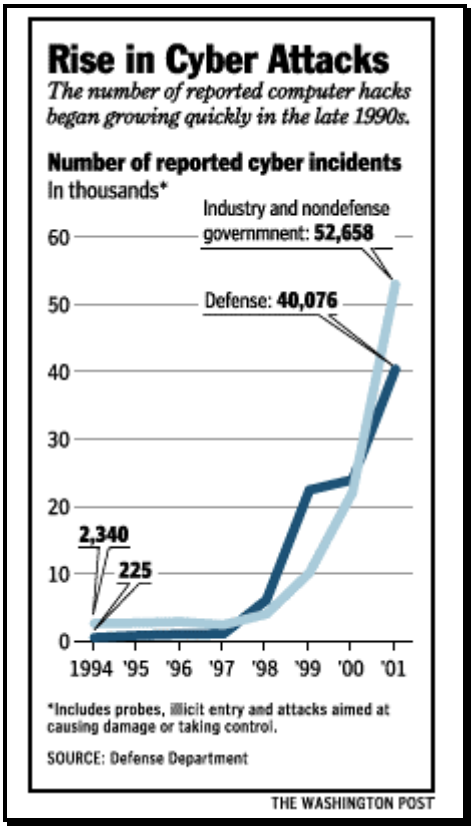

Figure 3. Cyber Attacks on the Rise[14]

Cyber warrior weapons are often readily available for download on the Internet. Unlike the tools of conventional warfare, the tools of this trade require no long term acquisition, training, and fielding process to mount an attack. As the typical PC has become more powerful and easier to use, so has the sophistication of the weapons that information adversaries have at their disposal. A comparatively low technology adversary with minimal funding, training, manning, and defense infrastructure is capable of employing these weapons on short notice from anywhere in the world. One key advantage afforded the information warrior is freedom from the burden of time and money needed to field and project a conventional force.

One common method to gain unauthorized access is through the normal log-on process from the command line prompt of a telnet or remote login session. User names and passwords may be gleaned from any number of methods. Free password cracking software is available on the Internet for anyone wishing to test the security of (or break into) networked systems. Once logged onto a system as a valid user an attacker may read, copy, delete, substitute, and modify data and programs on the host. Other computer vulnerabilities are easily found on the Internet to include corresponding exploitation tools.

Given access to a target system, the cyber warrior may inject, load, or install a program or script on the machine. Such programs may reside on the machine indefinitely if undetected, quietly gathering key information such as user names and passwords. They may provide backdoors to the systems for later entry at a time of the attacker's choosing. Trojan horse programs are seemingly legitimate operating system utilities or programs substituted by attackers for the real programs. Users run trojan horses believing they are real programs deriving expected results while unknown to them, additional malicious or destructive code executed in the background of the expected process is performing unintended tasks without user knowledge.

Toolkits are neatly bundled packages containing many of the above mentioned tools. They commonly incorporate easy to learn graphical (point and click) user interfaces. The danger of the proliferation of such tools is in the increased amount of damage a single attacker or organized group of attackers may inflict. These tools also provide the attacker anonymity and hinder trace actions.

Why are attacks on the rise? Several factors go into this equation: the growth of the internet raises the number of both attackers and targets, vulnerabilities of new software version releases continue to grow, and sophisticated hacking tools are readily available.

There are countless actions an intruder could take after gaining access to an information system. However, these acts can be summarized into four general categories: (1) modification, (2) fabrication, (3) interception, and (4) interruption.

Modification

Modifying data is also known as "spoofing". Unauthorized users who gain access to data can add, modify, or delete data. If done properly, this method can go unnoticed for a long period of time. Imagine the havoc caused simply be replacing all the "1s" with "7s" in an Air Tasking Order or Deployment Order.

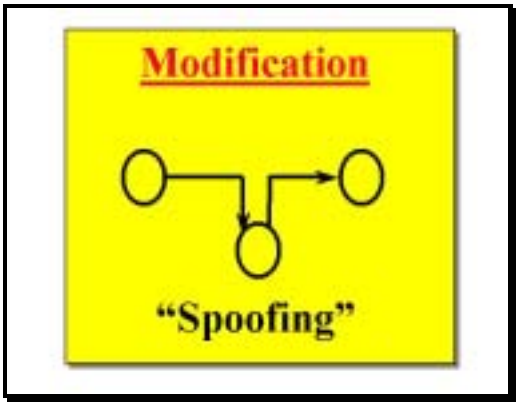

Figure 4. Modification

Fabrication

Fabricating or "injecting" data into a command and control system can wreak havoc on a system. Loss of confidence in the entire network can result. Imagine injections of new sorties into an Air Tasking Order or cancellation of needed logistics. This method

requires experience or knowledge in the attacked system in order for the injected messages to appear credible and authorized.

Figure 5. Fabrication

Interception

Interception or "Intelligence gathering" is the least intrusive technique. Simply monitoring or copying data for the purposes of gaining valuable intelligence on an enemy is very valuable to our adversaries. Imagine the impact of an enemy having a copy of our Air Tasking Order in advance. Targets could be relocated, defenses could be adjusted, counterair could be waiting in ambush.

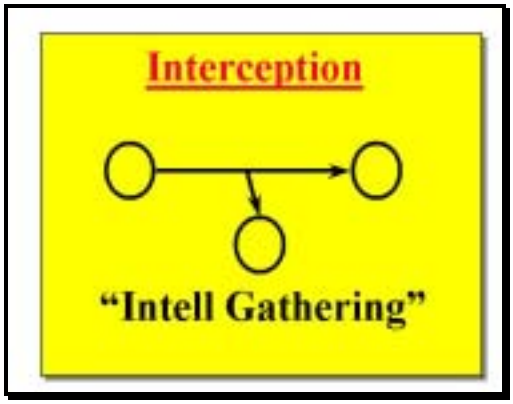

Figure 6. Interception

Interruption

Interruption or "Denial of Service" is probably the most intrusive technique. There is little doubt to a skilled adversary that the enemy is "inside the wire" and they are undergoing an attack when a denial of service attack occurs. Surprise is lost and future access to the target system may also be jeopardized. Timing is everything with denial of service attacks. Imagine the potential impact of a denial of service attack on a command and control system that coincides with a major military offensive.

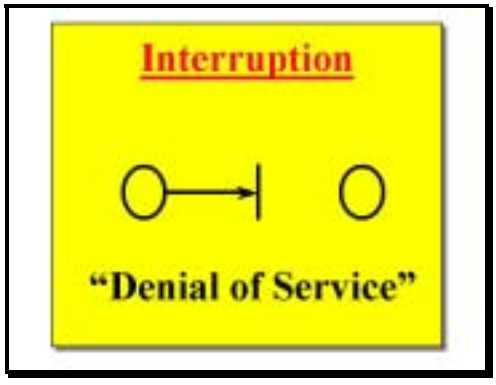

Figure 7. Interruption

Cyber Tactics, Techniques, and Procedures (TTPs) - How?

For decades, the world has witnessed unauthorized intrusions and web hacks from a myriad of actors: teenagers, industrial espionage experts, hacker groups and nation states. Newcomers to this area have infiltrated very sensitive systems with relative ease. There are many TTPs utilized by these actors.

Social Engineering/Dumpster Diving/Trashing

Social engineering is getting information from a person rather than breaking into a system. It is an attempt to have a legitimate user provide the hacker with useful information such as a name and password.[15] Social engineering is a hacker's clever manipulation of humans to gather information needed to access an information system. This method can be conducted in person (shoulder surfing), by phone, by dumpster diving or trashing (sorting through discarded trash) or even on-line. The natural tendencies of humans to help others are a vulnerability exploited very successfully by many hackers. Several of the world's most renowned hackers, including Kevin Poulsen and Kevin Mitnick, utilize this technique often.[16]

Polymorphic Viruses/Code

Polymorphic viruses or polymorphic code changes its fundamentals with each replication in order to preclude detection, filtering, blocking, or anti-virus software. Polymorphic viruses take on many forms. Some insert junk code into the virus source code, while others insert random numbers or extra line feeds. More sophisticated versions change their virus code variable names with each replication. This tactic is

intended to make detection much more difficult and allow viruses to proliferate further without restraint.[17]

WM95.Slow was the first true polymorphic macro computer virus. More recent ones include: *Nasty, Zevota,* and *Jug.A.* These viruses vary in several ways and further the ongoing cat and mouse game of virus authors and anti-virus software and network defenses. Detection of polymorphs is extremely difficult and pose a real concern for the future.[18]

Worms

Worms are independent programs that replicate themselves to congest networks. They can be very malicious and destroy valuable data. The *Nimda* worm caused an estimated $530 million in damages worldwide.[19] The *Code Red* worm (July 2001) infected a quarter million computers in nine hours and was labeled "a real and present threat to the Internet" by the National Infrastructure Protection Center.[20] *Code Red* caused an estimated $2.6 billion dollars in damages.[21] Worms are very costly and are serious threats.

Viruses

Viruses also cause a great deal of damage and are proliferating at ever-increasing rates. The *I Love You* virus (May 2000) infected millions of computers worldwide and caused billions of dollars in damages in just 5 hours. It had over 80 variants and was traced back to one individual. The *Melissa* virus set records with its unprecedented rapid spread around the world and set new standards for the world.

Denial of Service Attacks

Denial of Service attacks are characterized by intruders obstructing access to a computer system from one or more authorized users. The damage done to national security interests by such attacks depends on the functions of the actual system attacked.

October 2002 marked the most coordinated attack on the Internet itself seen to date. Attackers sent floods of traffic to the Internet's 13 core domain name servers. These devices serve as the Internet's phone book properly routing traffic to its destination. 9 of the 13 were taken off-line. Denial of service floods of this type have been predicted for over two years. This attack demonstrated both the intent and capability to potentially take down the Internet.[22]

Categories of Information Targets - Where?

Recent discussions by experts before Congress have included targets such as: the Centers for Disease Control, financial networks, water supplies, major cities, electrical grids, dams, the Internet, telephones, air traffic control, rail, and public transportation systems.[23]

The President's Commission on Critical Infrastructure Protection (PCCIP) divided our national infrastructures into five sectors: (1) information and communication, (2) physical distribution, (3) energy, (4) banking and finance, and (5) vital human services.

Information and Communications

This sector includes the public telecommunications networks, the Internet, and millions of computers at homes, business, industry, and government.

Physical Distribution

This sector includes our interconnected network of highways, rail lines, ports, pipelines, airports, mass transit, and trucking companies.

Energy

This sector includes industries that produce and distribute electrical power, oil, and natural gas.

Banking and Finance

This sector includes banks, financial services companies, mutual funds, securities, and commodities exchanges.

Vital Human Services

This sector includes water supplies, emergency services such as police and fire, and critical government services such as social security and unemployment payments.[24]

The Weakest Link

Terrorists have a history of scoping out targets for months or even years. Post 9/11, America has dramatically increased its defenses on several fronts: border patrols, immigration, physical protection at key sites, and new operating procedures. The key here is to not become the weakest link. With the rise in physical protection, more and more Force Protection Condition (FPCON) measures implemented, and security improvements, the cyber world may soon become the weakest link. If a terrorist is precluded physical access to its targets, his methods may shift to other asymmetric methods such as: mail bombs, cyber attacks, or biological attacks.

Motives - Why?

Physical attacks are the simplest. Nuclear, chemical, and biological attacks require very specific skills, knowledge, and materials and may be much more difficult to implement. In an asymmetric world, terrorists will look for alternate methods to spread terror. The cyber world may prove to be the simplest and quickest alternative to traditional physical attacks.

Cyber Attack

Motives of cyber attacks vary greatly: intimidation, coercion, retaliation, influence, power, specific objectives, revenge, induce fear or panic, decrease public confidence in infrastructures, spread ideology (religious and/or political), or financial gain. Terrorists motives will likely be the same as physical attack motives. The dilemma in the cyber world is to not only detect who is attacking you (individual, group, nation) but understand why.

Effects/Results

Terrorists will likely seek: financial impact, ransom, disruption, decreased military capability, fear/panic, publicity, news impact, decrease confidence in critical infrastructures, psychological operations, great physical damage, and/or loss of life.

Advantages

There are many distinct advantages to cyber attacks: cheap, fast, tough to trace, low risk, no martyrdom required, no handling of explosives, no border crossings, low probability of detection, easy to hit and run, detection and trace actions are difficult, borders do not have to be crossed, logistics requirements are low, remote, anonymous,

can operate from anywhere on the globe and be mobile, range, appeals to younger generations, and are stealthy.

Disadvantages

There are also disadvantages: takes resources, new skills for many terrorists, could possibly be traced, takes lead time to gain accesses, hard to control, less drama and emotional appeal, may not try new methods until old ones are inadequate or protected against, controlling systems can be complex without the right skills. The cyber world is relatively new in the terrorist world. However, future generations that grow up computer savvy may see this as the future's perfect asymmetric attack method.

Timing is Critical - When?

Stand Alone/Isolated Attack

Cyberattacks, whether stand alone or coordinated attacks, occur at the time and choosing of the adversary. They are inherently stealthy and can be used at critical periods such as: as U. S. forces deploy, take actions, a critical point in a war, retaliation for trials, prosecutions, sentencing, or for specific events. Terror attacks are often randomly timed and sporadically targeted in order to maximize the aspect of surprise. Cyberattacks have the same characteristics.

Coordinated/Compound Attack

> What I fear is the combination of a cyberattack coordinated with more traditional terrorism, undermining our ability to respond to an attack when lives are in danger.
>
> Representative Jane Harman, Democrat, California
> House Intelligence Committee Panel on Terrorism and Homeland Security

It is likely that cyber attacks will accompany physical attacks to enhance the impact and reduce our response capabilities. Complimenting physical attacks with cyber attacks magnify their impact and limit first responders and assistance. This type of attack could serve as a force multiplier for the terrorists. Initial destruction followed by limited timely response capability could significantly magnify the end effect of the attacks.

Notes

[12] "National Strategy to Secure Cyber Space", Draft version, September 2002.

[13] *Computer Security*, *Issues & Trends*, Vol. IV, No.1, Winter 1998, Computer Security Institute, page 1.

[14] "Cyber-Attacks by Al Qaeda Feared" at www.washingtonpost.com/ac2/wp-dyn/A50765_2002Jun26?start=24&per=24, October 30, 2002.

[15] "Methods of Hacking: Social Engineering" at www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html, October 24, 2002.

[16] "Social Engineering Fundamentals, Part 1: Hacker Tactics" at www.online.securityfocus.com/infocus/1527, December 18, 2001.

[17] "Polymorphic Macro Viruses, Part One" at www.online.securityfocus.com/infocus/1635, October 23, 2002.

[18] "Polymorphic Macro Viruses, Part Two" at www.online.securityfocus.com/iforuc/1638, November 5, 2002.

[19] "Cyber-Attacks by Al Qaeda Feared" at www.washingpost.com/ac2/wp-dyn/A50765-2002Jun26?start=48&per=16, October 30, 2002.

[20] "Cyber Terror – Potential for Mass Effect" at www.iac.dtic.mil/iatac, Winter 01/02.

[21] "Is Cyber Terror Next?" at www.ssrc.org/sept11/essays/denning_text_only.htm, October 30, 2002.

[22] "Is a Larger Net Attack on the Way?" at www.msnbc.com/news/827209.asp?cp1=1, November 1, 2002.

[23] "Cyberspace Full of Terror Targets" at www.usatoday.com/life/cyber/tech/2002/05/06/cyber-terror.htm, September 11, 2002.

[24] "President's Commission on Critical Infrastructure Protection", Appendix A, Sector Summary Reports.

Chapter 4

Recent Real-World Cyber Events

Our enemies and our would-be enemies are working very hard at cyberterrorism….They are trying to level the playing field because they know they can't beat us tank for tank, plane for plane.

Representative Curt Weldon, PA

Eligible Receiver

ELIGIBLE RECEIVER (ER) 1997 was a no-notice Joint Staff exercise designed to test DoD planning and crisis action capabilities when faced with attacks on DoD information infrastructures. This exercise revealed significant vulnerabilities in DoD information systems and specific deficiencies in responding to attacks on their information systems. ER ’97 involved DoD, Joint Staff, the Services, USACOM, USPACOM, USSPACECOM, USSOCOM, USTRANSCOM, NSA, DISA, NSC, DIA, CIA, FBI, NRO, and the Departments of State, Justice, and Transportation.

ER ’97 included an actual attack on key DoD information systems. Known vulnerabilities were exploited and computer systems were actually disrupted. DoD Red Team computer experts derived techniques and tools from open source research (primarily from the Internet), used commercial internet accounts, and exploited actual vulnerabilities. Their targets included: the National Military Command Center (NMCC) in the Pentagon, USPACOM, USSPACECOM, USTRANSCOM, and USSOCOM. The

Red Team intruded computer networks, denied services, changed/removed/read e-mails, and disrupted phone services. The team gained superuser access in over 36 computer systems which meant they could create new accounts, delete accounts, turn the system off, or reformat the server hard drives. The key observations of the exercise included:

- poor informational/operational security practices contributed to DoD vulnerabilities
- attribution of attacks is very difficult (determining who and why)
- DoD has little capability to detect or assess cyber attacks
- detection, reporting, response processes are unresponsive to the speed of cyber attacks.[25]

ER '97 demonstrated, in a real world exercise, that DoD was not properly organized for IO and did not detect/report/respond to IO attacks in a timely manner. The Red Team attackers successfully demonstrated that, by using open source vulnerabilities and exploitation tools and techniques (readily available on the Internet), DoD and national infrastructure networked computer systems can be severely degraded.[26]

SOLAR SUNRISE

> I would characterize it [DoD computer network attacks] as being systematic and moderately sophisticated…I think this was, more than anything, a serious wake-up call.
>
> Dr. John J. Hamre
> Deputy Secretary of Defense

SOLAR SUNRISE was a series of DoD computer network attacks that occurred from 1-26 February 1998. The attack pattern was indicative of a preparation for a follow-on attack on the DII. DoD unclassified networked computers were attacked using a well-

known operating system vulnerability.[27] The attackers followed the same attack profile: (a) probing to determine if the vulnerability exists, (b) exploiting the vulnerability, (c) implanting a program (sniffer) to gather data, and (d) returning later to retrieve the collected data.

At least eleven attacks followed the same profile on Air Force, Navy, and Marine Corps computers worldwide.[28,29] Attacks were widespread and appeared to come from sites such as: Israel, the United Arab Emirates (UAE), France, Taiwan, and Germany. The attacks targeted key parts of the defense networks and obtained hundreds of network passwords. Although all DoD targeted systems were reported as unclassified, we must remember many key support systems reside on unclassified networks (Global Transportation System, Defense Finance System, medical, personnel, logistics, and official e-mail).

DoD established a 24-hour emergency watch, installed intrusion detection systems on key nodes, and assisted law enforcement in computer forensics and investigation. SOLAR SUNRISE confirmed earlier ELIGIBLE RECEIVER findings: DoD has no effective indications and warning system, intrusion detection systems are insufficient, DoD is not organized effectively for IO, and that identifying the threat group and motives is extremely difficult.[30,31]

These attacks occurred when the U.S. was preparing for potential military action against Iraq due to UN weapons inspection disputes and could have been aimed at disrupting deployments and operations.[32] So who was behind these attacks—Iraq, terrorists, foreign intelligence services, nation states, or hackers for hire? The attackers were two teenagers from California and one teenager from Israel.[33,34] Their motivations

were believed to be ego, power, and the challenge of hacking into U.S. DoD computer systems.[35] I began the SOLAR SUNRISE description by stating that the attacks occurred on unclassified DoD systems. One of the California teenagers additionally admitted to penetrating computer networks at Lawrence Livermore Labs (a national nuclear research facility) and claims it was a classified system and that the FBI was extremely interested in his involvement with this site.[36] Total costs for the investigation included: data recertification, cleansing infected systems of possible malicious code, trojan horses, and backdoors. The attacks did not cause any serious damage to DoD systems, however they could have severely impacted DoD during heightened tensions with Iraq.

ER ’97 and SOLAR SUNRISE demonstrated the vulnerabilities of DoD computer networks. As Dr. Hamre, Former Deputy Secretary of Defense, said, "this should serve as a serious wake-up call".[37] If high-school kids can infiltrate DoD systems with ease, imagine the damage that could be done to U.S. security by skilled professionals or potential adversaries in future asymmetric conflicts.[38]

Al Qaeda’s Use of Cyber World

Today, Al Qaeda is America’s number one terrorist adversary. Would terrorists actually use the cyber world? Is this a realistic concern? Let’s take a closer look at how Al Qaeda has used cyber technology thus far. Al Jazeera reported that senior aides to bin Laden described the instructions for the 9/11 attacks were transmitted to Mohammed Atta via encoded e-mail.[39] Many Al Qaeda supporters and sympathizers are establishing websites (alneda.com, jehad.net, aloswa.org) to show their support for bin Laden. These extremists have found shelter on the Internet.[40] Sites such as 7hj.7hj.com teach surfers the art of computer attack and trains hacking skills to serve Islam. This has global appeal

to young Muslims who can enter the fight without traveling to Afghanistan and risking their lives in service to the cause.

Al Qaeda terrorists are using the Internet to research infrastructure information on American water and wastewater systems. The FBI released bulletins that said, "U. S. law enforcement and intelligence agencies have received indications that Al Qaeda members have sought information on Supervisory Control And Data Acquisition (SCADA) systems available on multiple SCADA-related web sites." SCADA systems allow utility companies to monitor and direct equipment at unmanned facilities from a central location.[41] Computers of bin Laden associates were found to include structural engineering data and programs related to dams and other water retaining structures. Other infrastructure related information, available on the Internet, is being accessed from sites around the world.[42] Lamar Smith, Representative from Texas, said that Congress has been briefed on Al Qaeda operatives probing the electronic infrastructure in search of ways to disrupt or disable power, phones, and water supplies. They are especially interested electrical systems in California.[43] Researching SCADA systems demonstrates a high level of sophistication.

Ramzi Yousef, the original World Trade Center bomber, stored detailed plans to destroy American airliners on encrypted files on his laptop computer.[44] Terrorist groups are also using the Internet to recruit like-minded people to their cause. A recent term has emerged called "hacktivists" which includes cyber protests, floods, denials of service, and hacks for a political cause. We have seen a rise in actions taken immediately following real-world events. We saw several new viruses and web server attacks

following 9/11. These included the *W32.Nimda.A@mm* virus and the attacks of Iranian and Taliban websites.[45]

Khalid Ibrahim is a member of a Pakistani terrorist group (Harkat-Ul-Ansar) and a bin Laden supporter. He is known to use death threats and social engineering to gain information on how to hack U. S. military networks. He sent certified checks in the mail to potential informants within the US. He is seeking retaliation on U. S. strikes against Al Qaeda.

Al Qaeda has not been known to use cyber attacks in the past. However, bin Laden has suggested that he has the expertise to use the computer as a weapon. Bin Laden was quoted by the Ausaf newspaper after the 9/11 attacks, "hundreds of young men had pledged to him that they were ready to die and that hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and ranging from computers to electronics against the infidels." This statement implies bin Laden is threatening computer attacks against America.[46] Bin Laden has posted a rambling 11,000 word declaration of war against the U. S. on-line. This document is known as "The Ladenese Epistle". It calls for the expulsion of U. S. forces from Saudi Arabia and the overthrow of the current Saudi government. He calls this a jihad or holy war.[47]

The CIA is already alert to the possibility of cyber warfare by Al Qaeda and describes this group as becoming "more adept at using the Internet and computer technologies." Al Qaeda are believed to be developing cyber terrorism plans.[48] The Washington Post and CBS news have reported that Al Qaeda prisoners have informed interrogators about their intent to use cyber attack tools. Captives said Al Qaeda is on the

threshold of using the Internet as a direct instrument of bloodshed. It is a question of when, not if.[49]

Damage/Death via a Cyber Attack

A terrorist must go beyond webpage defacements, simple hacks, or pranks and "attack people". In order to gain the publicity for his cause that he seeks, he must cause widespread damage, destruction, and death.

In 1998, a 12-year-old hacker broke into the SCADA computer systems that run the Arizona's Roosevelt Dam. Federal authorities said he had complete control of the dam's massive floodgates. This dam holds back as much as 489 trillion gallons of water. He could have totally flooded the cities of Mesa and Tempe which have a combined population of nearly a million people.[50] Had the floodgates been opened, lives would have surely been lost. There are an estimated 3 million SCADA devices in use today.

Hackers affiliated with Al Qaeda are conducting suspicious surveillance of nuclear power plants, dams, and other critical infrastructures. Information about SCADA devices and hacking them were found on Al Qaeda computers seized in raids in Afghanistan. Al Qaeda prisoners have informed interrogators about their intent to use these methods to attack the U. S. to cause death and destruction.[51] If a terrorist group gained access to one of these critical infrastructure systems, it would not take a lot of imagination to develop a plan that could cause widespread damages and death. Examples include: opening flood gates on a dam, closing down a city's electrical grid, switching a passenger train to collide with a freight train, or turning off an air traffic control system during a winter storm. Given that this could be a successful strategy, do terrorists have the capabilities to carry out these type plans?

[25] Joint Staff/J39 Briefing, “IA-The Way Ahead”, March 1998.

[26] Ibid.

[27] Glave, James. *Wired News*, “DoD Cracking Team Used Common Bug”, March 5, 1998.

[28] Lardner, Richard and Pamela Hess, “Pentagon Looks for Answers to Massive Computer Attack”, *Defense Information and Electronics Report*, February 13, 1998.

[29] Graham, Bradley, “11 U.S. Military Computer Systems Breached by Hackers This Month,” *Washington Post*, February 26, 1998, page 1.

[30] Ibid.

[31] Joint Staff/J39 Briefing, “IA—The Way Ahead,” March 1998.

[32] Graham, Bradley, “11 U.S. Military Computer Systems Breached by Hackers This Month,” *Washington Post*, February 26, 1998, page 1.

[33] Van Derbeken, Jaxon and Jim Doyle and Glen Martin, "Hacking Suspect Caught in Cloverdale", *San Francisco Chronicle*, February 27, 1998.

[34] Glave, James, “Analyzer Nabbed in Israel?,” *Wired News*, 16 March 1998.

[35] AntiOnline, "Interview with Makaveli", March 2, 1998.

[36] Reed, Dan, "Pentagon Hacker Suspect Tells of Plans for Retaliation", *San Jose Mercury News*, March 3, 1998.

[37] Department of Defense News Briefing, OSD/PA Press Release, February 25, 1998.

[38] “Information Assurance – the Achilles’ Heel of Joint Vision 2010,” Brad Ashley, et al, Armed Forces Staff College research paper, March 1998.

[39] “Cyber News, Virtual Soldiers in a Holy War” at www.ds-osac.org/edb/cyber/news/story.cfm?KEY=9026, September 27, 2002.

[40] Ibid.

[41] “FBI Issues Water Supply Cyberterror Warning” at www.online.securityfocus.com/news319, September 30, 2002.

[42] Ibid.

[43] “Al Qaeda Cyber Alarm Sounded” at www.fcw.com/fcw/articles/2002/0722/web-attack-07-25-02.asp, September 11, 2002.

[44] “Cyber-terrorists Wield Weapons of Mass Disruption” at www.news.bbc.co.uk/1/hi/sci/tech/specials/washington_2000/648429.stm, September 11, 2002.

[45] “Malicious Internet Activity Increases Following 11 September Attacks” at www.janes.com/security/international_security/news/jir/jir010925_1_n.shtml, September 25, 2001.

[46] “Report Warns of Al-Qaeda’s Potential Cybercapabilities” at www.infowar.com/class3/02/class3010902aj.shtml, September 11, 2002.

[47] “You’ve Got War” at, www.wired.com/news/topstories/0,1287,14608,00.html, September 11, 2002.

[48] ”CIA Identifies Cyber Terror Groups” at www.vnunet.com/news/1136404, October 30, 2002.

[49] “Use of Web in Terror Attack Feared” at www.cbsnews.com/stories/2002/06/27/attack/main513582.shtml, September 11, 2002.

Notes

[50] "Cyber-Attacks by Al Qaeda Feared" at www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26?start=24&per=24, October 30, 2002.

[51] US Fears Nuclear Cyber Terror Attacks, Nick Farrell, June 27, 2002.

Chapter 5

Terrorist Capabilities Assessed

> *The difficulty of accurate recognition constitutes one of the most serious sources of friction in war...war has a way of masking the stage with scenery crudely daubed with fearsome apparitions.*
>
> —Carl von Clausewitz

How do we measure if a terrorist or terror group is capable? There is an accepted model within DoD that assesses threat based on several factors: existence, capabilities, intentions, history, and targeting. This model can be applied to the Al Qaeda to gain some insight on their assessed cyber threat.

Threat Level Determination[52]

This threat-analysis methodology is used by the Defense Intelligence Agency (DIA), the Joint Staff, and the unified and specified commands for assessing the level of threat. It considers five main factors: existence, capability, intentions, history, and targeting. Various threat levels are determined by the presence of these factors. Figure 8 describes these in more detail.

Explanation of Factors	
Factor 1: **Existence.** A terrorist group is present, assessed to be present, or able to gain access to a given locale. Factor 2: **Capability.** The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks. Factor 3: **Intentions.** Recent demonstrated anti-US terrorist activity or stated and/or assessed intent to conduct such activity. Factor 4: **History.** Demonstrated terrorist activity over time. Factor 5: **Targeting.** Current credible information on activity indicative of preparations for specific terrorist operations and/or specific intelligence that shows an attack is imminent.	
Threat Levels	
Critical	Factors 1, 2, and 5 are present. Factors 3 or 4 may be present.
High	Factors 1, 2, 3, and 4 are present.
Medium	Factors 1, 2, and 4 are present.
Low	Factors 1 and 2 are present. Factor 4 may be present.
Negligible	Factors 1 and/or 2 may be present.

Figure 8. Threat Level Determination

Al Qaeda Assessed

> There is a 50 percent change that the next time Al Qaeda terrorists strike the United States, their attack will include a cyberattack.
>
> Lamar Smith, Representative, TX

Let's take a closer look at Al Qaeda using the above assessment model and its 5 factors.

Existence

YES - a terrorist group is present, assessed to be present, or able to gain access to a given locale.

Capabilities

YES - The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

Intentions

YES - Recent demonstrated anti-US terrorist activity or stated and/or assessed intent to conduct such activity.

History

Yes - for reconnaissance, **No -** for demonstrated cyber terrorist activity.

Targeting

YES - Current credible information on activity indicative of preparations for specific terrorist operations and/or specific intelligence that shows an attack is imminent.

Therefore, the overall assessment of the Al Qaeda cyber threat is: **Critical**.

A June 2002 survey of technology industry experts revealed that 74% thought it was nearly certain that there will be a cyber attack against America within one year. 59% said they expect a major cyber attack against the federal government within one year. These dramatic findings prompted a call for the creation of a Cyber Security Agency within the proposed Homeland Security Department.[53] Bin Laden has threatened the use of cyber attack but there is no documented history of Al Qaeda cyber attacks. However, with his vast finances, he certainly could develop or hire out this capability.

A February 2002 CIA Directorate of Intelligence Memorandum said Al Qaeda had "far more interest" in cyberterrorism than previously believed and contemplated the use of hacker for hire to speed the acquisition of capabilities.[54]

Notes

[52] "Intelligence, Counterintelligence, and Threat Analysis" at www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/appc.htm, October 23, 2002.

[53] "Al Qaeda Cyber Alarm Sounded" at www.fcw.com/fcw/articles/2002/0722/web-attack--7-25-02.asp, September 11, 2002.

[54] "Cyber-Attacks by Al Qaeda Feared" at www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26?start=24&per=24, October 30, 2002.

Chapter 6

Summary

…the struggle for power changes when knowledge about knowledge becomes the prime source of power.

—Alvin Toffler

Figure 9. Ashley's Cyberterrorism Model Revisited

In order to successfully understand the world of cyberterrorism, we must study its components and analyze the who, what, how, where, why, and when questions. As a new

dimension of warfare, the cyber environment must be thoroughly studied and analyzed. Hopefully, my cyberterrorism model contributes to this new body of knowledge.

America's Cyber Future

U. S. National Security Strategy

The latest U. S. National Security Strategy document focuses on defeating global terrorism, preventing our enemies from threatening us, and denying new sanctuaries. The bulk of this document addresses the physical world; however, most of its major tenets and ideas apply to the cyber world as well. The cyber world is such a new "dimension" of national security that our policy and doctrine will take time to catch up to the possibilities of the technologies. Until that time, cyberspace will remain much like the old wild west where the strong survive and rules are sporadically enforced. Criminals run amuck and the rules of engagement continue to evolve.

National Strategy to Secure Cyberspace[55]

"Cyberspace is essential to both homeland security and national security; its security and reliability support the economy, critical infrastructures, and national defense." The strategy describes initiatives to secure U.S. information systems against deliberate and malicious disruption.

The national strategy definitely considers a cyber terrorist attack as a viable reality. "Though the U.S. possesses both the world's strongest military and largest national economy, these two aspects of the nation's power increasingly rely upon certain critical infrastructures, which include cyber-based information systems. As witnessed on 9/11, enemies of the U.S. (nations, groups, and indeed, even individuals) are prepared to strike

in unconventional ways. These adversaries have explicitly stated the intention, not only to strike at U.S. citizens, but to attack the nation's infrastructures and cyberspace-the pillars of the economy."[56]

The President is expected to sign the National Strategy to Secure Cyberspace within a few months. The draft document calls for the development of a clear roadmap to protect critical infrastructures. "Cyberspace is essential to both homeland security and national security; its security and reliability support the economy, critical infrastructure, and national defense", the document states.

Recommendations

The events of 9/11 caught us by surprise. We cannot afford to disregard the cyber threat and be caught by surprise by a major cyber assault. Unless we take the appropriate steps to protect ourselves against cyber attacks now, America will surely suffer tragic cyberterrorist attacks that will include loss of life.

There are several key recommendations to improve the current U. S. cyber security posture:

- Accept cyberterrorism as a viable near-term threat
- Organize for success and establish the new Department of Homeland Security and its new Cyber/Infrastructure Division
- Debate the issues with Congress and the public to raise awareness
- Increase punishment for cyber crimes with terror or death as a motive
- Finalize the national cyber security plan and implement it
- Conduct Inter-Agency Cyber Exercises

- Commit Congressional funding to improve cyber security
- Commit manpower and training to implement the plan effectively

We must prepare for an inevitable and perhaps imminent cyberterrorist attack. It took a tragic event on 9/11 to improve the nation's physical security strategy. We should not wait for a similar cyber tragedy before we take action to improve our security. We know terrorists are pursuing this capability. Major cyberterror attacks against America will occur. It is a matter of when, not if.

Notes

[55] "National Security Strategy to Secure Cyberspace", Draft, September 2002.
[56] Ibid, pg 7.

Appendix A - Glossary of Terms[57]

Command and Control Warfare (C2W): The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations. Also called C2W. C2W is both offensive and defensive: a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. See also command and control; electronic warfare; information operations; intelligence; military deception; operations security; psychological operations.

Defense Information Infrastructure (DII): The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving Department of Defense (DOD) local, national, and worldwide information needs. The defense information infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information. Also called DII. See also global information infrastructure; information; infrastructure; national information infrastructure.

Global Information Infrastructure (GII): The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. Also called GII. See also defense information infrastructure; information; information system; national information infrastructure

Information: Facts, data, or instructions in any medium or form. The meaning that a human assigns to data by means of the known conventions used in their representation

Information Assurance (IA): Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA. See also information; information operations; information system

Information Operations (IO): Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Superiority: That degree of dominance in the information domain which permits the conduct of operations without effective opposition. See also information operations.

Information System: The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Information Warfare (IW): Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Intelligence Preparation of the Battlespace (IPB): An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB.

National Information Infrastructure (NII): The nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure. Also called NII.

Notes

[57] "DoD Dictionary" at http://www.dtic.mil/doctrine/jel/doddict/index.html, October 22, 2002.

Bibliography

AntiOnline, "Interview with Makaveli" at www.antionline.com, March 2, 1998.

Campen, Alan D., Col, USAF, "Information War Techniques Supersede Kinetic Weapons", *SIGNAL*, May 1998, pg 33-36.

Computer Security, Issues & Trends, Vol. IV, No.1, Winter 1998, Computer Security Institute, p. 1.

Defense Science Board Report, "Task Force on Information Warfare-Defense (IW-D)" at www.jya.com/iwd.htm, November 1996.

Denning, Dorothy, "Is Cyber Terror Next?" at www.ssrc.org/sept11/essays/denning_text_only.htm, October 30, 2002.

Department of Defense Directive S-3600.1, *Information Operations*, Washington, GPO, December 9, 1996.

Department of Defense News Briefing, OSD/PA Press Release, February 25, 1998.

GAO Report, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks" at www.fas.org/irp/gao/aim96084.htm, May 22, 1996.

Glave, James, "Analyzer Nabbed in Israel?," *Wired News*, March 16, 1998.

Glave, James, "DoD Cracking Team Used Common Bug," *Wired News*, March 5, 1998.

Graham, Bradley, "11 U.S. Military Computer Systems Breached by Hackers This Month," *Washington Post*, February 26, 1998, page 1.

Lardner, Richard and Pamela Hess, "Pentagon Looks for Answers to Massive Computer Attack," *Defense Information and Electronics Report*, February 13, 1998.

Overholt, Matt, "Overview of Cyber-Terrorism" at www.cybercrimes.net/terrorism/overview/page1.html, September 12, 2002.

Prepared Testimony of Jim Christy, AF Investigator before the Senate Government Affairs Committee Permanent Investigations Sub-Committee, June 5, 1996.

President's Commission on Critical Infrastructure Protection Report, "Critical Foundations, Protecting America's Infrastructures," October 1997.

Reed, Dan, "Pentagon Hacker Suspect Tells of Plans for Retaliation", *San Jose Mercury News*, March 3, 1998.

Szappanos, Gabor, "Polymorphic Macro Viruses, Part Two" at www.online.securityfocus.com/iforuc/1638, November 5, 2002.

United States Department of Army Memorandum. FORSCOM Network Security Improvement Program (NSIP) Action Plan (Draft), pg. 7.

United States Joint Chiefs of Staff, CJCS Instruction 6510.01B, *Defensive Information Operations Implementation*, Washington, GPO, June 30, 1997.

United States Joint Chiefs of Staff, *Concept for Future Joint Operations, Expanding Joint Vision 2010*, Washington, GPO, May 1997.

United States Joint Chiefs of Staff, JCS Pub 3-13, *Joint Doctrine for Information Operations*, January 28, 1998, page I-22 and GL-14.

United States Joint Chiefs of Staff, *Joint Vision 2010*, Washington, GPO, 1996.

United States Joint Chiefs of Staff, J39, Information Operations Division Briefing, *IA-The Way Ahead*, March 1998.

United States Joint Chiefs of Staff, J6K, Information Assurance Division Briefing, *Rome Labs Case*, November 1997.

Van Derbeken, Jason and Jim Doyle and Glen Martin, "Hacking Suspect Caught in Cloverdale", *San Francisco Chronicle*, February 27, 1998.