NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

RESPONDING TO THE THREAT OF CYBERTERRORISM THROUGH INFORMATION ASSURANCE

by

Joel G. Ogren
James R. Langevin

June 1999

Thesis Advisor:	John S. Osmundson
Co-Advisor:	Timothy J. Shimeall

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 1999	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE : Responding to the Threat of Cyberterrorism Through Information Assurance.	5. FUNDING NUMBERS
6. AUTHOR(S) Joel G. Ogren and James R. Langevin	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

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

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

13. ABSTRACT *(maximum 200 words)* The number of people connecting to the Internet is growing at an astounding rate: estimates range from 100% to 400% annually over the next five years. This unprecedented level of interconnectedness has brought with it the specter of a new threat: *cyberterrorism*. This thesis examines the impact of this threat on the critical infrastructure of the United States, specifically focusing on Department of Defense issues and the National Information Infrastructure (NII). A working definition for cyberterrorism is derived, and a description of the Nation's critical infrastructure is provided. A number of possible measures for countering the threat of cyberterrorism are discussed, with particular attention given to the concept of *information assurance*. Information assurance demands that trustworthy systems be developed from untrustworthy components within power-generation systems, banking, transportation, emergency services, and telecommunications. The importance of vulnerability testing (or *red-teaming*) is emphasized as part of the concept of information assurance. To support this, a cyberterrorist "red team" was formed to participate in the Marine Corps' Urban Warrior Experiment. The objective of this thesis is to address the impact of these issues from a Systems Management perspective. This includes taking into account the changes that must occur in order to improve the U.S.' ability to detect, protect against, contain, neutralize, mitigate the effects of, and recover from attacks on the Nation's Critical Infrastructure.

14. SUBJECT TERMS Terrorism, Information Terrorism, Cyberterrorism, Information Infrastructure, Critical Infrastructure, Information Assurance, Vulnerability Testing, Information Warfare.	15. NUMBER OF PAGES 90
	16. PRICE CODE

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

Approved for public release; distribution is unlimited

RESPONDING TO THE THREAT OF CYBERTERRORISM THROUGH INFORMATION ASSURANCE

Joel G. Ogren
Major, United States Marine Corps
B.S., Southwest State University, 1986

James R. Langevin
Lieutenant, United States Coast Guard
B.S., Arizona State University, 1987

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 1999

Authors:

Joel G. Ogren

James R. Langevin

Approved by: John S. Osmundson

John S. Osmundson, Thesis Advisor

Timothy J. Shimeall

Timothy J. Shimeall, Co-Advisor

Gail Fann Thomas

Reuben T. Harris, Chairman
Department of Systems Management

ABSTRACT

The number of people connecting to the Internet is growing at an astounding rate: estimates range from 100% to 400% annually over the next five years. This unprecedented level of interconnectedness has brought with it the specter of a new threat: *cyberterrorism.* This thesis examines the impact of this threat on the critical infrastructure of the United States, specifically focusing on Department of Defense issues and the National Information Infrastructure (NII). A working definition for cyberterrorism is derived, and a description of the Nation's critical infrastructure is provided. A number of possible measures for countering the threat of cyberterrorism are discussed, with particular attention given to the concept of *information assurance*.

Information assurance demands that trustworthy systems be developed from untrustworthy components within power-generation systems, banking, transportation, emergency services, and telecommunications. The importance of vulnerability testing (or *red-teaming*) is emphasized as part of the concept of information assurance. To support this, a cyberterrorist "red team" was formed to participate in the Marine Corps' Urban Warrior Experiment. The objective of this thesis is to address the impact of these issues from a Systems Management perspective. This includes taking into account the changes that must occur in order to improve the U.S.' ability to detect, protect against, contain, neutralize, mitigate the effects of, and recover from attacks on the Nation's Critical Infrastructure.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

I. INTRODUCTION

A. OVERVIEW

The number of people connecting to the Internet is growing at an astounding rate: estimates range from 100% to 400% annually over the next five years [Ref.1]. When one considers that there are approximately 160 million users as of April 1999 [Ref. 2], these figures become truly staggering. Negroponte estimates that by the year 2005, there will be over 2 billion people connected through the Internet [Ref. 3]. This unprecedented level of interconnectedness, touching nearly every part of the globe, brings with it the specter of a new threat: *cyberterrorism*. This thesis examines the impact of this threat on the critical infrastructure of the United States, specifically focusing on Department of Defense (DoD) issues.

As the world comes to rely more and more on its information infrastructure, new vulnerabilities begin to emerge. The United States, in particular, is becoming increasingly dependent on its National Information Infrastructure (NII). The matter has been deemed of enough concern that a Presidential Decision Directive (PDD-63) was issued for the protection of the Nation's Critical Infrastructure by President William J. Clinton. The faces of our Nation's real and potential adversaries have changed significantly with the emergence of cyberterrorism. While the DoD has become a primary target in the information age, it is but one of many within the NII. This increasing threat to our critical infrastructure demands that security practices for the 21st century shift their focus. It is no longer sufficient to build defensive "walls" around our systems; our critical infrastructure must be provided with a quantifiable level of "information assurance." The challenge is to continue to function while under attack, even when the attack is partially successful.

Information assurance demands that we develop trustworthy systems from untrustworthy components within power-generation systems, banking, transportation, emergency services, and telecommunications. This thesis addresses the impact of these issues from a Systems Management perspective. This includes taking into account the changes that must occur in order to improve our ability to detect, protect against, contain, neutralize, mitigate the effects of, and recover from attacks on our Critical Infrastructure.

B. OBJECTIVE

The purpose of this thesis is to assess the impact of cyberterrorism on the United States' critical infrastructure, with specific emphasis on the National and Global Information Infrastructures. The approach taken was to identify the characteristics of cyberterrorism, create a definition for it, assess the current state of the practice for combating it, and determine a methodology for countering this threat that applies to the 21st century.

C. METHODOLOGY

To assess the impact of cyberterrorism on the DoD, National, and Global Information Infrastructures, in depth literature reviews, Internet searches, and discussions with personnel from the National Assessment Group, National Security Agency, Naval Postgraduate School, Navy Fleet Information Warfare Center, Air Force Information Warfare Center, and National Computer Emergency Response Center were conducted. Among the topics covered were Information Warfare, Information Operations, Vulnerability Testing, Critical Infrastructure, Terrorism, Information Terrorism, and

Cyberterrorism. This research culminated in the formation of *Cyber Fi*, a scenario-based cyberterrorist organization used to simulate a "red teaming" capability for the Marine Corps Advanced Warfighting Experiment, Urban Warrior. The result was a requirement for the development of a truly strategic policy for combating this new face of terrorism.

D. THESIS ORGANIZATION

This thesis consists of seven chapters. Chapter II provides an in depth discussion of the threat of cyberterrorism. A definition of cyberterrorism is derived based on the research conducted. Chapter III discusses the impact of cyberterrorism on the National and Global Critical Infrastructure and the mechanisms available to counter this threat. The effects of interdependence among infrastructures are addressed, and the concept of information assurance is introduced. Chapter IV describes the formation of Cyber Fi, a simulated cyberterrorist organization, along with its involvement in the Marine Corps Advanced Warfighting Experiment and a plausible scenario that drives our conclusions for this thesis. The technique of Information Warfare "ghosting" is also discussed in this chapter. A review of the results of the "red teaming" conducted during the Urban Warrior Advanced Warfighting Experiment is presented in Chapter V. Chapter VI follows with a discussion of a possible direction for decision-making based on the mitigation of the effects of cyberterrorism, and includes recommendations for the implementation of the concept of information assurance. Chapter VII provides conclusions and recommendations for future work.

II. DEFINING THE THREAT

A. THE CONVERGENCE OF CYBERSPACE AND TERRORISM

What is *cyberterrorism*? Barry C. Collin, a senior research fellow at the Institute for Security and Intelligence in California, first used the term in the late 1980's. He describes it as "the convergence of cyberspace and terrorism." [Ref. 4] In a more recent treatise, Mr. Collin elaborates further on the concept, stating "it is the intersection of the physical and virtual worlds that forms the vehicle of cyberterrorism, the new weapon that we face." [Ref. 5] To gain a better understanding of this concept, however, its component terms must be clearly defined.

1. Cyberspace Defined

To begin with, we must define "cyberspace," a term which was first popularized in William Gibson's 1984 novel, Neuromancer [Ref. 6]. Winn Schwartau, author of Information Warfare, describes it as follows:

> Cyberspace is that intangible place between computers where information momentarily exists on its route from one end of the global network to the other. Cyberspace is the ethereal reality, an infinity of electrons speeding down copper or glass fibers at the speed of light from one point to another. Cyberspace includes the air waves vibrating with cellular, microwave, and satellite communications. [Ref. 7]

Cyberspace has also been defined as the "total interconnectedness of human beings through computers and telecommunication without regard to physical geography." [Ref. 8] Finally, a much more concise, albeit too simplistic, definition is provided by Merriam-Webster's on-line dictionary as "the on-line world of computer networks." [Ref. 9]

As described above, cyberspace does not only relate to the world of computers, but to the entire interconnected world of networks and telecommunications. The medium is irrelevant; satellite communication links, cellular telephones, undersea fiber-optic cables, wireless local-area networks, token-ring networks, etc. are all part of this mesh of information and communication networks.

2. Terrorism Defined

We must next develop a working definition for *terrorism*. This, in itself, can prove to be a daunting task, as Mitchell, et al point out in their cyberterrorism White Paper. They note that there is no universally accepted definition, and that "about the only constant is that people continue to disagree" on the subject. [Ref. 10]

a. Tucker

In an effort to establish some common ground, David Tucker, an Associate Professor at the Naval Postgraduate School in California, outlines the five most common elements to 140 different definitions of terrorism as "violence, political purpose, intention to influence an audience, an action that produces terror, and threat." [Ref. 11] Using these elements, Tucker provides the following definition for terrorism:

> It is more than crime and less than war… it is violence against innocents or noncombatants intended to influence an audience for the sake of some political objective. [Ref. 12]

b. Denning

The issue of violence or the threat of violence is also highlighted in the following definition by author Dorothy Denning:

> Terrorism refers to the actual or threatened use of violence with the intention of intimidating or coercing societies or governments. It can be conducted by individuals or groups and is often motivated by ideological or political objectives. [Ref. 13]

c. Webster's

Lastly, Merriam-Webster's on-line dictionary defines terrorism as "the systematic use of terror especially as a means of coercion," while providing the following definition for the terms "terror" and "terrorize" [Ref. 14]:

> **ter·ror**
> 1 : a state of intense fear
> 2 a : one that inspires fear : scourge b : a frightening aspect <the *terrors* of invasion> c : a cause of anxiety : worry d : an appalling person or thing; *esp* : brat 3 : reign of terror
> 4 : violence (as bombing) committed by groups in order to intimidate a population or government into granting their demands <insurrection and revolutionary *terror*>
>
> **ter·ror·ize**
> 1 : to fill with terror or anxiety : scare
> 2 : to coerce by threat or violence

3. Information Terrorism

Through our research, we found that "cyberterrorism" is generally considered to be interchangeable with "information terrorism." However, we feel that, in order to utilize these terms synonymously, it is important to understand that "information" is being used to denote content, as well as medium. "Information" must refer not only to data, facts, knowledge, etc., but also to the systems, technologies, and infrastructures used to transfer or store these. In this context, "information" is analogous to "information space" or, more appropriately, "cyberspace." Thus, "information" can be, at once, the battlefield, the weapon, and the target in cyberterrorism.

B. INFORMATION TERRORISM VERSUS INFORMATION WARFARE

1. Information Warfare Defined

How does one differentiate between information terrorism (IT) and information warfare (IW)? Winn Schwartau describes information warfare as an "electronic conflict in which information is a strategic asset worthy of conquest or destruction." He goes on to write that computers and other communications and information systems actually become "attractive targets" in the world of IW [Ref. 15]. The Joint Chiefs of Staff (JCS) provide a more formal definition of Information Warfare in JP 3-13:

> Information Operations (IO) conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries. [These IO] activities may be offensive or defensive in nature. [Ref. 16]

JP 3-13 further explains:

> Information Operations involve actions taken to affect adversary information and information systems, while defending one's own information and information systems. They apply across all phases of an operation, throughout the range of military operations, and at every level of war. [Ref. 17]

Rod Stark summarizes these concepts by defining Information Warfare as "any action to deny, exploit, corrupt, or destroy an adversary's information and its functions, while protecting military assets against those actions and exploiting its own military information operations." [Ref. 18] IT is considered an "important subset" of IW [Ref. 19]; however, this relationship is not as clear-cut as many authors make it out to be. The lines defining IW and IT are very gray and, in many cases, indistinguishable from each other. The main distinction between information terrorism and information warfare lies in the perpetrator and the intent. If the perpetrator is state-sponsored or the terrorist actions are actually committed by a state, then the actions should be classified as information warfare. If the perpetrator's intent is not politically, socially, or ideologically motivated, then act is probably criminal (e.g., for financial gain) or simply malicious in nature.

2. Use of Information Warfare

Information warfare is by no means a new phenomenon. Denning asserts that "it is not even unique to the human species." [Ref. 20] She gives several examples in which fauna and flora use deception techniques for their survival. By modifying their adversaries' perception of reality, these "information warriors" of nature are able to defend themselves or vanquish their prey. History is rife with examples of man's use of information warfare, as well. From the protection of confidential information, to the use of deception and espionage, information warfare has figured predominantly in almost every facet of human life. But the face of information warfare changed dramatically with the invention of the computer, and more importantly, the emergence and explosion of the Internet.

3. Information Warfare and The Internet

In a span of only ten years, the Internet has gone from a mere 300,000 users to an incredible 163 million estimated users, as shown in Figure 1 [Ref. 21]. And this is only the tip of the iceberg, according to many industry pundits. Nicholas Negroponte, the founder and director of Massachusetts Institute of Technology's Media Lab, predicts that there will be one billion users worldwide by the end of the year 2000, with the majority of this growth occurring in third world countries [Ref. 22]. He bases these numbers on the belief that many of the world's developing nations will be leapfrogging past the need for a conventional telecommunications infrastructure. Instead, these nations will make use of current and emerging technologies – such as Iridium and Teledesic – that may be able to provide the same connectivity without the associated high costs and lengthy building process.

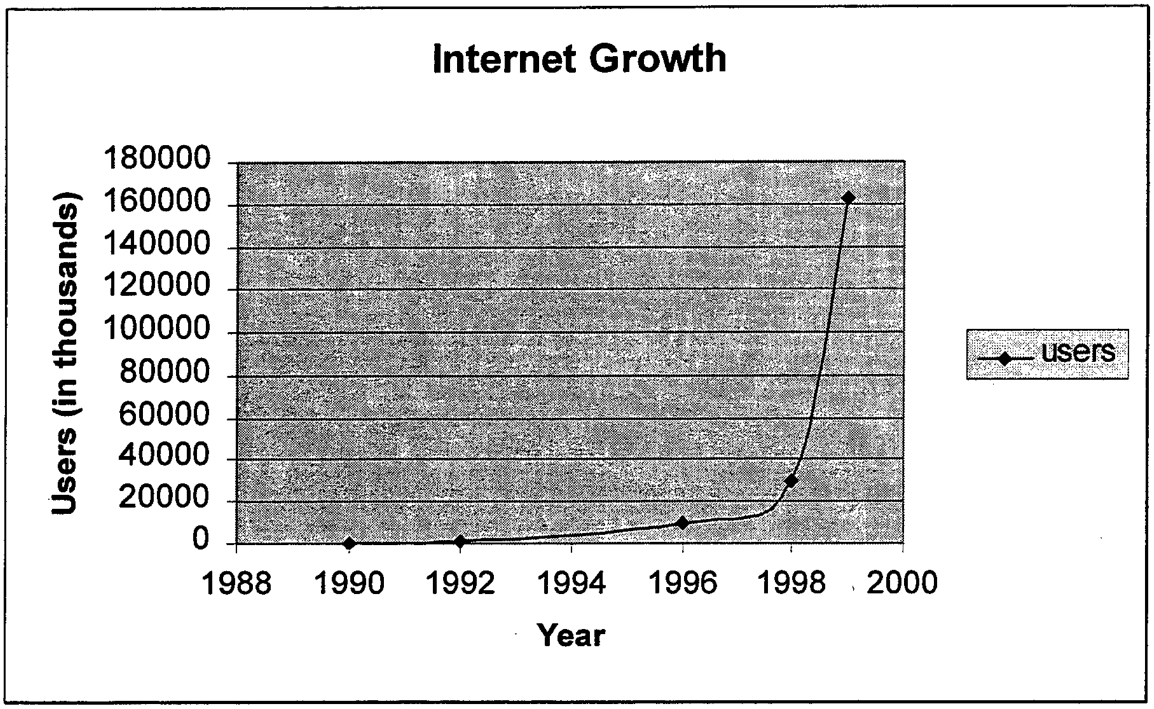

Figure 1. Growth of Internet Users.

4. Emerging Vulnerabilities

This level of worldwide interconnectivity has not come without a price. As our Nation – and the world – continues to move its critical infrastructure into cyberspace, the potential for exploitation by those interested in furthering their own agendas increases dramatically. Communications, commerce, banking, finance, entertainment, education, health services, and nearly all other aspects of our daily lives are inextricably tied to the information network realm. Even our Nation's defense information infrastructure (DII) is not exempt, with over 95 percent of military communications being routed over civilian links [Ref. 23]. This reliance on information technology is precisely the vulnerability targeted by cyberterrorists. And it is also the main reason why cyberterrorists may be capable of inciting a tremendous amount of fear and anxiety, without having to resort to physical violence.

C. DEVELOPING A WORKING DEFINITION FOR CYBERTERRORISM

In order to derive a working definition for cyberterrorism, all of the issues discussed above must be taken into account. This definition must address the act (or activity), the perpetrator, the target (or victim), the weapon (or medium), and the purpose (or intent). Several definitions have already been proposed for information terrorism and cyberterrorism, but we found most to be incomplete. However, the definitions proposed by Rod Stark [Ref. 24] and Mark Pollitt [Ref. 25] encompassed nearly all of these issues. The authors developed the following definitions, using their work as a foundation:

> *Cyberterrorism* is the purposeful attack or threat of attack by non-state individuals or groups against any portion of a nation's information infrastructure, accomplished by leveraging information technology, with the intention of influencing its society or government through fear and intimidation, for the sake of some political, social, or ideological objective.
>
> *Information infrastructure* refers to the underlying computer and telecommunications framework, including, but not limited to, information systems, computer systems, computer programs, and data.

1. Tools and Targets of Cyberterrorism

In order to leverage information technology, the cyberterrorist must use it as a tool or as a target. For example, if cyberterrorists blow up the computers used to control the flow of oil through a pipeline, with the intention of disrupting the supply of oil to a nation, they are using information technology as a target. If, on the other hand, they insert a computer virus into the same system, with the same intentions, then they are using it as a tool (as well as a target). While the direct target of a cyberterrorist attack can be digital or physical in nature, its ultimate goal is to influence or coerce through fear and intimidation. This is accomplished by causing – or threatening to cause – loss of life, injury, or the destruction or disruption of a nation's critical infrastructure, consisting of telecommunications, banking and finance, electric power, transportation, gas and oil, emergency services, and government services.

2. Conventional versus Information Terrorism

The distinguishing factor between conventional terrorism and information terrorism lies in the means by which the intended coercion is or may be accomplished. Conventional terrorism requires the use of actual or threatened physical violence in the pursuit of a political objective, to create a general climate of public fear and destabilize society, and thus influence a population or government policy. However, while physical violence can be a factor in information terrorism, it also includes the intentional abuse of an information system, network, or component, toward an end that supports a terrorist campaign or action. These activities may not necessarily result in direct physical violence to any person, while still inciting fear among the intended victims [Ref. 26]. Thus, without having to commit acts of physical violence, an information terrorist may still be able to achieve the intended results of coercion and influence.

3. Categories of Cyberterrorism

Information terrorism appears to fall into three of four broad categories, as suggested by Devost [Ref. 27]. He classifies these categories in terms of the weapon used and the intended target. The weapon used can be physical (such as a bomb) or digital/information-based (such as a computer program). The target can also be physical (such as a radio transmission tower) or digital/information-based (such as a computer database). An example of each of these categories is provided in Table 1. The first category (physical on physical) relates to "conventional" terrorism, while the remaining three categories can be considered information terrorism. [Ref. 28]

		TARGET	
		Physical	*Digital*
TOOL	*Physical*	(a) Conventional Terrorism (Oklahoma City bombing)	(b) IRA Attack on London Square Mile, 4 Oct 1992.
	Digital	(c) Hacker spoofing an air traffic control system to bring down a plane.	(d) Trojan horse in public switched network.

Table 1. Categories of Terrorism.

The category most commonly associated by the popular media with cyberterrorism is digital on digital (category d). The impact of these types of attacks is not due to violence, or the threat of violence, but rather, it is due to the disruption and potential chaos that they produce. This disruption can – and frequently does – lead to the requisite "state of intense fear" or anxiety described in the above definitions. Because of this, cyberterrorists do not have to resort to the use of physical violence (e.g., blowing up buildings or killing people). Instead, they can threaten with the disruption or destruction of a country's critical infrastructure.

While cyberterrorists have the capability to commit acts of violence through IW means (as suggested in category c), we found that the majority of the incidents to date have been of a disruptive nature. These disruptions were generally a result of the destruction or alteration of data, and merely served to antagonize or annoy the intended targets. Again, this is not to say that cyberterrorism can not encompass violent means, as well. There are numerous actual or potential scenarios in which a cyberterrorist act resulted or might have resulted in the serious injury or death of its victims. While specific details about actual incidents have been omitted due to their level of classification, current popular fiction is rife with examples of the destructive potential of cyberterrorism.

4. Impact of Cyberterrorism Attacks

The absence of violence in a cyberterrorist act does not make it any less dangerous. While the psychological and emotional impact resulting from this type of an attack may not be as significant to the victims as that resulting from a conventional terrorist act, the actual impact could be greater from a political, economic, or social perspective. This is due, in part, to the fact that a cyberterrorist act has the potential to reach (and, thus, affect) a much greater audience. An explosive device placed in a train station, for instance, can only directly affect those persons unfortunate enough to be caught in the blast (not accounting for the emotional toll on the population as a whole). However, a cyberterrorist attack has the potential to reach a much wider segment of the population in one single act.

D. THE THREAT OF CYBERTERRORISM TO AMERICA

The level of importance being given to countering this threat is evidenced by President William J. Clinton's address to the National Academy of Sciences on January 22, 1999. In his speech, the President issued a call to arms in the battle to "keep America secure for the 21st century," and discussed emerging threats to America's security "as we reach a new century." [Ref. 29] President Clinton announced major new initiatives to strengthen America's defenses against the emerging threats posed by biological and chemical weapons, and attacks to our critical infrastructure, computer systems, and networks. The proposed program will cost a total of ten billion dollars for fiscal year 2000. While the lion's share of this amount will be going towards "conventional" counter-terrorism security programs, nearly fifteen percent is being earmarked for the defense of our critical infrastructure, including power-generation systems, banking, transportation and emergency services, and telecommunications. This $1.46 billion investment – a forty percent increase over the previous two fiscal years – will help secure computer systems and networks that are potentially vulnerable to computer attack. [Ref. 30]

How can these systems be secured? This is the crux of the problem we face, as a result of our increased reliance on the information network realm. In order to address this question, we must first identify the critical infrastructure we are hoping to secure. It is not just our National Information Infrastructure that we are growing more dependent on. As more and more global telecommunications and information system consortiums are formed (such as Iridium, Teledesic, and INMARSAT), transnational boundaries begin to blur. Satellite communications, global positioning, and cellular communications are only a few of the areas that are being absorbed into this Global Information Infrastructure. As we continue to make use of (and rely on) the GII, it becomes increasingly difficult to provide an acceptable level of security for it.

The protection of our critical infrastructure has taken on a new urgency as our dependence on it increases and technology continues to advance at a blistering pace. In the following chapter, we describe the composition of this critical infrastructure and discuss its vulnerabilities. We provide an overview of the current "state of the practice," in terms of infrastructure protection, and discuss how the development and implementation of new technologies affects these practices.

III. PROTECTING THE INFORMATION INFRASTRUCTURE

A. DEFINING THE INFRASTRUCTURES

There is a growing concern within the U.S. Government that our Nation's infrastructures are becoming increasingly vulnerable to the threat of cyberterrorism. The primary reason for this increased vulnerability is the level of reliance and interconnectivity that has emerged between these infrastructures. While this interconnectedness has made it possible to provide more services to more people than ever, it has become nearly impossible to discern where one service ends and the other begins. But exactly what are these infrastructures and how are they interrelated?

1. The Critical Infrastructure

In their 1997 report, the President's Commission on Critical Infrastructure Protection (PCCIP) defined "infrastructure" as a "network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services… They are the lifelines of the Nation." [Ref. 31] They listed the critical elements of this network – the Critical Infrastructure – as *transportation*, *oil and gas production and storage*, *water supply*, *emergency services*, *government services*, *banking and finance*, *electrical power*, and *information and communications* infrastructures. Of these, the information and communications infrastructure has emerged as the most essential and pervasive component. Every other critical infrastructure element relies on the information infrastructure to transfer data, provide access to services, etc.

The importance of our critical infrastructure (and, in particular, our NII) is best illustrated by the following excerpt from the PCCIP report:

> Reliable and secure infrastructures are... the foundation for creating the wealth of our Nation and our quality of life as a people. They are fundamental to development and projection of the military power that enables our diplomacy to be effective. They make it possible for us to enjoy our inalienable rights and take advantage of the freedoms on which our Nation was founded. Certain of our infrastructures are so vital that their incapacity or destruction would have a debilitating impact on our defense and economic security. [Ref. 32]

2. The Information Infrastructure

The phrase "information infrastructure" has an expansive meaning. Information infrastructure generally refers to "the information resources, including communications systems, that support an industry, institution, or population. Examples are a corporate information infrastructure, the financial information infrastructure, the defense information infrastructure (DII), the national information infrastructure (NII), and the global information infrastructure (GII)." [Ref. 33] An information infrastructure includes more than just the physical facilities used to transmit, store, process, and display voice, data, and images. It encompasses a wide and ever-expanding range of equipment, including cameras, scanners, keyboards, telephones, fax machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, optical fiber transmission lines, microwave nets, switches, televisions, monitors, printers, and much more. There is practically no part of the critical infrastructure that does not make use of one or more of these systems.

B. EFFECTS OF INFRASTRUCTURE INTERDEPENDENCE

1. Cascading Failures

How does the level of interconnectivity between these critical infrastructures get leveraged into increased vulnerabilities? The main reason for this lies in the nature of their reliance on each other. The PCCIP reported that these infrastructures "may be vulnerable in ways they never have been before," primarily due to their mutual dependence and interconnectedness. This collective interdependence provides great opportunities, as well as dangerous vulnerabilities. There is a very real risk of "cascading technological failure," resulting in a "cascading disruption in the flow of essential goods and services." [Ref. 34] In other words, if one of these vital infrastructures collapses, there is a strong possibility that others will follow. Computerized interactions within and among infrastructures have become so complex that it may be possible to do harm in ways we cannot yet conceive.

2. Increased Reliance

It is precisely because of these complex interactions that the NII has become the most crucial element of our critical infrastructure. As technology advances, the level of automation and connectivity continues to increase, as does the level of interdependence. This, in turn, creates a greater potential for disaster resulting from attacks on the information infrastructure. As Denning [Ref. 35] notes:

> Computers and telecommunications systems... support energy distribution, emergency services, transportation, and financial services. Could the entire public telecommunications network be shut down for weeks? If so, what would be the consequences? Over 95% of military communications are routed over civilian links, so an attack of this nature would affect military operations as well as civilian activity.

Advancements in technology also provide new and more sophisticated tools for these attacks, further compounding the problem.

3. Department of Defense Issues

As the military becomes increasingly reliant on the civilian information infrastructure for communications, intelligence, and command and control, the issue of how to protect, defend, and, if necessary, restore these systems takes on a new urgency.

To further compound this problem, there is a significant trend towards globalization in the commercial sector. Due, in part, to the ubiquity of the Internet, increasing numbers of corporations – particularly in the areas of information technology and telecommunications – are merging to form pan-national consortiums. This trend poses new problems for our National Defense. How can we develop an acceptable level of trust and reliance in a system that is essentially out of our control (e.g., a cellular communication service owned/operated by another country)? How can we conduct offensive information operations (IO) against the NII of another nation, when it may be directly tied to the GII on which we must rely? In this New World of the 21st century, we may find ourselves protecting portions of the GII, even as our adversaries are using it against us.

The DoD's trend of increasing reliance on the commercial sector is not limited to the telecommunications arena, either. The DoD is investing a substantial amount of their research and development budget on the use of Commercial-Off-The-Shelf (COTS) software and hardware. For instance, through their recent IT-21 initiative, the U.S. Navy has implemented Microsoft Windows NT and Office 97 as their standard operating system and office productivity suite, respectively. The result of this approach is that the DoD must rely on the commercial sector to provide many of the security measures necessary for the protection of its information infrastructure.

C. COUNTERING THE THREAT

How can we protect our information infrastructures from this growing threat? Is it even feasible to attempt to safeguard and secure such a complex and interconnected "system of systems?" Indeed, it is not only possible, but also necessary. However, while many information resources can be reasonably hardened against all but the most sophisticated attacks, 100% security is generally considered neither possible nor worth the price. As Denning states, "The goal is risk management, not risk avoidance at all cost." [Ref. 36] The rate at which technology continues to advance makes it even more unlikely that any one solution will be adequate to provide all-around protection.

1. Categories of Defensive Mechanisms

There are numerous mechanisms and tools that can be employed to provide for the protection and defense of our information infrastructures. These mechanisms have been found to fall into one (or more, since they are not mutually exclusive) of the following six categories: prevention, deterrence, indications and warnings, detection, emergency preparedness, and response. Table 2 lists these categories and provides some examples of the classes of mechanisms associated with each. [Ref. 37]

2. Implementing Defensive Measures

Until fairly recently, the commercial sector had not truly focused its efforts on developing and implementing robust security capabilities within its products. The main reason for this is that, up until the late 1980's, there was no real need for these features, since the level of interconnectivity was minimal. With the explosive growth of the Internet and the emergence of electronic commerce, the demand for strong security and system reliability has grown. The main impetus for this has been the evolution of business on the Internet. As more and more businesses and consumers turn to the Internet to engage in commerce, the issue of security has come to the forefront.

a. Prevention

The first approach taken to implement security – and one that is still very popular today – relied almost exclusively on elements from the prevention category. This approach was based on building "virtual walls" around a system to protect it from external threats. In creating this virtual perimeter, the goal is to isolate unauthorized users from accessing a particular system. In order for this type of security to be effective, a delicate balance between usability and protection must be struck. If a system has too many barriers, it becomes impossible to use; if it does not have enough, it becomes too vulnerable. Thus, this approach is essentially a compromise between ease of use and security.

CATEGORY	PURPOSE	CLASS OF MECHANISM
Prevention	Serves to keep an attack from occurring in the first place.	Information hiding, authentication, access controls, and vulnerability assessment.
Deterrence	Seeks to make an attack unattractive, but not necessarily prevent it.	Laws and the threat of criminal or civil penalties.
Indications and Warnings	Aims to recognize a potential attack before it occurs or during the early stages, so that other measures can be taken to avert the attack or diminish its effect.	Collection of historical information about attacks and analysis of trends.
Detection	Has a similar objective to I&W, but generally refers to the use of monitors to recognize an attack after it has started.	Audit logs, system scans, and other network monitoring tools.
Emergency Preparedness	Refers to the capability to recover from and respond to attacks after they occur.	Backups, site mirroring, redundant systems, and implementation of an information dissemination capability.
Response	Refers to actions that are taken after an attack occurs.	Containing and recovering from damages and hardening defenses.

Table 2. Categories of Defense Mechanisms

Most prevention mechanisms are primarily geared towards developing a "fortress" model of security, building a virtual wall around the system. Tools such as firewalls, login programs, and gateways were developed for access control. Encryption, which continues to be the subject of controversy within the U.S. Government, is used to hide information, as well as provide authentication (through digital signatures). Even many of the vulnerability assessment techniques focus only on the "outsider" threat. Unfortunately, this leaves the door wide open to insider attacks, which account for sixty to eighty percent of all attacks. [Ref. 38]

b. Detection

To complement these preventive tools, numerous detection mechanisms were utilized. These included logs, audit trails, and other record-keeping tools that provide a "post-attack" picture of a particular attack or intrusion event. As in a physical crime scene, these tools yield some insight as to the extent of the damage caused by an attack, the methods used to conduct the attack, etc. They can be used to monitor both insider and outsider activities, helping to close some of the gaps described above. However, the purpose of these detection mechanisms is not to stop an attack while it is underway, but instead to use the information gained to prevent similar attacks in the future. Unfortunately, not all attacks leave clear trails, and some may leave none at all.

c. Barrier Defense

These two concepts – prevention and detection – have been the focus of industry's and government's approach to providing security for our information infrastructures. The majority of the COTS security products currently on the market are designed to provide a barrier defense. Implemented as both software and hardware solutions, these products have met with varying degrees of success. Unfortunately, no single solution has ever been sufficient (aside from unplugging the system), and any flaws and vulnerabilities are quickly discovered and exploited by attackers. The ability to counter these attacks or threats of attack will require a significant shift in how we currently do business. Fortunately, this change is already underway, both in government and industry.

3. A New Approach

The problem is now being approached from a different perspective than had been considered standard practice only a few years earlier. Before, the issue was whether the systems were sufficiently secure. The *new* approach deals with whether we have an acceptable level of "information assurance." The concept behind this approach is to attempt to address all areas of concern, in terms of protecting and defending an information infrastructure. Whereas *security* tends to deal only with the protection of a system, *assurance* relates to a much broader set of issues.

a. Information Assurance Defined

Information assurance – a term that has only recently come into use – is described in Joint Publication 3-13 as follows:

> 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. [Ref. 39]

For there to be information assurance, a system must be able to operate in a "trustworthy" mode, even when it has been compromised. Much like the premise behind the original Internet (DARPANET), the system must be able to "heal itself" (by restoring or rerouting), and continue to provide an acceptable level of security and reliability to the user. There must be a certain *level of assurance* associated with the information being used. But, how is this level of assurance obtained?

b. Defense in Depth

In order to provide information assurance, the concept of "defense in depth" must be implemented. Defense in depth relies on the layering of defensive mechanisms at all levels, from the individual user to the GII. This approach is certainly not new; examples of its use abound in military history. The idea of setting up a layered defense was central to much of the warfare conducted during the middle ages. Clearings (kill zones), moats, drawbridges, keeps, crossbows, archers, swordsmen, and postern gates provided medieval castles with multiple redundant ways of countering attackers [Ref. 40]. The same concept is used in modern warfare, where sensors (e.g., satellite-based cameras) and weapons (e.g., missiles, aircraft, etc.) can be configured to provide a layered defense. By applying defense in depth to information systems, we are able to better manage the risks to our critical infrastructures, creating trustworthy systems from untrustworthy components.

Although newer and more powerful prevention mechanisms continue to be developed, the level of complexity resulting from the tremendous amount of interconnectivity that exists in today's Internet makes it impossible to identify and isolate all possible flaws and vulnerabilities. As the infrastructure grows, its interactions become more and more complex and difficult to analyze. Thus, it is impossible to set up a barrier against every possible attack. As noted earlier, doing so would render the system unusable. It is therefore necessary to implement defense in depth.

Countering the threat of cyberterrorism requires that information infrastructures – from the corporate level to the global level – operate with a minimum level of information assurance. For example, a cyberterrorist might plan an attack on New York's central power grid during the holiday season in an attempt to cause a major airline disaster during the busiest time of year. With an appropriate level of information assurance, cyberterrorists would have to first overcome several layers of preventive measures (i.e., firewalls, authentication programs, etc.). Then, if they were able to do so, their attack would simply result in one of several redundant or back-up systems coming on-line, with minimum impact on the critical infrastructure of the city. Also, the ability to continue to operate safely and with a minimum of disruption can not depend on the method of attack used. For information assurance to be effective, the impact must be the same whether the attack was physical (e.g., a bomb) or digital (e.g., a computer virus) in nature.

4. Initiatives to Counter Cyberterrorism

Without an acceptable level of information assurance, any cyberattack has the potential to not only harm military operations, but also disrupt banking and finance, create power shortages, interrupt transportation needs and crash entire communications networks. What is being done by the Federal Government and private sector in response to this threat? There are a number of public and private initiatives currently underway, designed to counter or mitigate the threat of information terrorism. [Ref. 41]

a. CERT Coordination Center

CERT/CC studies internet vulnerabilities, provides incident response services to sites that have been the victims of attack, publishes a variety of security alerts, researches security and survivability in wide-area networked computing, and develops information to improve network security. CERT/CC is widely known as a vital and integral organization dealing with computer security.

b. National Infrastructure Protection Center

Attorney General Janet Reno announced the National Infrastructure Protection Center in February 1998. It replaced the Computer Investigations and Infrastructure Threat Assessment Center and involves the intelligence community and the military. It was formed in response to concerns about the safety of national computer systems and charged to detect, deter, warn, respond to, and investigate unlawful acts involving intrusions and other threats against vital infrastructures. The National Infrastructure Protection Center uses several intelligence and law enforcement agencies to conduct investigations into threats to the Nation's critical infrastructure. The Department of Justice (DOJ) itself is seeking increased funding for fiscal year 2000 to protect government infrastructure and to improve internal information technology operations.

c. The Center for Intrusion Control

The Center for Intrusion Control will be modeled on the Centers for Disease Control and will be able to swiftly mobilize resources and personnel to fend off an organized cyberattack. It will identify and respond to serious cyberwarfare threats such as infiltration of financial institutions or other critical industries. It is not yet known whether this center will interact with the National Infrastructure Protection Center. Additionally, the status of the funding for this center remains uncertain.

d. The SHADOW Project

Directed by Steven Northcutt, the SHADOW Project is the U.S. Military's on-going effort in the development of automatic intrusion detection systems.

e. The President's Commission on Critical Infrastructure Protection

The President's Commission on Critical Infrastructure Protection (PCCIP) was formed to advise and assist the President of the United States by recommending a national strategy for protecting and assuring critical infrastructures from physical and cyber threats.

f. The Critical Infrastructure Assurance Office

Announced by President William J. Clinton in May 1998, the CIAO will facilitate the creation of a national plan to protect the services that we depend on daily: telecommunications, banking and finance, electric power, transportation, gas and oil, emergency services and government services. Critical infrastructure assurance is a new capability that resides right at the point where our national security and economic security merge. This initiative will require a new level of commitment to partnership between the public and private sectors, specifically in the areas of policy formation and information sharing.

g. The Information Systems Security Organization

The Information Systems Security Organization of the National Security Agency (INFOSEC) has historically protected information critical to National Security, and they help protect communications and information systems of the Department of Defense and other federal agencies. INFOSEC is primarily focused towards information assurance.

h. *CSIS Task Force on Information Warfare and Security*

The Center for Strategic and International Security (CSIS) Task Force on Information Warfare Security is a government-industry partnership addressing the threats to, and interdependencies of, our most critical infrastructures. They address a range of legislative, technological, and organizational recommendations and processes to better protect our infrastructures. Task force findings can be found in the recent publication *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo* [Ref. 42].

i. *Department of Defense Initiatives*

The Department of Defense (DoD) has not taken these threats hands down. For "Eligible Receiver," a DoD information warfare exercise conducted last year, a team of 30 to 35 hackers was hired to see how far they could penetrate government and critical infrastructure systems. Over a period of three months, these hackers used off-the-shelf hardware, software, and hacker scripts downloaded from the Internet to attempt to hack these systems. The DoD was shocked to find its systems "surprisingly vulnerable" to attack, especially since most government communication is conducted over commercial channels [Ref. 43]. Michael Vatis, the chief of the National Infrastructure Protection Center, sees the DoD as the "big banana, the final exam" [Ref. 44] for hackers and this is the prime target for individual hackers that want to test their skills.

IV. CYBER FI

A. OVERVIEW

At the Naval Postgraduate School (NPS) in Monterey, California, a team of graduate students and faculty members assembled a working group to conduct research on the cyberterrorism threat and its impact on the National Information Infrastructure and the Department of Defense. This group, known as *Cyber Fi*[1], is made up of graduate students with a common interest in computer security, cyberterrorism, and information warfare. Cyber Fi's objective is to identify areas of improvement in our ability to detect, protect against, contain, neutralize, mitigate the effects of, and recover from cyberterrorism attacks. Based on the information presented in lectures and classes at NPS, the group is convinced that cyberterrorism poses a very real and imminent threat to the security of the United States.

B. BACKGROUND

> The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems. [Ref. 45]

Advances in information technology have provided critical infrastructures with improvements, allowing systems to become increasingly automated and interconnected. As discussed in the previous chapter, these advances have also brought about an increased reliance on our information infrastructure, leading to new and unforeseen vulnerabilities. Terrorists and transnational criminals are rapidly becoming aware of these vulnerabilities, and are exploiting them through the power of information warfare.

[1] Credit for this term goes to Professor John Arquilla.

The explosion of the Internet has provided a means by which a cyberterrorist can wreak havoc from anywhere in the world through the use of a simple home computer.

In order to mitigate or eliminate the threat of cyberterrorism to our information infrastructure, it is imperative that the potential effects of such an attack be understood. Research in this area has been somewhat limited, particularly in terms of large-scale vulnerability testing. Although exercises such as Eligible Receiver are invaluable to this type of research, they are (unfortunately) few and far between. Such attacks would have severe consequences for the Department of Defense, which has become dependent on computers and communications infrastructure.

C. THE GENESIS OF CYBER FI

1. Developing the concept

The Cyber Fi working group was conceived as a result of thesis research conducted by Maj Fritz Doran, a graduate student in the Computer Science (CS) department at NPS. A quest for thesis sponsors led him to the desk of Capt Jim Powell, the military chair of the Information Warfare Department. After Maj Doran told him what he was interested in, Capt Powell suggested a co-advisor team of Timothy Shimeall and John Arquilla.

Prof. Shimeall, an associate professor in the CS department at NPS, has focused much of his research on computer security issues. His recent sabbatical at the CERT Coordination Center (CERT/CC) at Carnegie-Mellon University had made him very familiar with not only the various methods of attack that hackers were currently using, but also with the potential for damage to the Nation's critical infrastructure inherent in such attacks. Prof. Arquilla, an associate professor in the National Security Affairs

(NSA) department at NPS, has conducted extensive research on the topic of terrorism in the information age. He has published numerous articles (beginning around 1993 with "Cyber War is Coming!") warning that this threat is indeed very real.

The professors and Maj Doran agreed that nothing short of a serious incident (such as a major U.S. city's infrastructure being successfully attacked, or a military exercise or operation being affected by a cyberterrorist attack) would convince all doubters of the validity of this threat. They began exploring options on how to provide convincing evidence of this fact without hampering or destroying either civilian infrastructure or military capabilities.

A follow-on discussion between Maj Doran and Prof. Shimeall solidified the idea that a common interest was cyberterrorism, and that there is a need to prove that cyberterrorism is a real threat in today's increasingly computerized world.

2. Information Warfare Ghosting

Through their discussions on information warfare attacks and simulations, and on Prof. Shimeall's work at the CERT/CC, Maj Doran and Prof. Shimeall evolved the concept of "ghosting" an IW attack against either civilian or military targets. While the specifics of ghosting an IW attack are more fully addressed in Maj Doran's thesis [Ref. 46], "ghosting" can be broadly defined as follows:

> Information Warfare Ghosting is a scaleable attack upon the computers and network infrastructure of either an operational or simulated network. [Ref. 47]

IW Ghosting is scaleable in that the levels of attack range from completely passive to highly active. These levels fall into seven categories.

a. Hypothesis

At the low end, a completely passive ghost attack would involve knowing about either an existing or planned infrastructure or military operation and hypothesizing about methods of cyberattack. Also, open source research on the potential for success of such attacks would be conducted.

b. Informed Hypothesis

At the next level, the attacker would have available to him or her some specifics about the target. However, actions would still be limited to hypothesizing about potentially successful attacks. The difference would be that the attack could now focus on specific aspects of the target infrastructure.

c. Simulation

The attacker not only knows specifics about the target, but also has the resources to set up a simulation of the target system. Then, using the results of (b.) above, the attacker can actually see what the potential results of attacks would be and perhaps focus on low-risk, high-payoff attacks.

d. Passive Observation

At this level of ghosting, the attacker observes the actual working infrastructure that is the target. This observation could take place surreptitiously (as in spying) or permissively (as a trusted or semi-trusted insider) to gain further knowledge of the target. As before, the attacker (or attackers) could then use (b.) and (c.) above to distill the number of potential attacks down to the ones most likely to succeed.

e. Active, Non-intrusive Attack

At this level, an attacker (with or without the benefit of information or observation) attempts to attack the target with the goal of penetrating the network. If this attack is successful, the intruder only views available information and/or maps the network.

f. Active, Non-hostile Intrusion

The attacker at this level has the express intent of "leaving a placeholder" to demonstrate to the attacked party (perhaps in real-time) that their network has been penetrated. Nothing is intentionally deleted, and intrusion is limited to markers such as "you have been penetrated" warnings on web pages, or e-mail messages from key users to themselves (perhaps with a copy to the net administrator) stating that their e-mail has been penetrated.

g. Active Takedown

This is the most extreme and intrusive IW ghosting attack and involves the attacker actively trying to disable some or all of the network infrastructure. At this level, "the gloves are off" and the attacker is free to do whatever he or she can think of to bring down the network.

3. The Cyber Fi Profile

What if a group of disgruntled, technically-oriented current and/or former military officers were to get together, pool their knowledge and expertise, and conduct a cyberterrorist attack against a U.S. military operation? Their motivation could be:

- Profit - selling their services to the target of the U.S. attack;
- Ideology - opposing what they deem an unjust aggression by the U.S. against a country or organization;

- Old-fashioned revenge for perceived mistreatment at the hands of the U.S. government; or

- A combination of the previous three.

Whatever their motivation, such a group would be a formidable opponent for defensive IW personnel, and would be representative of groups probably in existence in the world today.

Using this scenario as the profile for their Cyber Fi group, Maj Doran and Professors Shimeall and Arquilla began making plans to conduct a ghost attack against a yet-to-be-determined target.

4. The Target

As the discussions continued, the players identified possible opportunities for the Cyber Fi group to pursue. The local newspaper, The Monterey County Herald, had been running a series of articles about the upcoming Marine exercise that was to be conducted in Monterey in the March timeframe. Called Urban Warrior (or UW), this "experiment" (in reality, an advanced concepts demonstration) called for a scenario in which a terrorist organization had seized a weapon of mass destruction (WMD) and had the potential to use it. A host country, friendly (or, at least, neutral) to the United States, had requested assistance from the U.S. military in getting rid of this unwanted group of terrorists on their soil. The planners of Urban Warrior intended to use this framework as the basis for their demonstration During the discussion of UW, the group realized that this was a golden opportunity to pursue the idea of ghosting an IW attack against a U.S. military exercise that was to occur literally on the doorsteps of the Naval Postgraduate School!

5. The Team

Maj Doran and Professors Shimeall and Arquilla decided to take advantage of this opportunity. In discussions with other CS and Information Technology Management (ITM) students, Maj Doran found that many people were doing thesis work in closely related fields, such as signals intelligence, hacking toolkits, wireless LAN security, and satellite communications security.

Maj Doran and the two professors formulated a plan for putting together a team of such students (already familiar to each other) to conduct an exploration into what such a team might be capable of performing. This was the origin of the Cyber Fi team concept. They identified a diverse group of students whom they felt might be interested in participating in Cyber Fi, based on their military specialties, thesis topics, or expressed areas of interest. The final composition of the Cyber Fi team, and each member's area of expertise, is listed in Table 3.

For the most part, these team members were already well acquainted and were aware of many of each other's strengths and weaknesses. Additionally, most members were intimately familiar with military doctrine concerning amphibious landings, which was to be the main showpiece of Urban Warrior. Maj Ogren, Lt Langevin, and Maj Doran adopted aspects of Cyber Fi as a main thesis, while the other team members made a commitment to support the team's efforts as much as possible. With this team and this idea, Cyber Fi began their efforts to prove that the cyberterrorism threat was alive, well, and simply waiting for the right team to demonstrate it.

NAME	SERVICE	OCCUPATIONAL SPECIALTY	THESIS TOPIC OR ROLE	COMMENTS
John Arquilla	NPS Faculty	Irregular Warfare	Co-Advisor for	Choi/Doran
Tim Shimeall	NPS Faculty	Internet Security	Co-Advisor for	Choi/ Langevin/ Doran/Ogren
John Osmundson	NPS Faculty	Software Engineer	Co-Advisor for	Ogren/ Langevin
Fritz Doran	USMC	Data Comm	Cyberterror	Team Leader
Joel Ogren	USMC	Data Comm	Cyberterror	Satellite expert
James Langevin	USCG	Info Tech	Cyberterror	Security expert
Rod Choi	USMC	Infantry	Hacker Toolkit	Doctrine expert
George Greenway	USN	Cryptology	SIGINT Collection	
Wayne Collins	USMC	Data Comm	Wireless Networks	
Kay Holt	USN	Cryptology	Info War	Insider (Reservist)
Kristen Tsolis	Civilian (MIIS)	Management	Social Engineer	
Marc Sanders	USCG	Info Tech	WWW Design	Associate of group

Table 3. Composition of Cyber Fi.

D. THE SCENARIO

A middle-aged man in a nondescript trench coat, sipping coffee at a Belgrade café's outdoor table, fires up his cellular phone. While appearing to idly flip through the pages of a local newspaper, he enters the international access code and phone number for a phone in Monterey, California. Within milliseconds, his voice signal is converted from analog to digital format, compressed, encrypted and interleaved, then transmitted in rapid-fire data bursts using spread-spectrum techniques to protect the privacy of his call. The call is seamlessly handed off from cell to cell until reaching the cellular network's main base. There, it is decoded and delivered to a landline telephone network, then uplinked to a low-earth-orbit (LEO) satellite communications network. Bounced from satellite to satellite, it zips across the Atlantic Ocean toward the East Coast of the U.S., where it is downlinked to another landline telephone service and connected to the called party.

Only seconds after being sent, the clandestine message is heard: "Hello, the U.S. military is landing helicopters inside the grounds of the U.S. Embassy. I'm taking a taxi to the airport before the shelling begins again."

Back in Monterey, a small group of cyberterrorists goes to work. A large amount of background work has already been done over the past 12 months. All the information that they've used has been collected from "surfing" a host of web sites on the Internet, conducting social engineering in and around military bases, and conducting a variety of hacker attacks on selected web sites. At this time, the group knows with high certainty what military units are involved in the ongoing operations in Belgrade, Yugoslavia. They also know their basic tactics, techniques, and procedures as well as the IP addresses for the servers that these units are using for their own Internet connection.

The assault unit going into the Embassy has been equipped with the latest Commercial-Off-The-Shelf (COTS) technology, including small handheld radios, a Compaq^{TM} Libretto palm top computer, and Wavelan^{TM} wireless technology. The cyberterrorists in Monterey quickly hack into the bookmarked site over an IP address that was mapped months ago. They trigger the Trojan Horse that was inserted into the site earlier, which introduces a random error in computations of a popular software package used on the Libretto.

The U.S. Service members at the Embassy begin receiving a constant stream of small arms fire along with an occasional Rocket Propelled Grenade (RPG). They call for a fire mission using the software on the Libretto. The fire mission is communicated through their network to a U.S. Navy aircraft carrier sitting off the coast, and immediately an officer on board assigns a pair of F-18s who are airborne waiting for tasking. Their job: taking out the enemy forces on the ground. The F-18s punch in the data to their smart weapons, using the geo-positioning data provided in the fire mission from the Embassy forces. The target is identified, locked, and fired upon. Minutes later, multiple explosions rock the downtown area, where the historic public library has been turned into a pile of rubble. Meanwhile, back at the Embassy, the U.S. forces continue to receive fire from an enemy that wasn't touched by the F-18s, who just destroyed a target 5 miles away.

Welcome to the world of cyberterrorism.

V. THE URBAN WARRIOR EXPERIMENT

A. THE MARINE CORPS WARFIGHTING LAB

1. Overview

General Charles C. Krulak, the Commandant of the Marine Corps, established the Marine Corps Warfighting Laboratory (MCWL) in October 1995. It is located at Quantico, Virginia, and is part of the Marine Corps Combat Development Command (MCCDC).

2. Mission

MCWL's mission is to serve as the focal point for refinement of future warfighting capabilities. To this end, the Lab develops tactics, techniques and procedures, and evaluates advanced technologies that create or enhance future warfighting capabilities. It also integrates tactics, techniques, procedures and advanced technologies into the Marine Corps Combat Development System.

3. Concept-Based Experimentation

New warfighting capabilities are developed through a process called concept-based experimentation. A concept is developed by MCCDC that may improve future warfighting capabilities. Required warfighting capabilities to support those concepts are identified, analyzed and refined through wargaming, complemented by advanced technology if necessary, and then evaluated through experimentation to determine warfighting relevance.

This experimentation usually yields three results. The capabilities either work, don't work, or need further refinement. If a capability works, it is integrated into the Combat Development Process at Quantico. If it fails – not every idea that looks good on paper works in the real world – it is discarded. Failed experimentation is, in itself, a success. If a capability doesn't work but shows promise, it is refined for further experimentation. [Ref. 48]

4. The Advanced Warfighting Experiment

The Marine Corps Warfighting Laboratory developed a five-year program called the Advanced Warfighting Experiment (AWE). AWE's mandate is to exploit information technology opportunities, and develop innovative solutions to address technology gaps in a layered defense. The AWE's seek to leverage critical warfighting concepts and general technological bases that show future potential. [Ref. 49]

B. THE URBAN WARRIOR AWE

The Urban Warrior Advanced Warfighting Experiment was developed as a subset experiment to examine new concepts, tactics, techniques, procedures, and technologies to meet the challenges of conflict in urban environments.

An excellent overview of the framework for Urban Warrior is summarized by Wood [Ref. 50] in the following statements:

> Urban Warrior...begins with an assessment of future context and what conditions may lie ahead. The Marine Corps Warfighting Lab translates that context into concepts for employing forces. In turn, the concepts are broken down into essential capabilities. These are the grist for the Urban Warrior series of experiments. Reflecting this logic, the Urban Warrior Conceptual Experimental Framework presents the urban warfare concepts and enabling capabilities that we believe should guide experiment-based development of naval expeditionary operations on the urban littoral.

This framework also addresses technology, as follows:

> As we prepare to embark on joint experimentation, the premium on clear thinking and rigorous analysis grows. Choosing intelligently demands an understanding of future context and concepts. These give us logical backboards against which to bounce various technology alternatives and make operationally sound choices.

1. Mission Drive

The Advanced Warfighting Experiment was created to test and evaluate potential system level solutions into a set of integrated comprehensive solutions to military issues. Once a solution is determined to be viable, the systems are engineered into the overall architecture. Upon incorporation into the overall architecture, the entire architecture must be reevaluated to determine the impact of the modifications prior to deployment. These newly integrated systems can't be deployed haphazardly. The architecture, system, and management levels must all be clearly understood in order to put these systems together, and there must be an understanding of what you have once you've done this.

2. Current Focus

There have been significant accomplishments in the research conducted in the information survivability area, including enhanced barrier protection in the prevention area and innovative methods in intrusion detection.

The realm of information technology operations (ITO) is changing focus to the world of information assurance. This provides the ability to take technologies out of the information systems programs, and start integrating them into a comprehensive architecture. The next phase for the ITO would be a program based on inherent survivability. This research area has recently begun to focus on the global intrusion detection problem and intrusion tolerance.

C. URBAN WARRIOR EXPERIMENT RESULTS

1. The Monterey Scenario

The scenario for the Urban Warrior Experiment, which took place in Monterey, California, was developed to test the Marines' ability to deal with terrorist threats, provide disaster assistance, and simulate civil-military relations in an international setting.

The scenario depicted Monterey as a city in a fictional, sovereign international country that had requested support from the United States. The Special Purpose Marine Air-Ground Task Force (Experimental) (SPMAGT-X), located aboard an off-shore amphibious ready group (ARG), landed Marines to help stabilize the situation and search for individuals who may be manufacturing a (simulated) biological weapon of mass destruction. The scenario called for the initial force to be reinforced by the Chemical-Biological Incident Response Force (CBIRF), a Marine unit from Camp Lejeune, N.C., created specifically to respond to the threat of chemical and biological weapons.

2. Focusing on the Urban Environment

The Marine Corps' top minds foresee a majority of the conflicts and other military interventions in the future taking place in the canyons and peaks of urban terrain, perhaps the most difficult and chaotic region to overcome. As LtGen John Rhodes, commanding general of the Marine Corps Combat Development Command, has stated:

> It was much easier when we just had bad guys and good guys... today there's far less certainty in regards to the where, when, how and why [of combat]. [Ref. 51]

To better prepare the Corps for such challenges in the urban environment, the Marine Corps Warfighting Lab has dedicated a third of its five-year experimentation process to testing new tactics, equipment, and philosophies in this unpredictable terrain. "Urban Warrior" is the second phase in the Lab's effort to ready Marines for combat in the next century.

3. Cyber Fi's Analysis

As described in the previous chapter, Cyber Fi's involvement was intended to include observation of the Red Cell efforts, passive signals collection (SIGINT); modeling and simulation of the UW network architecture (allowing active network intrusion efforts on the simulation LAN); and passive collection of wireless LAN signals during the experiment. The late entry of the research team into the experiment limited our participation to passive monitoring. Nevertheless, a number of salient points were discovered.

a. Testing

While Cyber Fi felt that the Urban Warrior Experiment did not provide a thorough test and evaluation of the many new technologies involved, the authors understand the purpose was more akin to a "proof of concept" for these technologies. It would have been impossible for the planners to incorporate full red-teaming activities, given the constraints they had to work with. If the Information Warfare red team had been given full latitude in their attacks, Urban Warrior would have ground to a complete halt, and none of the other new technologies being looked at could have been evaluated. However, it is of utmost importance that the results be considered in this light; that is, these technologies proved to be viable (or not) only in a benign, controlled environment.

The only decision that should be made based on Urban Warrior is to discard those systems that did not prove to be effective. Those that seemed to have operational value MUST be experimented with further before bringing them on-line. Although this may seem to lengthen the development and acquisition process somewhat (a concept DoD is trying to get away from), it is necessary to ensure that the systems being endorsed for battlefield use will indeed be of real value to the warfighter. These systems will have to be tested and evaluated in much more rigorous conditions, facing red teams that are being given sufficient leeway to pose a significant and realistic threat.

b. Technology Integration

The integration of emerging technology must be consistent with sound security testing used with current technology. How should this testing be accomplished? The effectiveness of "red teaming" or "scrimmaging" has long been known. From military units, to sports teams, to professionals, practicing for an event using a realistic opponent is invaluable in determining whether your strategy for success is valid. In terms of information technologies, the best way to find your system's vulnerabilities is to actively attack it, in a realistic operational environment.

The Cyber Fi group encountered this situation during Urban Warrior. One of the new technologies being tested was the End User Terminal (EUT), and their vulnerabilities in terms of sniffing, spoofing, and Denial of Service (DoS). The systems must be tested in much more rigorous manner, particularly in terms of its human-interface interaction.

If the system is rendered inoperative or compromised, how can the information be disseminated to the users? What measures can the users take to ensure the authenticity of the information they are receiving? To what degree can the users troubleshoot the equipment in the field? What are the users doing to ensure a certain level of COMSEC and COMPUSEC in the field? If an adversary intrudes upon the network via wireless means, can this intrusion be detected and its effects mitigated somehow? What are the effects of such an intrusion on the system, both tactically and operationally? The only way to develop appropriate contingencies to these and a myriad other situations is by thoroughly testing and experimenting with the technologies in a realistic setting.

As a caveat, it is important to note that, because of its inherent complexity, red teaming and vulnerability assessments will not find *every* possible weakness in a typical information system. However, if even a small percentage of these vulnerabilities are discovered and mitigated, the system will be that much more reliable and effective on the battlefield. By developing contingencies for these vulnerabilities, many others that may arise during actual operations may be handled more effectively. Red teaming will be discussed further in Chapter VI.

c. Parallel Growth

Careful consideration must be given to balance the integration of new technology. When developing software, the "hack and patch" technique will never find all the vulnerabilities in a system. Many in the industry assert that you can't build security into a system after the fact; it must be part of the original design. This said, it is unlikely that organizations would be able to obtain COTS systems that meet their security needs out of the box. It is even more improbable that these systems could later be modified to fully meet these requirements.

While this gives a fairly grim outlook on the security of systems, it is nothing new: many experts assert that no system can be built that is completely secure.

However, if organizations keep this constraint in mind, they can mitigate the effects of their system's vulnerabilities through many other means. Back-ups, redundant systems, and contingency planning are but a few of these methods.

VI. SECURITY IS A JOURNEY, NOT A DESTINATION

A. OVERVIEW

A twist on the old adage of "education is a journey, not a destination" applies to system security: "security is a journey, not a destination." Most agencies have a small number of people managing computer security who have extremely limited authority, training, and virtually no budget. Yet, as part of the Internet, these organizations are being relied upon to provide a minimum level of security and defense against malicious users. Fortunately, recent accomplishments within industry and government research centers have focused on information assurance as the next step in the "journey" towards a secure system of systems.

The work done over the last decade primarily focused on providing a "stopgap" measure to "plug the holes" in the Internet while the GII was still in its formative stage. These stopgap measures historically focused on the "prevent" side (i.e., access control technologies), with an emphasis on authentication technologies, conventional security technology, and forensic technology. Unfortunately, the only way to make an information system completely secure is to unplug it, encase it in concrete, and bury it in the ground. While this may seem like an exaggeration, anything short of this introduces vulnerabilities that can be exploited by adversaries. Obviously, taking such extreme measures makes the system completely unusable. So, how can systems be made usable to the general population, while providing a measure of security and assurance?

Providing this defensive posture for the Internet - which was never meant to be used in a secure setting - has created an environment where technology is influencing the environment its used in. Burton and Obel provide a counterpoint to this, stating that "an organization must influence and change the technology." [Ref. 52] In other words, the organization must choose its technology. If this argument is accepted, then information assurance must be chosen as the next step in the journey. From either perspective, the organizational structure and the technology must offer each other a good fit.

There is a growing awareness of the increasing threat to the NII and the GII, but what can be done about it? Securing and safeguarding this highly complex "system of systems" should be one of the Nation's highest priorities. The ability to counter these threats, however, will require a significant shift in how business is currently being done. Fortunately, this change is already underway, both in government and in the industrial complex.

B. FROM VISION TO REALITY

> Technology begets doctrine, and doctrine begets organization; we need that sequence of events badly. We have the technology, and now we have a clear-cut strategic doctrine at the national level for information operations. [Ref. 53]

This strategic doctrine is focused on providing tools for intelligence agencies and military services to develop defensive, offensive, and exploitation information operations capabilities. However, this doctrine falls short of being truly strategic, since it does not provide the tools for vulnerability testing (i.e., red teaming), nor addresses the balancing act between cost, implementation, performance, and people. These issues are of paramount importance, and will be addressed later in this chapter.

How can mission-critical information technology and the Nation's critical infrastructure be protected against electronic attack? First, an appropriate vision must be developed. The Information Technology Office (ITO) at DARPA, developed a vision statement that is supportive of the development of new technology:

> Create technologies for use in building hardened information systems and networks that have strong barriers to attack, can detect malicious and suspicious activity, can isolate and repel such activity where possible, and can guarantee minimum essential continued operation of critical system functions in the face of concerted information attacks. These technologies will enable the construction of secure enclaves, and will allow distributed computing to span such enclaves, as is required in ISO's systems. These technologies will combine the strength needed for DoD, while retaining the cost savings resulting from use of COTS. [Ref. 54]

The growth of the "global village" through the expansion of the Internet has prompted industry to begin stepping up to the challenge of developing strategies for survivability, assurance, and security research. The current strategy is to develop technologies that can be combined to form a layered defense for information systems. This layered defense is the enabler for providing information assurance to the decision-maker. An overview of these technologies follows.

1. Barriers to Penetration

The term "layered defense" is frequently discussed as part of many of the "strategic visions" that the authors have reviewed. In keeping with the layered defense strategy, barriers to penetration have to be addressed at multiple system levels. This is the case not only in the traditional network and operating system layer, but also in the increasingly important middleware layers for the distributed system security and distributed computing systems. There is also a need to push security technology into the application level, allowing the integration of COTS and legacy systems into military systems.

2. Network Security

At the network level, security for the Internet's domain name system has been developed, providing authenticated name address mapping between domain servers, security for routing tables, etc.

3. Middleware

Recently, middleware layers have benefited from the development of fine grained access control for Common Object Request Broker Architecture (CORBA), an increasingly important technology for distributed computing. CORBA essentially provides the architecture for the plumbing of a distributed system. The CORBA Security Service (CORBAsec) includes facilities for authentication [Ref. 55]. The CORBA Immune System at Odyssey Research Associates [Ref. 56] is using CORBA interceptors (wrappers) to look for anomalous operation invocation sequences. This has created an opportunity to define true interoperability among systems by specifying how the Object Request Brokers (ORB's) from different vendors can interoperate.

4. Operating Systems

Security used to be a big part of operating systems (OS) research. The divergence of performance-oriented OS work and security-oriented OS work over the years needs to be recombined so that innovative security programs can be incorporated into research projects at the ground level. The result of this would be that when these programs are ready for implementation, security and performance would already be built in. This concept was developed as part of the Khazana project at the University of Utah [Ref. 57]. The OS allows secure encapsulation of services, so that conventional file and network services can invoke separate encapsulated servers for authentication cryptography, and all of this can be controlled and managed by a separate policy server.

5. Coordination

Some significant work has been done in developing a coordinated intrusion detection effort within the information infrastructure. This work has led to the establishment of an Internet Engineering Task Force (IETF) [Ref. 58] working group to create a common set of interfaces and protocols for exchanging information among detectors. A draft of this standard is expected by the end of 1999.

What's the significance of this coordination? To assess this, one must consider a truly national - or global - scale system, where detection reports are propagated up through the hierarchy of the system, in order to identify when attacks that are coordinated across different systems and administrative domains might be taking place.

Once this global detection is coordinated, the issue of false alarms must be addressed. A lot of events reported are either trivial, or are only of local interest. A method needs to be developed to allow only the important information to propagate up the chain. Similarly, once the assessments have been done at the higher level, a global context needs to be provided that can be used to drive the local intrusion detection mechanisms, and tell them what information is significant (i.e., what information needs to be collected that isn't being collected now). The follow-on step to this is inferring a model of what we think our adversaries are doing, and predicting what the next phase of the attack will be. This provides the opportunity to conduct some sort of pre-emptive action.

6. Intrusion Tolerance

Intrusion tolerant networks are capable of maximizing the residual capacity of the network infrastructure following partial compromise. This can be done in three parts.

a. Fault Tolerance

In order to do this, the basic fault tolerance and robustness of the network infrastructure must first be improved.

b. Countering Denial of Service (DoS) Attacks

A second part of this revolves around denial of service attacks. Can resource consumption in the network be controlled, in order to prevent DoS attacks? An example of countering a DoS attack is constraining the attacker's resource consumption. One idea is to use advanced resource allocation methods, such as those based on market or economic schemes that will limit the resources available to the attacker. [Ref. 59]

c. Exploiting Technology

The third part is exploiting technologies that have been developed in other parts of the information technology world. An example of this technology includes inferring a model of what we think the adversaries are doing, and predicting what the next phase of the attack would be, and maybe taking some sort of pre-emptive action.

7. Attack Forensics

Attack forensics (or post-attack analysis) is the primary tool used for the development of attack profiles. By observing patterns of behavior – both normal and anomalous – these profiles can be established over a period of time. The problem with using attack forensics is that they produce too much information for security managers to effectively handle. [Ref. 60]

How can a method at looking at attack forensics be developed to determine what damage has occurred, and what needs to be done, in near real-time? DERBI, a program developed at the Software Research Institute (SRI), is being used to try to answer this question. It is touted as "a state of the art program in intrusion damage assessment and reconstitution." Human functions are automated in the assessment of damage and rebuilding of a system to a previously assured state. [Ref. 61]

These seven strategies form the foundation for the next phase of technology to support information assurance goals. Yet, their implementation will fall short if not applied using a strategic approach. Vulnerability testing and the balancing of cost, implementation, performance, and personnel must be done in order to have a truly strategic and effective implementation of information assurance.

C. BALANCING ACT

The additional leverage gained by an increasing focus on information assurance may provide the impetus for the development of trustworthy systems from untrustworthy components. This change is necessary to balance technology with cost, implementation, performance, and personnel.

1. Cost and Implementation

The amount of money spent on the research and development of new information systems and the subsequent investment in security for these systems far outweighs the money spent on their implementation and integration. This condition needs to be brought into balance. For instance, training of our system administrators and operators, basic operator education, and incentives to maintain a "corporate memory" should receive an equitable investment.

The implementation of an information system must be completed in a timely fashion, in balance with the capabilities of the system its being introduced into, as well as its environment (i.e., personnel and equipment). When implementation is too drawn out, the rapid pace at which technology advances tends to cause serious problems: a system can become obsolete before it has even become operational.

2. Performance

Performance takes on a different connotation within the DoD than it does within a commercial organization. DoD personnel carry out their assigned missions with the understanding that they may be called upon to do so at risk of life or limb. In such instances, they must rely on their information infrastructure to perform with a minimum level of assurance. A similar situation exists in many critical civilian applications, such as law enforcement, medicine, emergency services, etc. If these minimum levels are not met, the results could be disastrous.

Performance is closely tied to risk management: in order to gauge the assurance level of a particular system, it is necessary to conduct vulnerability testing. This testing must be continuous in order to keep pace with changes in the cyberterrorism threat.

3. Personnel

People are our weakest link and our strongest adversary. To our benefit, the essence of our competitive advantage lies in the fact that, regardless of the source of motivation to excel, the goal of DoD personnel is the same as that of private sector organizations: to do what they do, better than anyone else. Unfortunately, one size doesn't fit all when trying to identify the best set of policies and practices for all involved in information assurance.

D. DEVELOPMENT OF TRUSTWORTHY SYSTEMS

Developing secure systems that provide an acceptable level of information assurance in a constantly changing environment requires a diversified, iterative approach, as shown in Figure 2. It is not enough to concentrate on any one particular area; each element of the model is crucial to success. In the past, the burden of security and assurance was typically placed on system designers and developers. Dr. David Fisher of CERT has highlighted the downfall of this approach:

> Anything that is "extremely unlikely" can be made into a vulnerability and be exploited by a malicious user. The statistical development of software and operating systems in a "clean room" does not resolve the associated security issues. You can't build secure systems through statistical methodologies. [Ref. 62]

Recent accomplishments in information survivability programs over the last few years have emphasized a much more multi-dimensional approach. Security and assurance are being addressed at all levels and as an on-going process.

Over the last two years, industry has renewed its focus on developing attack barriers, while looking at combining detection mechanisms into coordinated constellations of detectors that can detect large-scale attacks. In spite of the best efforts at preventing and detecting these attacks, there will still be successful attacks that at least partially compromise system assets. Once these large-scale constellations are operational, the next step to take is improvements in intrusion tolerance: developing methods where information survivability can be insured, even while the system is under attack. This natural progression begs the question: how can we rapidly assess damage, repair damage, keep the system functioning, keep critical operations running, and mitigate the effects of the attack? The use of vulnerability testing and the implementation of system diversity play a major role in answering this question.

1. Red teaming

Why should a renewed emphasis be applied to the concept of vulnerability testing through red teaming? First and foremost, red teaming is the most important aspect of information assurance. The investment in information technology is significantly out of balance with the investment in providing assurance and security protection to the same system. Red teaming provides risk assessment for the evaluation of our information infrastructure. This impact is seen from the local level all the way to the Global Information Infrastructure. It identifies the possible and probable impacts of the introduction of new technology into these information infrastructures. The focus on the fortress mentality earlier in this decade only addressed known threats.

Barrier defense mechanisms are designed to address external threats only. Insider threats are typically unaffected by these types of defensive measures. The increased interconnectivity of our information systems compounds this problem even further. As Dr. Fisher has stated, "we live in a world where everyone is an insider; you literally don't know what machines are attached to your system if you are connected to the Internet." [Ref. 63] Thus, as Internet use continues to grow, both the "insider threat" and the external threat become increasingly prevalent. Red teaming provides a means of identifying security gaps and vulnerabilities from an insider's – as well as an outsider's – perspective.

Vulnerability assessment provides an important tool for risk management. In order to be manageable, risks must first be clearly identified. Once identified, these risks can then be mitigated. Thus, red teaming is central to the concept of information assurance: if you can't identify a vulnerability or a weakness, you can't reduce the associated risks, and you can't provide assurance.

So how is information assurance implemented? Figure 2 provides an example that combines enablers from industry and the Marine Corps Advanced Warfighting Experiment (AWE). A system model has been assessed as needing an enhancement through the implementation of commercial-off-the-shelf (COTS) technology. The Marine Corps Warfighting Lab (WFL) and industry representatives develop an operational model, implementing many of the emerging capabilities previously discussed in this chapter. This model is introduced into the system model where it is continually experimented with and analyzed by the AWE and WFL. Simultaneously, the system model is red teamed from an independent vulnerability assessment organization, with a "no holds barred" mentality. This continuous cycle provides the decision-maker with an intrusion tolerant network that maximizes the residual capacity of the network structure, even following a partial compromise.

The methodology for developing trustworthy systems from untrustworthy components is depicted in Figure 2. The system model is consistently assessed against models of missions, adversaries, and vulnerability assessments. The adversarial models are particularly useful in creating a counterattack profile. The ability to develop various levels of response, including autonomous and "cyber command and control," is developed through the roadmap within the model.

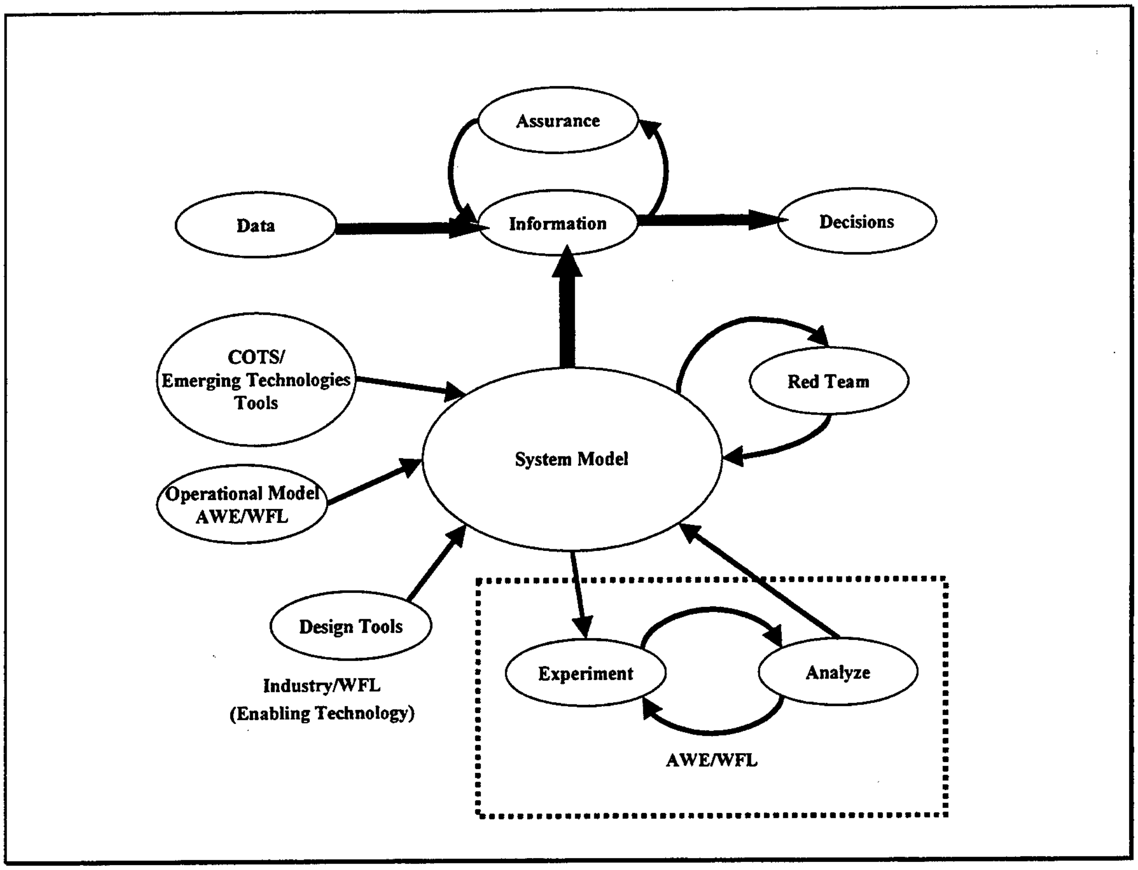

Figure 2. Information Assurance Model.

Vulnerability Testing conducted as a singular event, whose focus is on system and network administrators, provides an extremely limited vision that is anything but strategic. Red teaming should be continuous, unexpected, and have the ability to utilize any method available through open sources.

2. Diversity

Future defense systems are likely going to be composed largely of commercial-off-the-shelf (COTS) and third party components, some of these such as popular commercial operating systems (OS's) introduce shared vulnerabilities into these systems. A vulnerability in one part of the code is replicated hundreds of thousands of times across the system and can represent a serious vulnerability to the overall operation of the system. How can controlled diversity be introduced into these COTS systems in order to mitigate some of these vulnerabilities?

In a heterogeneous network, if an intruder only knows mandatory access control security (MACS), and breaks into the system, an adaptive system can re-route or isolate the attack. Then, if the rest of the system is composed of different architectures (i.e., is diverse), the intruder will have a hard time trying to break in. This is usually the case because most attackers are familiar (i.e., experts) with only one type of system.

It becomes too expensive for attackers to have the technology and capability to break into multiple, heterogeneous systems. It is cheaper to be an expert in only one (unique) system than to be expert at many different systems. The key is to make breaking in to a system expensive relative to the value the attacker receives.

> Ultimately, we must get away from the fortress mentality and find another solution. The reason is that the fortress mentality is expensive, and based on unique systems that still have vulnerabilities. When attacked, they create a greater loss. Responding with any form of Incident Response Team is not very efficient, and has limited value. [Ref. 64]

E. INFORMATION SURVIVABILITY

If experience is the best teacher, as the saying goes, then we've been in school a long time and learned some valuable lessons. Information assurance is the next chapter in the Revolution of Military Affairs (RMA). The history of the United States is rife with analogies supportive of this statement. An excellent example is the advent of air power, and the significance of its influence on warfare as we know it today.

The significance of the cyberterrorist threat to the Nation's critical infrastructure is causing a similar revolution to occur. The infrastructure, with its inherent insecurities, has had too much invested in it to discard. Therefore, the only alternative is to modify it, providing security and assurance to an entity that was never designed for those attributes.

Within DoD, significant and lasting modifications to warfighting doctrine occurred based on the requirements developed through the introduction of air power. The requirement for providing information survivability through information assurance necessitates similar action.

This philosophy is supported by the notion that technology drives doctrine (through requirements), and doctrine drives organizational behavior. How can this be modified to support the RMA being experienced today? As depicted in Figure 6-2 education is training, training identifies requirements for technology, which drives doctrine, which drives organizational behavior, which in turn drives education.

Many of the information technologies developed in the last decade focused on providing a strictly defensive capability. How do we capitalize on this information and formulate a strategy that will provide a reaction that allows for mission accomplishment? There are two answers to this. First is the autonomous level, the automatic response - or quick reaction cycle - when an attack is detected. Second, we must have command and control functions that understand what the impact of that state (of attack) is and how to respond to it.

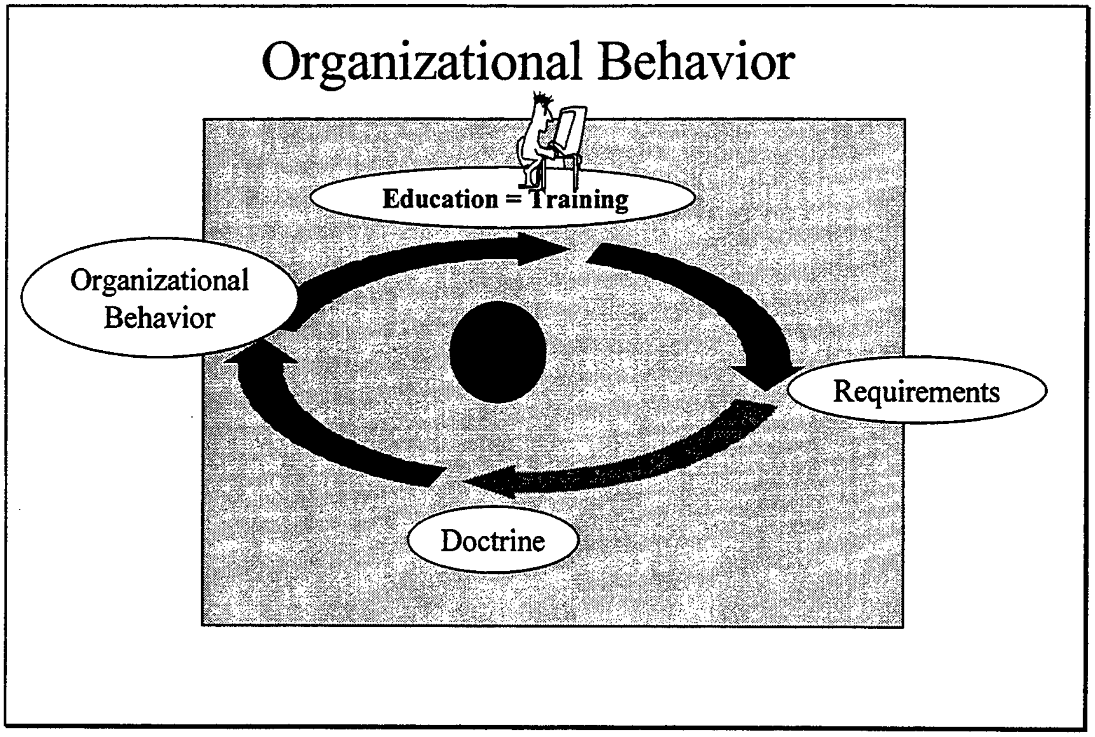

Figure 3. Organizational Behavior Loop.

What are the rapid defense mechanisms that can be implemented to contain an attack of this type? Considering the nature of the attack in context of the mission requires some sort of human intervention (i.e., higher level brain function) to give the system a global understanding of the strategy that an adversary might be using, and formulate a measured response to it. The development of our defensive posture has resulted in a variety of sensors and exploitation mechanisms. The higher level functions that extract information state awareness from these sensors are now sorely needed. All of this supports an overall defense strategy.

F. THE NEXT STEP

Serendipity; it means making fortunate and unexpected discoveries by accident. The idea of providing information assurance was discovered at the realization that a fortress mentality was not applicable to the Internet. Information assurance is a natural progression in the war against nefarious intruders of the information infrastructure. The raising of consciousness due to the advent of these attacks on our information infrastructure has provided the catalyst for senior leadership in industry and government to focus on the issues of information assurance.

Significant consideration has been given to the realm of prevention and detection of anomalous behavior. There has been a large amount of work done in terms of prevention, but it has lost the momentum it once held. The advances of information terrorism have mitigated the effectiveness of prevention.

The recent accomplishments in industry discussed previously have been driven by the requirement to provide at least some level of autonomous response. The increasingly technical aspects of the GII, combined with the disparate lack of security within it, have provided the basis for this requirement. No matter how good the system is, people are still the weak link. The inability to provide a proper balance of the implementation of information technology with trained personnel and system administrators actually detracts from information assurance. There are no silver bullets here. Providing information assurance necessitates a well rounded, in depth approach. Particular attention must be given to those areas previously neglected, such as the implementation of vulnerability testing of emerging and existing information technology.

This will only be truly successful if an equitable balance in the investment associated with research and development and implementation is achieved. Then - and only then - will information assurance truly provide decision makers with confidence in their information systems, even when under attack or stress, through integrated information security in next-generation defense systems.

VII. CONCLUSIONS

> Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur. [Ref. 65]

What is the impact of cyberterrorism on DoD, and how must we manage the requirement to focus on this as a threat? The goal of this thesis was to provide some insight into this question through research of this new face of terrorism, and identify what can be done to provide assurance to the flow of digital information that is viewed as a target by cyberterrorists. A variety of views on cyberterrorism were researched, including the creation of a scenario-based cyberterrorist organization, Cyber Fi. Cyber Fi was created to facilitate research of current and future cyberterrorist threats and counter measures during one of the Marine Corps Advanced Warfighting Experiments, Urban Warrior. The result of these evaluations was a requirement for the development of a truly strategic policy for cyberterrorism. Our research also highlighted the criticality and difficulty of crafting a vision to direct and shape a change effort.

The problem with establishing a set policy on cyberterrorism arises from the fact that the full extent of the threat spectrum is, as yet, unknown. The need for policy – and the lack of one within the federal government – is forcing agencies to go their own way and establish their own. Martin Libicki proposed: "If we are to have a cooperative international agreements and treaties, a declared policy is an essential starting point." [Ref. 66] He went on to say, "the policy should be coordinated with industry and public debate encouraged to secure support and resources required to protect our interests." [Ref. 67]

A. THE SHIFT TOWARDS INFORMATION ASSURANCE

The continued migration of society's support functions into Cyberspace requires a trusted environment that allows critical operations, even when the system is partially compromised. This increasing dependence will lead to increasing vulnerabilities. There will be a parallel increase in the utility of cyberterrorism as well. These issues demand the foundation of a trusted environment that is necessary for information sharing between government (including DoD) and industry. This trusted environment paves the road towards information assurance. In this thesis, the authors discussed how information assurance:

- enables the creation of a strategic cyber defense network,
- is part of an evolutionary change from a point security or barrier defense to the next (necessary) step of providing defense in depth to support the decision makers' needs,
- allowed for the development of trusted systems made up of untrustworthy components,
- provides capabilities for the protection, detection, reaction, and restoration of information systems,
- requires extensive and realistic red teaming,
- must provide a quantifiable level of security and assurance, and
- is sensitive to system design, thereby highlighting differences in competing concepts.

Critical to the implementation of information assurance is the positive momentum in the convergence of government and the commercial sector in the area of Information Operations (IO), Information Warfare (IW), and cyberterrorism. A proposal for enhanced red teaming was presented in Chapters V and VI. Red teaming allows evaluators to identify performance measures that ultimately provide a system effectiveness value. This value can be used to compare the relative capabilities of emerging technologies that are integrated into a risk management approach. This risk management approach is then applied to an evaluation of the overall information infrastructure to satisfy the decision-makers needs. Ideally, this proposed evaluation will be used by information infrastructure architects to evaluate competing information systems intended for DoD, National, and Global use.

B. PERSONNEL ISSUES

The human resources frame is built on core assumptions that highlight the linkage between people and organizations. Increased competition for human capital provides the catalyst for a proactive (vice reactive) approach to personnel issues. Human resources must be managed by leaders in order "to obtain organizational performance by channeling individual potential into organizational achievement." [Ref. 68] The authors focused on personnel issues affecting the DoD, with the following observations:

- The training of our system administrators and operators, basic operator education, and incentives to maintain a "knowledge base" should receive an equitable investment when compared to the cost of information technology.

- The level of training and education of information technology personnel must be significantly improved.

- The commitment incurred to acquire this level of training should also be increased.

- The implementation of information systems must be completed in a timely fashion, in balance with the capabilities of the system it's being introduced into, as well as the environment (i.e., personnel and equipment).

C. STRATEGIC POLICY

Cyberterrorism is likely to mature rapidly; therefore, we must minimize the threat through strategic policy. This policy must incorporate the use of red teaming, and address the increasingly convoluted personnel issues associated with the rapid advance of information technology. If we fail to address these issues, we may find ourselves enveloped in the fog of cyberwar. Incorporation of these ideas into national policy will provide precedence for dealing with future cyberterrorist threats against the United States critical infrastructure.

D. FUTURE RESEARCH

- Develop a cost-benefit analysis model for implementing vulnerability testing (red teaming).
- Develop a training and retention model for people with the skill sets and core competencies required to do the job.
- Conduct a study of different methods (e.g., bonuses/longer term commitments) to aid in the retention of information technology personnel.
- Develop measures of effectiveness/metrics to quantify a system's level of assurance.
- Identify an acceptable (baseline) level of information assurance.
- Develop models for the associated response to different levels of cyberterrorist attacks.

LIST OF REFERENCES

1. Denning, Dorothy, *Information Warfare and Security*, p.14, ACM Press, 1999.

2. Nau Web Site, "On-line Surveys," [www.nua.ie/surveys/how_many_online/index.html]. May 1999.

3. Negroponte, Nicholas, "The Third Shall be First." [http://www.wired.com/wired/archive/6.01/negroponte.html]. January 1999.

4. Denning, Dorothy, *Information Warfare and Security*, p.69, ACM Press, 1999.

5. Collin, Barry C., "The Future of CyberTerrorism," [http://www.acsp.uic.edu/oicj/pubs/cjintl/1302/130214.shtml]. March 1997.

6. Whatis Website, "Definition of Cyberspace," [http://www.whatis.com/cyberspa.html], September 1998.

7. Schwartau, Winn, *Information warfare: chaos on the electronic superhighway*, p. 49, New York: Thunder's Mouth Press, 1994.

8. Whatis Website, "Definition of Cyberspace," [http://www.whatis.com/cyberspa.html]. September 1998.

9. Merriam-Webster On-Line Dictionary, [http://www.m-w.com/cgi-bin/dictionary]. 1999.

10. Mitchell, M., and others, "Cyberterrorism White Paper," Work in Progress for Defense Intelligence Agency at Naval Postgraduate School, 5 May 1999.

11. Tucker, David, *Skirmishes at the Edge of Empire: The United States and International Terrorism*, p. 53, Praeger, 1997.

12. Ibid.

13. Denning, Dorothy, *Information Warfare and Security*, p.68, ACM Press, 1999.

14. Merriam-Webster On-Line Dictionary, [http://www.m-w.com/cgi-bin/dictionary]. 1999.

15. Schwartau, Winn, *Information warfare: chaos on the electronic superhighway*, p. 13, New York: Thunder's Mouth Press, 1994.

16. Joint Chiefs of Staff, "Joint Publication 3-13," [http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf]. 9 October 1998.

17. Joint Chiefs of Staff, "Joint Publication 3-13," [http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf]. 9 October 1998.

18. Stark, Rod, "Cyberterrorism: Rethinking New Technology," [http://www.infowar.com/mil_c4i/stark/Cyber_Terrorism-Rethinking_New_Technology1.html]. 1999.

19. Devost, M., Houghton, B., and Pollard, N., "Information Terrorism: Can You Trust Your Toaster?," [http://www.terrorism.com/terrorism/itpaper.html]. 1997.

20. Denning, Dorothy, *Information Warfare and Security*, p. 13, ACM Press, 1999.

21. Denning, Dorothy, *Information Warfare and Security*, p. 14, ACM Press, 1999.

22. Negroponte, Nicholas, "The Third Shall be First," [http://www.wired.com/wired/archive/6.01/negroponte.html]. January 1998.

23. Denning, Dorothy, *Information Warfare and Security*, p. 17, ACM Press, 1999.

24. Stark, Rod, "Cyberterrorism: Rethinking New Technology," [http://www.infowar.com/mil_c4i/stark/Cyber_Terrorism-Rethinking_New_Technology1.html]. 1999.

25. Pollitt, Mark, "Cyberterrorism – Fact or Fancy?," [http://www.cs.georgetown.edu/~denning/infosec/pollitt.html]. Accessed on May 1999.

26. Devost, M., Houghton, B., and Pollard, N., "Information Terrorism: Can You Trust Your Toaster?," [http://www.ndu.edu/inss/siws/ch3.html]. 1997.

27. Ibid.

28. Ibid.

29. "Clinton proposes anti-terrorism plan," [http://cnn.com/ALLPOLITICS/stories/1999/01/22/clinton.terrorism/]. 22 January 1999.

30. Hamblen, Matt, “Clinton commits $1.46B to fight cyberterrorism,”

[http://cnn.com/TECH/computing/9901/26/clinton.idg/index.html].

26 January 1999.

31. Senator Nunn, Sam, “Critical Foundations: Thinking Differently,” The President’s Commission on Critical Infrastructure Protection Advisory Committee, 7 September 1997.

32. Ibid.

33. Denning, Dorothy, *Information Warfare and Security*, p. 22, ACM Press, 1999.

34. Senator Nunn, Sam, “Critical Foundations: Thinking Differently,” The President’s Commission on Critical Infrastructure Protection Advisory Committee, 7 September 1997.

35. Denning, Dorothy, *Information Warfare and Security*, p. 17, ACM Press, 1999.

36. Denning, Dorothy, *Information Warfare and Security*, p. 12, ACM Press, 1999.

37. Denning, Dorothy, *Information Warfare and Security*, pp. 38-39, ACM Press, 1999.

38. Dalton, Gregory, “Acceptable Risks?,”
[http://www.informationweek.com/698/98iursk.htm].
31 August 1998.

39. Joint Chiefs of Staff, “Joint Publication 3-13: Joint Doctrine for Information Operations,” [http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf].
9 October 1998.

40. Knighthood, Chivalry, and Tournaments Resource Library,
[http://www.chronique.com/index.htm].
27 November 1998.

41. Tsolis, Kristen, “Cyberthreats and Countermeasures,” submitted for publication, IEEE Software, Monterey, California, March 1999.

42. “Cybercrime...Cyberterrorism...Cyberwarfare... Averting An Electronic Waterloo,” [http://www.csis.org/pubs/cyberfor.html]. 1998.

43. No ‘Right’ to Crypto Export? [http://www.wired.com/news/print]. 29 July 1998.

44. "FBI Unit Reports 'Substantial' Cyber Attacks," [http://www.infowar.com/hacker/hack_061198b_j.html]. 11 June 1998.

45. Dalton, Gregory, "Acceptable Risks?," [http://www.informationweek.com/698/98iursk.htm]. 31 August 1998.

46. Major Doran, Fritz, "Cyber Fi: The Cyberterrorism Threat and Urban Warrior," Masters Thesis (draft), Naval Postgraduate School, Monterey, California, September 1999.

47. Interview between Professor Timothy Shimeall, Naval Postgraduate School, Monterey, California and Major Fritz Doran, Naval Postgraduate School, Monterey, California, 18 December 1998.

48. Marine Corps Warfighting Lab, "Urban Warrior Conceptual Experimental Framework," [http://208.198.29.7/mcwl-hot/documents/cef.pdf]. April 1998.

49. Marine Corps Warfighting Lab, "Urban Warrior Brief," [http://208.198.29.7/mcwl-hot/documents/uwbrief.pdf]. April 1998.

50. Marine Corps Warfighting Lab, "Urban Warrior Conceptual Experimental Framework," [http://208.198.29.7/mcwl-hot/documents/cef.pdf]. April 1998.

51. LTGen Rhodes, J., "Navy and Marine Corps Officials Meet With Top Executives," [http://208.198.29.7/mcwl-hot/uw/media/articles_html#NAVY AND MARINE CORPS]. February 1999.

52. Burton, Richard M., and Obel, Borge, pp. 234 *Strategic Organizational Diagnosis and Design*, Kluwer Academic Publishers, 1998.

53. Robinson, Clarence A., *Information Operations Center Provides Attack-Thwarting Tools,* Signal Information Assurance Series, 1999.

54. Koob, G., "Vision Statement," [http://www.darpa.mil/ito/research/is/vision.html]. Accessed on 15 May, 1999.

55. Glinski, N., "CORBA: The Middleware That's Everywhere," [http://www.omg.org]. Accessed on 21 May 1999.

56. Dr. Forrest, S., and others, "Computational Immunology For Distributed Large Scale Systems," [http://www.oracorp.com/Projects/Current/CompImm.htm]. Accessed on January 1999.

57. Carter, J., "Khazana: An Infrastructure for Building Distributed Services," [http://www.cs.utah.edu/projects/khazana/index.html]. September, 1998.

58. IETF Website, "The Internet Engineering Task Force," [http://www.ietf.org/home.html]. Accessed on 7 May 1999.

59. White, G.B., Fisch, E.A., and Pooch, U.W., *Computer System and Network Security*, p. 94, CRC Press, 1996.

60. White, G.B., Fisch, E.A., and Pooch, U.W., *Computer System and Network Security*, p. 110, CRC Press, 1996.

61. Saydjari, S., "Explaining and Recovering from Computer Break-ins," [http://www.ai.sri.com/~derbi/]. February 1998.

62. Interview between Dr. David Fisher, CERT, Carnegie Mellon University, Pittsburgh, PA, and the authors,
16 March 1999.

63. Ibid.

64. Ibid.

65. Douhet, G., "Command of the Air," [http://raven.cc.ukans.edu/~kansite/ww_one/bio/d/douhet.html]. 1921.

66. Wheatley, G.F. and Hayes, R.E., *Information Warfare and Deterrence*, p. 24, Washington, DC: National Defense University Press. December 1996.

67. Ibid.

68. Defense Technical Information Center, Rewarding, *Organizing and Managing People for the 21st Century: Time for a Strategic Approach*, p. I, June 1997.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center..2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, Virginia 22060-6218

2. Dudley Knox Library..2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, California 93943-5101

3. Director, Training and Education...1
   MCCDC, Code C46
   1019 Elliot Rd.
   Quantico, Virginia 22134-5027

4. Director, Marine Corps Research Center...2
   MCCDC, Code C40RC
   2040 Broadway Street
   Quantico, Virginia 22134-5107

5. Director, Studies and Analysis Division..1
   MCCDC, Code C45
   300 Russell Road
   Quantico, Virginia 22134-5130

6. Marine Corps Representative..1
   Naval Postgraduate School
   Code 037, Bldg. 330, IN-116
   699 Dyer Road
   Monterey, California 93940

7. Marine Corps Tactical Systems Support Activity...1
   Technical Advisory Branch
   Attn: Maj J.C. Cummiskey
   Box 555171
   Camp Pendelton, California 92055-5080

8. Marine Corps Warfighting Lab...1
   Commanding General MCWL
   Attn: LtCol Bott
   3255 Myers Avenue
   Quantico, Virginia 22134

9. United States Coast Guard..2
COMDT (G-SRF)
Attn: LCDR Stevens
2100 Second Street SW
Washington, DC 20593

10. Professor John S. Osmundson (Code CC/OS)..1
Naval Postgraduate School
Monterey, California 93943-5002

11. Professor Timothy Shimeall 1
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, Pennsylvania 15213

12. Major Joel G. Ogren, USMC 2
2225 S.E. King Street
Lee's Summit, Missouri 64063

13. Lieutenant James R. Langevin, USCG...2
6135 East Lafayette Boulevard
Scottsdale, Arizona 85251