THE INFORMATION INFRASTRUCTURE SYSTEMAS A NATIONAL SECURITY RISK AND U.S. INFORMATION INFRASTRUCTURE SYSTEM NATIONAL SECURITY POLICY, 1990-2000

by

Dighton McGlachlan Fiddner, Jr.

(Bachelor of Science, Davidson College), 1963

(Masters of Arts, University of Kansas), 1981

Submitted to the Graduate Faculty of the

Graduate School of Public and International Affairs in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

University of Pittsburgh

2003

UMI Number: 3097622

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

Graduate School of Public and International Affairs
University of Pittsburgh
Doctoral Studies Program

Oral Dissertation Defense: Evaluation

An oral Dissertation Defense will be conducted by members of the Dissertation Committee and not be confined to materials in and related to the dissertation. As University Policy, the date time and place of the Defense should be published well in advance in the University Times, and must be approved by the Coordinator (3) weeks prior to its occurrence.

Student's Name DIGHTON M. FIDDNER
Dighton M. Fiddner

Date FEBRUARY 11, 2003

Time 3 PM

Place 3652 POSVAR HALL

Dissertation Title THE INFORMATION INFRASTRUCTURE SYSTEM AS A NATIONAL SECURITY RISK AND U.S. INFORMATION INFRASTRUCTURE SYSTEM NATIONAL SECURITY POLICY, 1990-2000

Four (4) passing votes needed – circle one and sign

Chairperson Phil Williams, PhD — [✓ Pass] Conditional Pass Fail

Member Davis Bobrow, PhD — [✓ Pass] Conditional Pass Fail

Member — Pass Conditional Pass Fail

Member Paul Y. Hammond, PhD — [✓ Pass] Conditional Pass Fail

Outside Member (See attached sheet) Tom Longstaff, PhD — [✓ Pass] Conditional Pass Fail

Note: ***All members of the committee must attend the Dissertation Defense. Unavoidable exceptions must be approved in writing by the Doctoral Program Coordinator prior to the defense.***

Comments including description of any necessary revisions should be attached on a separate sheet of paper.

Doctoral Program Coordinator
William F. Matlack, PhD

Date Feb 25, 2003

Revised 8/30/02

November 17, 2003

Phil Williams, Chairman of the Doctoral Examination Committee
University of Pittsburgh
Room 3G52, Posvar Hall
Pittsburgh, PA 15260

Dear Sir:

I am writing this letter to confirm that I support the dissertation written by Deighton (Mac) Fiddner on Information Security Policy. I concur that this dissertation meets the requirements for award.

Mac's thesis serves as an important contribution to our nation's security. By linking our information infrastructure to risks in the physical environment, this work provides important insights in the prioritization of protection and response assets. I predict that the findings relayed in this work will be used to guide national policy for the US government and private companies that operate our information infrastructures.

In addition to a careful description of our vulnerabilities, Mac's work in the comparison of government structures created to address these threats provides insights into how future response and government actions could be streamlined to provide more effective response to our infrastructures. As pointed out in the thesis, the US infrastructure is most at risk from technological vulnerabilities. These vulnerabilities must be carefully studied to predict the nature and scope of attacks.

It is with great pleasure that I state that this dissertation meets all requirements of the Ph.D. degree. I am pleased and proud to have been an advisor during this process and wish Mac the best in his future career options.

Sincerely,

Thomas A. Longstaff
Manager, Survivable Network Technology, SEI/CERT

ABSTRACT

THE INFORMATION INFRASTRUCTURE SYSTEM AS A NATIONAL
SECURITY RISK AND U.S. INFORMATION INFRASTRUCTURE
SYSTEM NATIONAL SECURITY POLICY, 1990-2000

Dighton McGlachlan Fiddner, Jr., PhD
University of Pittsburgh, 2003

As the Y2K, Yahoo/EBay, and countless examples of hackers and viruses attest, the information infrastructure system is extremely vulnerable. The United States is dependent upon the data this infrastructure provides for virtually every aspect of our modern life, to include the nation's national security. Although the federal government was first warned about these risks in 1992 by several federally sponsored studies, has acknowledged the risk in its National Security Strategy since 1995, and was advised of the interconnected risks to the other civil infrastructures by a federally sponsored panel in 1996, no comprehensive federal information infrastructure security policy existed until after 2000. This research demonstrates that no policy existed because of the inherent complexity of the problem itself: the network structure of the IT system, pervasive software defects, and a rush-to-market mentality by IT producers. However, much of the problem lies with the organization and commitment of the federal government to address the problem: six competing policymaking processes with responsibility to produce national security IT policy and a relative paucity of funds spent on both security for the system and for security R&D

FORWARD

My thanks go first and foremost to my family: my spouse, Patricia, and our children, Stefanie and Andrew. They endured this effort much too long. I am indebted to them for their patience.

I would also like to acknowledge the support of my major academic advisors at the Graduate School of Public and International Affairs at the University of Pittsburgh. Dr. Phil Williams was consistently helpful, encouraging, and patient not only as my Dissertation Chair but also throughout my entire doctoral process. Dr. Paul Hammond has been a true friend and advisor since my initial enrollment in the doctoral program. He has always been available to listen, provide sage advice, and support my efforts. Dr. Davis Bobrow has provided invaluable advice during the dissertation process with his insights on the public policy process and analysis and the United States' federal bureaucratic process. Dr. Tom Longstaff provided valuable technical advice on the information infrastructure system, its vulnerabilities, and its risk to the United States' national security.

Lastly, I would like to acknowledge the support of my colleagues at Indiana University of Pennsylvania. Drs. Steve Jackson, Gwendolyn Torges, Sarah Wheeler, Gawdat Bahgat, and Mary Micco were unstinting and steadfast in their encouragement and their belief in the worthiness of my research. For this, I am grateful.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

As the United States embraces the Information Age, Americans are becoming increasingly more aware of the risks[1] associated with the information (infrastructure)

[1] Confusion over IT security definitions is the norm rather than the exception, especially in the early years of information technology and continuing through the 1990s. Efforts have been made by different government, academic, and business organizations during the decade to standardize the definitions. Throughout the research, I use, but in many cases broaden, the somewhat infrastructure-constrained following definitions of the President's Commission on Critical Infrastructure Protection (PCCIP):

1. **Attack**: A discrete malicious action of debilitating intent inflicted by one entity upon another.
2. **Capability**: The ability of a suitably organized, trained, and equipped entity to access, penetrate, or alter government or privately owned information or communications systems and/or to disrupt, deny, or destroy all or part of a critical infrastructure.
3. **Critical Infrastructure**: Infrastructure that is so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security.
4. **Debilitated**: A condition of defense or economic security characterized by ineffectualness.
5. **Destruction**: A condition when the ability of a critical infrastructure to provide its customers an expected upon level of products and services is negated.
6. **Economic Security**: The confidence that the nation's goods and services can successfully compete in global markets while maintaining or boosting real incomes of its citizens.
7. **Incapacitation**: An abnormal condition when the level of products and services a critical infrastructure provides its customers is reduced. While typically a temporary condition, an infrastructure is considered incapacitated when the duration of reduced performance causes a debilitating impact.
8. **Information and Communications**: A critical infrastructure characterized by computing and telecommunications equipment, software, processes, and people that support:
   - the processing, storage, and transmission of data and information (As will be shown in Chapter 2. Information Infrastructure System, I use this definition of Information and Communications as the definition for an information infrastructure system),
   - the processes and people that convert data into information and information into knowledge, and
   - the data and information themselves.
9. **Infrastructure**: the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the

defense and economic security of the United States, the smooth functioning of the government at all levels, and society as a whole.

10. **Intent**: Demonstrating a deliberate series of actions with the objective of debilitating defense or economic security by destroying or incapacitating a critical infrastructure.

11. **National Security**: The confidence that Americans' lives and personal safety, both at home and abroad, are protected and the United States' sovereignty, political freedom, and independence, with it values, institutions, and territory intact are maintained.

12. **Public Confidence**: Trust bestowed by citizens base on demonstrations and expectations of:
    - their government's ability to provide for their common defense and economic security and behave consistent with the interests of society; and
    - their critical infrastructure's ability to provide products and services at expected levels and to behave consistent with their customers' best interests.

13. **Risk**: The probability that a particular critical infrastructure's vulnerability will be exploited by a particular threat.

14. **Risk Management**: Deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level.

15. **Threat**: A foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and the malicious intent of debilitating defense or economic security.

16. **Vulnerability**: A characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat. (As can be seen by the rather lengthy discussion in footnote 5, the exact definition of "vulnerability" is subject to much discussion and nuances) (United States White House, "Glossary," Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection, Washington, D.C., October 1997).

The concept of **threat** is an example of my broadening the PCCIP's definition. For this research, I follow Barry Boehm's example in Software Risk Management and define the terms as follows:

- A **threat** is any possible accidental or deliberate danger or harm to a system resulting in significant damage to the system or loss of resources (Barry W. Boehm, Software Risk Management, Los Alamitos, CA: IEEE Computer Society Press, 1993, 67-68).

With this definition, threat does not necessarily have to emanate from a perpetrator but can emanate from anywhere or anything as long as it has this potential to result in significant damage to the system or loss of resources. Consequently, for Boehm the purpose of security is "to protect systems from a wide range of threats" (Boehm, 67). The concept of threat is discussed further in the Methodology section of this chapter.

systems[2] that make their lives easier and more productive, their economy more robust and competitive, and their government more responsive. These same risks have the potential to imperil the national security of the United States as President Clinton acknowledged in the 1995 National Security Strategy of the United States:

> "The threat of intrusions to our military and commercial information systems poses a significant risk to national security and must be addressed."[3]

The FBI has even quantified that the National Information Infrastructure is the fifth most serious "key issue to the nation's national security."[4]

[2] The PCCIP defines infrastructure as a framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of the government at all levels, and society as a whole (United States White House, Critical Foundations: Protecting America's Infrastructures).

From this point forward, I use the term "information infrastructure system" throughout the research to describe what is commonly referred to as the "information system." Information infrastructure system more accurately describes the system and places it in its true context as one of the U.S.'s (and other developed nations') critical infrastructures. The rationale is explained more fully in Chapter 2. Information Infrastructure System.

[3] United States White House, National Security Strategy of the United States, Washington, D.C., February 1995, 8.

Although first identified as a risk to the nation's national security in the 1991-92 national security strategy (United States White House, National Security Strategy of the United States, 1991-92), this statement by President Clinton is the first official unclassified public acknowledgement by the United States Government that the information infrastructure system is considered a **significant** national security threat to the United States' national security. Interest in information security by the federal government, however, was first addressed in 1982 with the formation of The President's National Security Telecommunications Advisory Committee (NSTAC), and gained prominence as the nation has become more dependent upon information systems (described in detail in Chapter 4. Policy Disorganization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy). President Bush signed the classified National Security Decision Directive 42 in 1990 which admitted that emerging technologies "... pose significant security challenges" (Winn Schwartau, Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age, 2nd edition, New York: Thunder's Mouth Press, 1996, 185-186).

Also in February 1990, a Network Security Task Force was established to address the vulnerability of the nation's telecommunication networks to intentional software disruptions or manipulations that could threaten national security or emergency preparedness communications (United States National Security Telecommunications Advisory Committee (NSTAC), Issue Review: A Review of NSTAC Issues Addressed Prior to NSTAC XIX, [Washington, D.C.]: The President's National Security Telecommunications Advisory Committee, March 1997, iii and Armed Forces Staff College, National Defense University, Formulation of National Strategy (Class 83) Volume II, Faculty Guidance, Norfolk, VA., January 1988).

[4] United States Department of Justice, Awareness of National Security Issues and Response (ANSIR) Program Homepage, Federal Bureau of Investigation, April 6, 1998,

All that is needed to jeopardize the nation's security, according to former President Clinton, is a potential intruder with the malevolent intent to exploit the vulnerabilities of the information infrastructure system. The FBI's National Security Issues and Response (ANSIR) Program assessment identifies that potential intruder as a

> "foreign power-sponsored or foreign power-coordinated intelligence activity directed at the U.S. Government, corporations, establishments, or persons targeting facilities, personnel, information, or computer, cable, satellite, or telecommunications systems which are associated with the National Information Infrastructure. Specific proscribed risks include:
>
> 1. denial or disruption of computer, cable, satellite or telecommunications services;
> 2. unauthorized monitoring of computer, cable, satellite or telecommunications systems;
> 3. unauthorized disclosure of proprietary or classified information stored within or communicated through computer, cable, satellite or telecommunications systems;
> 4. unauthorized modification or destruction of computer programming codes, computer network databases, stored information or computer capabilities; or
> 5. manipulation of computer, cable, satellite or telecommunications services resulting in fraud, financial loss or other federal criminal violations."[5]

Just what are the vulnerabilities[6] of this system that is so vital to the United States that they create risks that jeopardize the security of the nation? Also, given the importance

http://www.fbi.gov/hq/nsd/ansir/ansir.htm#threatlist.

[5] United States Department of Justice, Awareness of National Security Issues and Response (ANSIR) Program Homepage.

The Key Issue Threats to the United States' national security are:

1. Terrorism
2. Espionage
3. Proliferation
4. Economic Espionage
5. Targeting the National Information Infrastructure
6. Targeting the U.S. Government
7. Perception Management
8. Foreign Intelligence Activities (United States Department of Justice, Awareness of National Security Issues and Response (ANSIR) Program Homepage).

[6] The Common Vulnerabilities and Exposures (CVE) Editorial Board in 1999 found that there are at least two common uses of vulnerability:

> "The broad use of 'vulnerability' refers to any fact about a computer system that is a legitimate security concern, but only within some contexts. For example, since the finger service reveals user information, there are reasonable security policies that disallow finger from being run on some systems. Thus finger may be regarded as a 'vulnerability' according to this usage of the word.
>
> "A narrower view holds that some security-related facts fall short of being 'true'

of the system to the nation's existence, what policy or policies have the national government developed and implemented to secure this system and better protect the nation's security?

This research is intended to answer these questions by demonstrating exploitation of the vulnerabilities of the information infrastructure system could jeopardize American national security, to include our national defense. At the same time, I propose to demonstrate that several other conditions of the information infrastructure system offer as great a risk to our national security as the intrusions to which former President Clinton referred.

> vulnerabilities. With respect to the presence of the finger service, it may be argued that since finger behaves as it was designed to behave, it should not be considered to be a vulnerability in this narrower view."

The CVE Editorial Board then decided in August 1999 to identify both as "universal vulnerabilities" (i.e., those problems that are normally regarded as vulnerabilities within the context of all reasonable security policies) and "exposures" (i.e., problems that are only violations of some reasonable security policies). The difference is contingent on the condition of the security policy: "all" reasonable security policies versus "some" reasonable security policies. Universal vulnerabilities are those conditions that a security policy that includes at least some requirements for minimizing the threat from an attacker addresses. More specifically,

> "A universal vulnerability is a state in a computing system (or set of systems) which either:
>
> - allows an attacker to execute commands as another user,
> - allows an attacker to access data that is contrary to the specified access restrictions for that data,
> - allows an attacker to pose as another entity, or
> - allows an attacker to conduct a denial of service."

An "exposure" is a state in a computing system (or set of systems) which is not a universal vulnerability, but either:

> - allows an attacker to conduct information gathering activities;
> - allows an attacker to hide activities;
> - includes a capability that behaves as expected, but can be easily compromised;
> - is a primary point of entry that an attacker may attempt to use to gain access to the system or data; or
> - is considered a problem according to some reasonable security policy."

Since this research is concerned with any weakness in the information infrastructure system that could cause accidental or deliberate danger or harm to a system resulting in significant damage or loss of resources, I have chosen to use the broader "universal vulnerability" definition in this research but will truncate the term to "**vulnerability**" for ease of understanding and clarity (Mitre Corporation, Common Vulnerabilities and Exposures (CVE) Homepage, http://cve.mitre.org, May 9, 2001).

This focus of the research on the system's systemic vulnerabilities provides a different perspective for examining the issue. Most past analyses have viewed a security threat to an information system from an isolated subsystem, component, or equipment perspective. The research, thus, provides insight into the risks and consequences associated with the information infrastructure system's vulnerabilities. It also suggests strategies for the United States to address the vulnerabilities that have the potential to imperil our national security.

1.1. Relevance.

The 1990s are particularly relevant to the issue of information infrastructure system security. It was during this decade that the technology spread from predominantly the federal government, academia, and large businesses to become pervasive throughout the American society and culture. The decade is further relevant to this particular issue area because, with this growth in both the quantity and importance of the technology, protection of the network's data and the network itself became more salient. The Morris worm in 1987[7] had awakened technology professionals to the damage to which the information network itself might be subjected and prompted greater awareness of the need for security of the network and its components. Further, the Clinton administration staked much of its reputation and success, as least initially, on proliferation of information technology resources and integration of those resources into every aspect of American life.

[7] The program Morris created was technically not a virus but a worm. According to Bob Page, a "virus is a piece of code that adds itself to other programs and cannot not run independently but requires a "host" program be run to activate it." Whereas, a worm is a "program that can run by itself and can propagate a fully working version of itself to other machines." The program loosed on the Internet (ARPANET) was therefore clearly a worm (Ken van Wyk, "(Long) Report on the Internet Worm: A Report on the Internet Worm by Bob Page," The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 76 (November 12 1988), http://catless.ncl.ac.uk/Risks/7.76.html).

The research also reinforces the notion that national security is not just military defense. Conceptually, national security has always encompassed some aspect of the idea of a national self: values synonymous with the nation's will to survive and with the nation's prospects for long-term survival.[8] For the United States these national values traditionally have included a desire to:

- maintain the United States intact along with its institutions, people, and the fundamental values of human dignity, personal freedom, individual rights, and the pursuit of happiness, peace, and prosperity;
- ensure a healthy and growing U.S. economy; and
- promote open, democratic and representative political systems and an open international economic and trade system.[9]

For more than forty years the Cold War imposed a structural framework that equated national security with national defense to the virtual exclusion of these other national security concerns.[10] With no apparent adversary now capable of credibly threatening the nation's existence, the United States must anticipate a variety of more diffuse, amorphous, complex, and less direct developments[11] that jeopardize both its values of national self and its national defense.[12]

[8] Robert E. Osgood and Robert W. Tucker, Force, Order, and Justice, Baltimore: The Johns Hopkins Press, 1967, 271-272, 280, and 296 and United States White House, National Security Strategy of the United States, Washington, D.C., January 1988, 3.

The PCCIP's definition of national security captures the same elements: confidence that Americans' lives and personal safety, both at home and abroad, are protected and the United States' sovereignty, political freedom, and independence with it values, institutions, and territory intact are maintained (United States White House, "Glossary," Critical Foundations: Protecting America's Infrastructures).

[9] United States White House, National Security Strategy of the United States, Washington, D.C., January 1993, 3.

[10] The Stanley Foundation, Beyond Cold War Thinking: Security Threats and Opportunities (Report of the Twenty-Fifth United Nations of the Next Decade Conference, June 24-29, 1990, 1 and 6-7.

[11] The White House, National Security Strategy of the United States, January 1993, 1 and The Stanley

Threats to the information infrastructure system pose just such a risk. Because of the nature of the system, a threat to the information infrastructure systems is certainly not as direct as a military assault on American interests. And, America is currently more vulnerable to threats to the information infrastructure system's vulnerabilities than most other nations because it has more completely integrated the features of the "information revolution" into its society, business, and government.[13] And, these sectors increasingly depend on open and interconnected computer systems to manage their critical processes:[14]

- The U.S. government depends upon the information infrastructure system to carry out the business of governing,[15]
- American business is becoming increasingly more dependent upon the information infrastructure system to increase productivity and gain competitive advantage domestically and internationally;[16] and

Foundation, 26.

[12] See The White House, Critical Foundations: Protecting America's Infrastructures, for a more detailed explanation of how an infrastructure can affect the nation's health, welfare, and defense.

[13] Gary H. Anthes, "DoD on Red Alert to Fend Off Info Attacks," Computerworld 31, no.1 (January 6, 1997), 1.

"We are at higher risk than most countries because we have become more dependent on technology." (Toney Jennings as quoted in Anthes, 1).

"Of all the countries in the world, we are the most dependent on our electronics" [Phil Williams, "Transnational Criminal Organisations and International Security," Survival 36, no. 1 (Spring 1994)].

[14] United States National Security Telecommunications Advisory Committee (NSTAC), Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration, A Symposium Sponsored by the President's NSTAC in Conjunction with the Workshop on Security in Large-Scale Distributed Systems, Purdue University, West Lafayette, IN, October 20-21, 1998, 3.

[15] 95 percent of government communications travels over the public switched network (United States National Security Telecommunications Advisory Committee (NSTAC), Issue Review: A Review of NSTAC Issues Addressed Prior to NSTAC XIX, iii).

[16] Over the last decade, information technology has become an essential tool for corporations. It has enabled the cost cutting, reorganization, and re-engineering that have re-established the United States' global competitiveness and rejuvenated U.S. companies" (Robert W. Sterns, "The Promise of the National Information Infrastructure" in National Academy of Sciences, National Academy of Engineering, Revolution in the U.S. Information Infrastructure, Washington, D.C.: National Academy Press, 1995, 25).

- even our personal lives are becoming more and more entwined with the information infrastructure system as venues add home pages and interactive programs to attract more consumers and improve lives.

Information technology's importance is much subtler than just an increase in productivity. The IT industry's technology and services undergird all sectors now. It has become the bedrock upon which these societal and economic institutions are built. Not only does the system of networks provide the data necessary to provide goods and services, but the networks themselves are also becoming deeply embedded as essential elements of the organizations and institutions.

The information infrastructure system risk potentially is the most comprehensive threat to the United States' national security in the post-Cold War era. Because the complex management systems of electric power, money flow, air traffic, oil and gas, and other civil infrastructure services are dependent on the interconnected information infrastructure system such a threat has the potential to imperil the health and welfare and defense of the nation by jeopardizing our economy, daily aspects of our lives we normally take for granted (i.e., power, safe water, emergency services, etc.),[17] our trust in government, and the conduct of military planning and operations.[18] Because of this fundamental dependency, the system eventually would have become a national security risk for the United States irrespective of the Soviet Union's collapse. And, this risk has become even greater with the advent of

[17] The RAND Corporation. "Strategic Warfare Rising." MR-964-OSD. Santa Monica, CA.: The RAND Corp, 1998, 1-2.

[18] Roger Molander, Andrew S Riddile, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," MR661, Santa Monica, CA.: The RAND Corp., 1996, 3 and 4.

U.S. power projection plans might be deterred or disrupted by threats or attacks against infrastructures vital to overseas deployment (Gregory Slabodkin, "FBI Suspects Two Teens in DoD Systems Attack," Government Computer News 17, no. 5 (March 9, 1998), 2).

large-scale distributed computing in the mid-1990s. The infrastructures created by these relatively new distributed systems greatly increase the efficiency and sophistication of the network, but, at the same time, also greatly increase its vulnerability to exploitation.[19] The information infrastructure system's vulnerabilities may have been even a more serious risk sooner if the U.S.S.R. had continued as our major power protagonist.

The risk is not so much that an adversary could destroy the entire information infrastructure system, or even one civil infrastructure, but that an individual or collection of infrastructures could be jeopardized by large scale or massive disruption. Such a disruption could produce a strategically significant result by disrupting the economy and normal life, leading to loss of the populace's confidence in the government to provide necessary services. A series of large scale or massive disruptions would prolong the damage done to the citizens' health and welfare, the economy, national defense, and public confidence immeasurably.

This is not to minimize the effect the same conditions could have directly on the United States armed forces. In the commercial world, the transition to the electronic office and the electronic factory brought with it an increased web of tight dependence on particular skills in computer software, networking, supply, and maintenance that changed both the culture of the workplace and the balance of commercial power. The same change has occurred in military forces as well; particularly the U.S. military that like the rest of the nation has wholeheartedly embraced automation with increasingly greater use of integrated information systems. In a modern military force, there is not just one type of weapon at the

[19] Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff and Nancy R. Mead, "Survivability: Protecting Your Critical Systems," in Proceedings of the International Conference on Requirements Engineering, April 6-10, 1998.

front but many, each of which has distinct and often narrowly defined missions and tasks that must be monitored, evaluated, and integrated into the strategy and tactics.

With each new generation of smart systems, computing power and integration become more deeply embedded as an indispensable element of military systems. The modern U.S. military is increasingly becoming a complex, highly interconnected, integrated socio-technical system with a high degree of interdependence between and among units. As such, it requires intensive, timely information and logistic support to increasingly networked and centralized command-and-control.[20] Critical supplies and maintenance must be available just when and where they are needed if the very expensive weapons platforms are not to be useless or immobile. The linkages between units and functions are now both reciprocal and "tightly coupled."[21] The disadvantage is that these large, complex, tightly integrated, highly specialized, high-technology militaries can be disrupted with relatively simple weapons.[22]

The operational and support requirements of these sophisticated, computerized weapons systems are far more demanding than those of the simpler systems of the past.[23] The complexity of operation and differentiation of skills required to operate and maintain these highly technical systems mandate a larger and more complex managerial and coordination organization also. As in the civilian world, the zeal for more complex and

[20] Problems of modern command-and-control systems are legion: overconfidence, information overload, high support requirements, overdependence on automated systems, hidden flaws and mistakes in technical systems, the aura of timeliness without its reality, and the illusion of command without authority (Gene I. Rochlin, Trapped in the Net: The Unanticipated Consequences of Computerization, Princeton, N.J.: Princeton University Press, 1997, 204).

[21] Rochlin, 202.

[22] Classic examples include the U.S. and the Soviet experiences in Vietnam and Afghanistan, respectively (Rochlin, 175).

[23] Rochlin, 147.

automated equipment has been overtaken by the realization that although use of new technologies requires fewer operators, these operators have to be better educated and better trained.

Fewer trained personnel are required at the front, but far more are needed behind it.[24] Because the specialized skills are not and will not be available or are too costly on a fulltime basis, many of the support roles have been, or are being designated to be, transferred to civilian employees or contractors to conserve military manpower.[25]

The military shifts to ships built totally around their combat electronics and missile suites; to tanks, gun systems, and missiles that require electronics for control as well as for aim; and to aircraft that can neither fly nor fight effectively without relying on their sophisticated electronics, effectiveness and reliability come to depend on an elaborate, tightly linked web of maintenance, logistics, and repair. For every sophisticated high-technology weapon at the front, a long and increasingly tightly coupled train of logistics and other support provided by highly trained and increasingly valuable personnel is required to maintain, support, coordinate, and direct the operations.[26] Such changes alter the traditional "tooth-to-tail"[27] ratio and affect combat units, combat support systems, and the structure of military command, as well as the risks, role, and purpose of the military.[28]

During the Gulf War, the U.S. was able to mobilize, on its own schedule, whatever pieces were required out of a force structure intended to fight one and a half wars simultaneously, and then use them to fight a half-war under maximally favorable

[24] Rochlin, 145.
[25] Rochlin, 179.
[26] Rochlin, 132.
[27] The ratio of actual fighters to noncombatant support personnel (Rochlin, 132).
[28] Rochlin, 147.

conditions.[29] The high-technology weapons systems using black boxes were effective, but only at enormous expense.[30] Their support systems were allowed to train and operate without hindrance or time and resource constraint[31] and at a cost of moving almost all of the U.S. reserve repair capacity into sprawling Saudi bases that would have been quite vulnerable to a serious Iraqi attack. These maintenance bases in Saudi Arabia then had virtually unrestricted access to parts and to diagnostic and other critical skills; active duty, National Guard and reserve units were mined for resources. Personnel with critical specialties, always in short supply even in peacetime, were sought out and brought to the theater.[32]

Without networked information systems, organizations, to include the U.S. military, would not be able to function.[33] Americans' government, commerce, defense, and even lives now depend upon timely data from the information system. If that data cannot be assumed to be accurate, private when desired, or is not available, risks to our personal, institutional, economic, and national security ensues.[34] Given the United States'

[29] Even though such an effort almost totally stripped Europe and the U.S. of systems, spares, and maintenance capability (Rochlin, 177).

[30] As many as eight scarce and expensive electronic warfare aircraft were used to cover a dozen F-16s on a raid; such a high ratio of support to combat aircraft was not atypical for Gulf War air operations. Satellites intended to cover the Soviet Union and other areas of the world had to be moved into position to provide surveillance and intelligence. Command-and-control resources intended to fight a major global war were diverted to the Gulf to manage the intricacies of the battle. It took almost all of the six months to acquire, analyze, digitize, and program the key terrain and target information needed for programming the Tomahawk cruise missiles' guidance computers (Rochlin, 178).

[31] Rochlin, 184.

[32] Rochlin, 178.

[33] Rochlin, 49.

[34] United States National Security Telecommunications Advisory Committee (NSTAC), Issue Review: A Review of NSTAC Issues Addressed Prior to NSTAC XIX, 2-3.

dependence upon the information infrastructure system, information infrastructure system security equates to national security.[35]

And, the threat to the information infrastructure system and, by extension, to U.S. national security, is real. In addition to the well-publicized cases that affect great numbers of and some highly public information infrastructure system users, a study by Asta Networks and the University of California, San Diego, monitored a tiny fraction of the addressable Internet space and found almost 13,000 denial of service (DoS) attacks launched against over 5000 targets in just one week. The Computer Security Institute/FBI also found 85 percent of its sample experiencing computer intrusions, with 64 percent serious enough to cause financial losses of approximately $378 million (an increase of 43 percent from the previous year).[36]

1.2. Methodology.

I contend that today's threat to our information infrastructure systems is the same in intent (exploitation of data) as past threats targeting information, but at the same time differs because of changes in how that information is transmitted:

- a pervasive and interconnected information infrastructure system of multiple components; and
- the speed with which data is available

[35] Harris N. Miller, Fighting Cyber Crime, Testimony before the House Committee on the Judiciary. Subcommittee Crime, Oversight hearing on Fighting Cyber Crime: Efforts by Private Business Interests, June 14, 2001, http://www.itaa.org/govt/cong/61401testim.pdf, 1, 4.

"We know a former senior intelligence official who says, 'Give me $1 billion and 20 people and I'll shut America down. I'll shut down the Federal Reserve, all the ATMs; I'll desynchronize every computer in the country.' I come away persuaded that we in fact are going to see infoterrorism, not just by hackers playing games, but by countries or criminal syndicates that learn to do this stuff very effectively." (Alvin Toffler, Information Week, January 10, 1994, 10 as quoted in Donald L. Pipkin, Halting the Hacker: A Practical Guide to Computer Security, Upper Saddle River, N.J.: Prentice Hall PTR, 1997, 12).

[36] Miller, 3.

and its role in society: the dependency of American society, business, and government on the data generated, processed, stored, and transmitted by the system. These changes make the United States more vulnerable to both disruptions in the continued functioning of the infrastructure and exploitation of the data.

It is also my contention that the systemic organization of today's information technology is its greatest vulnerability. The U.S. information infrastructure system is intentionally organized as an open network architecture and connected with other information infrastructure systems in a global open network architecture.[37] While all systems have vulnerabilities, an open network architecture system is much more vulnerable to unauthorized access because of its inherent easy access.[38] Connection to other information infrastructure systems then provides ease of intra-/inter-system movement, i.e., movement between the various levels of the information infrastructure system and within the networks at a given level. It is essentially easy to access the system and to move around within the system once access has been gained.

Once in the information infrastructure system, a determined potential unauthorized user can concentrate on attacking the vulnerabilities of any of the different interconnected

[37] The Federal Communications Commission has mandated an evolution toward open network architectures that have as their goal the equal, user-transparent access via public networks to network services provided by network-based and non-network enhanced service providers. **Unfortunately, when implemented, the concept makes network control software increasingly accessible to both users and adversaries** (emphasis added by author). Implementation of the Telecommunications Act of 1996 will also required carriers to collocate key network control assets and to increase the number of points of interconnection among the carriers (United States Department of Defense, Report of the DSB Task Force on Information Warfare (Defense), Defense Science Board, Washington, D.C., January 8, 1997, Section 2.3 – "The Infrastructure").

[38] "The Internet [and the information infrastructure system by extension (exposition added by author)] lowers barriers to entry on a global basis -- global in both space and time" [Daniel E. Geer, Jr., "Risk Management is Where the Money Is," Risks-Forum Digest 20, no. 6 (October 12, 1998)]. The Internet recorded almost 90 per cent of reported security incidents from 1989-1995 as attempts to gain unauthorized access to files or (sub)systems (John D. Howard, "An Analysis of Security Incidents on the Internet 1989-1995," Ph.D. diss., Carnegie-Mellon University, April 1997, 235-236).

components of the infrastructure system. A knowledgeable intruder will already know, and an amateur will search for relentlessly, the vulnerabilities most easily defeated.[39] What is interesting about the unauthorized access threat is the apparent dilemma of reconciling open network architecture assets and vulnerabilities while at the same time preserving the confidentiality, availability, integrity, authenticity, and the verification of the origin and receipt (nonrepudiation)[40] of the data. Fortunately, or unfortunately depending upon your

[39] "It was a case of finding weak links in networked environments, using many techniques." Quote from member of Masters of Downloading (MOD) on the November 1997 intrusion of the U.S. Defense Information System Network (DISN) and the successful downloading of a copy of the Defense Equipment Manager (DEM) (Martyn Williams, "Hackers Penetrate Defense Department Computer Networks," Newsbytes, April 22, 1998, http://www.newsbytes.com, 1).

[40] Controversy also exists with the use of and definitions of terms within the information security field. There is a national movement away from Information Systems Security to the more complex discipline of Information Assurance. Definitions from National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, follow:

- "**Information Systems Security** (Information Security, ISS, INFOSEC) - Protection of information systems against unauthorized access to or modification of information whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats."
- "**Information Assurance** (IA) - Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (United States National Security Agency, National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Ft. Meade, MD: NSTISSC Secretariat (142), September 2000).

The controversy extends to definitions for the objectives themselves. Laprie (Jean-Claude Laprie, "Dependability – Its Attributes, Impairments, and Means" in B. Randell, J-C. Laprie, H. Kopetz, and B. Littlewood, eds. Predictably Dependable Computing Systems. Berlin: Springer, 1995) equates "reliability" to "dependability" as a property of a computer system that justifiably can be relied upon to deliver service. IEEE Standard Glossary of Software Engineering Terminology (Institute of Electrical and Electronics Engineers, IEEE Standard Glossary of Software Engineering Terminology (Std. 610.12-1990), Standards Committee, Computer Society of the IEEE, September 28, 1990) has no definition for "dependability." Laprie's other definitions:

- "readiness for usage" leads to "availability";
- "continuity of service delivery" leads to "reliability";
- "non-occurrence of catastrophic consequences on the environment" leads to "safety";
- "non-occurrence of unauthorized disclosure of information" leads to "confidentiality";
- "non-occurrence of improper alterations of information" leads to "integrity";
- "aptitude to undergo repairs and evolution" leads to "maintainability"; and
- associating integrity and availability with respect to authorized actions, together with confidentiality, leading to "security" are equally confusing (Carl E. Landwehr, Alan R. Bull, John P. McDermott, and William S. Choi, "A Taxonomy of Computer Program Security Flaws," ACM Computing Surveys 26, no. 3 (September 1994), 4) so I've elected not to use them.

At the same time, the following definitions of information assurance objectives (with their source point of view, the policy answers to that dilemma have already been made (at least for the United States and most other nations) in favor of easy access in order to provide the benefits of the information system to as many people as possible for as little cost as possible (The issue is discussed in more detail in Chapter 2. Information Infrastructure System).

Of course, an open network architecture is also vulnerable to "insider" abuse (unauthorized use to include access to unauthorized data by someone with authorized system or partial system access). Insider abuse is a security problem with any system. Much effort has been expended by security managers to identify and counter such abusers and is considered outside the scope of this particular research.

---

indicated) are advocated by Shafer, The Joint Staff, and Ruthberg and Tipton:

- "confidentiality" is ensuring that data is not disclosed to those not authorized to see it;
- "availability" is the prevention of unauthorized withholding of information resources;
- "integrity" is assurance that data cannot be deleted, modified, duplicated, or forged without detection (Kevin Shafer, Dictionary of Networking, San Jose: Novell Press, 1997, 900, 896, and 907, respectively);
- "authentication" is the verification of the identity of an individual or the source of the information (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C. July 4, 1996, 2-90); and
- nonrepudiation is the verification of the origin and receipt of messages and data (Zella G. Ruthberg, and Harold F. Tipton, Handbook of Information Security Management: 1995-96 Yearbook, Boston: Auerbach, 1995, S-273).

Given this controversy, I have chosen to use the definitions of the objectives as found in National Information Systems Security (INFOSEC) Glossary:

- confidentiality - assurance that information is not disclosed to unauthorized persons, processes, or devices;
- availability - timely, reliable access to data and information services for authorized users;
- integrity - quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information;
- authentication - security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information; and
- nonrepudiation - assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

I further contend that the increasing use of integrated software[41] (e.g., Supervisory Control And Data Acquisition (SCADA) system software and apparently programs within the Defense Information System Network (DISN)[42]); sharing common infrastructure components in the interest of efficiency, sophistication, and economy;[43] and greater interconnectedness of other critical infrastructures (i.e., emergency services, banking & finance, electric power, transportation, oil & gas delivery & storage, water, and government services[44]) with the information infrastructure exacerbate the threat to American national security.[45] Such systems also are, or will be, too "tightly coupled" with little "slack" and susceptible to the phenomenon Charles Perrow calls "system accidents" due to "interactive complexity."[46]

[41] Software/software integration combines the functionality of different applications by using the output of one application as input for another application to form a seamless environment. The user cannot tell where one application ends and the next begins. The integrated applications are more powerful to the user than any one application or the sum of the individual applications and eliminate inconsistencies caused by time delays in processing or data updating. With software/hardware integration, functional software programs are combined directly with hardware components to provide a single offering (Forest Horton, Jr., ed, Towards The Global Information Superhighway: A Non-Technical Primer for Policy Makers (Special Centennial Publication), FID Occasional Paper 11, Prepared by The FID Task Force on Global Information Infrastructures and Superhighways (FID/GIIS) and Collaboration Organizations, The Hague, Netherlands: International Federation for Information and Documentation (FID), 1995, 231; Andrew S. Targowski, Global Information Infrastructure: The Birth, Vision, and Architecture, Harrisburg, PA.: Idea Group Publishing, 1996., 214; and Laprie, et.al., "Definition and Analysis of Hardware-and-Software Fault-Tolerant Architectures" in Randell, Laprie, Kopetz, and Littlewood, eds.,104).

With software/software integration, a word processor, spreadsheet, and database, for example, are combined into a single offering. The evolving versions of Microsoft's Windows operating system provide a classic example of both increasing functionality and complexity due to integration. Each new version added additional functions that seamlessly operated from the Windows system by just "clicking" a mouse to provide greater ease of use for the user but at the same time made the program much more complex (Shafer, 281).

[42] The Defense Equipment Manager (DEM) was "used by the Defense Information Systems Agency (DISA) to routinely check and maintain the DISN hardware (routers, multiplexers, IDNX networks, repeaters, and GPS satellites and receivers) from a remote location" according to a member of the Masters of Downloading (MOD) (Martyn Williams, 1).

[43] Ellison, et.al., "Survivability: Protecting Your Critical Systems."

[44] United States White House, Critical Foundations: Protecting America's Infrastructures, 4.

[45] A National Agency Security (NSA) exercise gained access to a U.S. electric power grid through unauthorized intrusion into the information infrastructure system during an "Eligible Receiver" exercise to test government computers' vulnerabilities (Martyn Williams, 2).

[46] Charles Perrow, Normal Accidents: Living with High-Risk Technologies, New York: Basic Books, Inc.,

System accidents occur because complex systems are susceptible to failures that interact with each other and/or with other components of the system in unanticipated ways to produce unexpected effects. The sheer complexity of these truly complex systems precludes the designers' anticipation of all of the problems that might occur or how failures might affect all of the other parts of the system (See Chapter 3. Information Infrastructure System Vulnerabilities, Risks, and Threats for further discussion of complexity's intrinsic effects for software (and, by extension, system) design and development).

Furthermore, the unexpected effects of the unanticipated interactions of system accidents are so unique that they cannot be solved at the time they occur to allow corrective action to be taken. For systems that are tightly coupled, this phenomenon can be disastrous because of the rapidity of their processes. Since correction or recovery is initially not possible, the initial effects may spread rapidly, or "cascade,"[47] uninterrupted from the point of origin throughout all connected parts of the system. Also, since the interactive complexity process is not well understood and is outside of the normal design parameters, attempts at corrective action might indeed make the problem worst. The unanticipated, unintended effects from these vulnerabilities have the capability to be as debilitating to U.S. national security as any malevolent action toward the United States.

Even Perrow admits that these types of accidents are "uncommon, even rare," but are of serious concern because of the disastrous results they can potentially produce. The

Publishers, 1984, 4-5.

[47] United States National Security Agency, National Information Systems Security (INFOSEC) Glossary, defines cascading as downward flow of information through a range of security levels greater than the accreditation range of a system network or component. I use the term cascading" to refer to effects moving through connected parts of the system (regardless of whether they are downward or not). These subsequent effects may be the same as in the preceding part of the system, but more likely, will have additional effects added as different parts react to the faulty input.

information infrastructure system is just such a complex system (as will be shown in Chapter 2. Information Infrastructure System) and is becoming increasingly more so with software/software and software/hardware integration and increasing interconnectivity with other systems.[48]

The research that follows is designed to test these concepts expressed as the following hypotheses:

H_1: The United States' national security can be imperiled by the inherent structural vulnerabilities of the information infrastructure system's:

1. open architecture system,
2. interconnectedness within itself and with other critical infrastructures, and
3. integration of software programs and software with hardware.

H_2: These three structural vulnerabilities can produce:

$H_{2.1}$: Disruption of the information infrastructure system and/or data exploitation

$H_{2.2}$: Causal uncertainty of observed effects in the information infrastructure system.

The research initially defines the vulnerabilities of the information infrastructure system and how these vulnerabilities jeopardize U.S. national security. Traditionally, a threat to a nation's national security is defined as a capability to exploit a vulnerability with the malevolent intent to inflict unacceptable risk on a target:[49]

$$\textbf{Threat}_{\textbf{traditional}} = \textbf{vulnerability + risk + capability + intent.}$$

[48] Perrow, 4-5.
[49] The White House, Critical Foundations: Protecting America's Infrastructures, 14.

In today's security environment, however, malevolent intent is sometimes difficult to determine or does not necessarily exist. A better definition of the threat to the information infrastructure system is the one selected in footnote 1 that is not dependent upon intent for consequences, i.e., any possible accidental or deliberate danger or harm to the system resulting in significant damage to or loss of resources:[50]

$$\textbf{Threat}_{\textbf{post-Cold War}} = \textbf{vulnerability + risk + capability}.$$

Such a definition better accounts for the reality of the current international security environment and the nature of the information infrastructure system. This definition allows the proposed research to include the notion that vulnerabilities of the information infrastructure susceptible to exploitation without any malevolent intent from a hostile individual or organization create risks that are also national security threats.

What are these information infrastructure system vulnerabilities? The information infrastructure system is vulnerable to a host of potential external attacks that could physically damage or destroy the infrastructure itself or internal attacks using the infrastructure as a means to access the system to access data or inflict damage or destruction.[51] External damage or destruction of the information infrastructure system is similar to physical attacks on other infrastructure systems fully or partially dependent on physical components and is well understood within the security community. The focus of this research is only on attacks that use the infrastructure to gain access to, to exploit, or to

[50] Boehm, 67-68.

The same definition may serve as the better definition for any of the more amorphous, indirect threats (immigration, drug trafficking, etc.) to U.S. national security.

[51] See United States White House, Critical Foundations: Protecting America's Infrastructure, for a complete description of the types of threats to the telecommunications and information infrastructures.

deny data generated, processed, stored or transmitted by the system. (See chart following for summary of information infrastructure system vulnerability types and their effects.)

In this formulation of the problem, the system itself is only the means to an end for a perpetrator to effect his action, not the ultimate goal. The data gained, denied, altered, or added to the system is the object that has the potential to harm the target, not the physical action upon the information infrastructure system to access the data.

INFORMATION INFRASTRUCTURE SYSTEM'S VULNERABILITIES & POTENTIAL EFFECTS

External (Discounted for this research).

- **Physical** – damage or destruction of system or system components

Internal

- **Open network architecture organization** – easy access; relatively easy movement w/in system
- **Interconnectivity** – within information infrastructure system and w/other critical infrastructure
  - access to other users and other critical infrastructure,
  - "cascading" effects,
  - interactive complexity
- **Integration** – software/software and software/hardware
  - software defects,[52]

[52] "Errors in larger computer programs are the rule rather than the exception" (Leonard Lee as quoted in H. Kopetz, Software Reliability, London: Macmillan, 1979, 154).

The literature's use of terms that define a breakdown in the normal software operations and processes of the information infrastructure system resulting in the possibility of unauthorized access, denial of service, unauthorized disclosure, unauthorized destruction of data, or unauthorized modification of data is imprecise and inconsistent.

Laprie, defines a system failure as a "deviation from fulfilling the system function," the latter being what the system is "intended for" is almost identical to the IEEE's definition. However, Laprie's definition of an error as part of the system state which is "liable to lead to subsequent failure" and a fault as the "adjudged or hypothesized cause" of an error are much less specific than the IEEE's (Laprie, "Dependability - Its Attributes, Impairments, and Means" in Randell, Laprie, Kopetz, and Littlewood (eds.), 4).

Landwehr, et. al. combines all of these terms that denote a malfunction in the processes of the information infrastructure system as a "security flaw" defined as "part of a program that violates its security requirements." NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, does not include the causes of security compromises. The Institute of Electric and Electronics Engineers' (IEEE), had planned to publish a standard glossary of computer security and privacy terminology, (Standard 610.9), but withdrew the PAR and no longer endorses the publication (Institute of Electrical and Electronics Engineers, IEEE Standards Status Report: Glossary of Computer Security & Privacy

•• "cascading" effects,
•• interactive complexity

The vulnerabilities (both external and internal) potentially can lead to compromise of the information assurance objectives through the following types of actions:

- **Insider Abuse** – authorized access to system, but unauthorized use of specific parts of system (Discounted for this research).
- **Intrusion** – unauthorized access to the system or parts of the system
- **Interactive Complexity** – unintended and/or unanticipated disruptions due to interactive complexity reactions
- **(Distributed) Denial of Service** – inability of system to receive or send data

Given the previous discussion and the first hypothesis, for the purpose of this research:

Vulnerability$_{iis}$ = open system architecture + integration + interconnectedness.

As previously stated, a risk that jeopardizes a nation's existence, health and welfare, or goals would be unacceptable. Pervasiveness and interconnectedness of the information infrastructure system along with ever-faster data delivery speed make the information

Terminology (Std. 610.9), Computer/Standards Coordinating Committee, Computer Society of the IEEE, 8 December 1998 (date provided by Paul R. Croll, Chair, IEEE Software Engineering Standards Committee, pcroll@csc.co).)

The Institute's IEEE Standard Glossary of Software Engineering Terminology (Std 610.12) was initially published in 1990 and has not been updated since. Unfortunately, there is some confusion even with this source. The Glossary contains four definitions for "error":

1. the difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition;
2. an incorrect step, process, or data definition;
3. an incorrect result; and
4. a human action that produces an incorrect result.

The Glossary also contains the following Note under the definition for "error":

> "While all four definitions are commonly used, one distinction assigns definition 1 to the word "error," definition 2 to the word "fault," definition 3 to the word "failure," and definition 4 to the word 'mistake.'"

Further, the Glossary contains the following Note under the definition for "failure":

> "The fault tolerance discipline distinguishes between a human action (a mistake), its manifestation (a hardware or software fault), the result of the fault (a failure), and the amount by which the result is incorrect (the error)."

I use the IEEE's definitions of the terms throughout the research since the Institute is one of the foremost authorities in information technology and provides standardization with the information science community.

infrastructure system indispensable to the American public and raise the liability of a vulnerability's exploitation to an unacceptable level. The risk to the information infrastructure system is the possibility of disruption of the system's operation and exploitation of the system's data.

$$\mathbf{Risk_{iis} = dependency}$$

$$\mathbf{Dependency = pervasiveness + interconnectedness + data\ speed}$$

$$\therefore\ \mathbf{Risk_{iis} = pervasiveness + interconnectedness + data\ speed}$$

Capability is relatively easy and cheap to acquire.[53]

$$\mathbf{Capability_{iis} = easy + cheap}$$

All that is needed to complete the traditional national security threat relationship is malevolent intent. Within the security environment of today, there are certainly perpetrators that might intend malevolence for the United States, e.g. hackers, criminals, terrorists, and other nations. However, as previously stated, malicious intent is not always a necessary condition for a threat to jeopardize the information infrastructure system and U.S. national security.

1.3. Discussion.

"Basic to scientific research is the process of comparison, of recording differences, or of contrast."[54] Before comparison or contrast can proceed, however, a detailed

[53] "It doesn't take much capability to attack these infrastructures. It takes a computer or a few computers and some good hackers. All they need is a malicious intent and a few thousand dollars in equipment" (John C. Davis, National Security Agency commissioner to the President's Commission on Critical Infrastructure Protection in Slabodkin, 3).

"The number of computers on the Internet and the difficulty of configuring them securely mean that attackers have more chances of finding a way into systems than they did a decade ago. Along with low-cost Internet access, computers are inexpensive and the price is dropping. This means that more attackers can afford both the computer and Internet access needed for an attack" (Robert Vibert, "Who's to Blame for This New-Found Love?" May 2000. http://www.vibert.ca/wholove.htm).

description of the research subject has to exist. At this point, the vulnerabilities of the information infrastructure as a system have not been comprehensively described. Much research and effort have been devoted to examining and designing countermeasures for vulnerabilities of various components of the system, but this granular research has generally not been aggregated and published as a systemic analysis.

I begin by describing the information infrastructure system to define the research subject and its bounds. The information system's infrastructure can best be understood from a global perspective. The Global Information Infrastructure (GII) is envisioned as the system. The envisioned GII is a conglomerate of numerous sub-systems globally (the National Information Infrastructure (NII) is the conceptual subsystem within the United States) that connect with each other.[55]

Each sub-system, in turn, is composed of numerous other sub-systems that are interconnected with each other, [e.g., the NII is composed of the Government Information Infrastructure, the Department of Defense Information Infrastructure (DII) and other governmental and non-governmental sub-systems (e.g., energy, financial, transportation, corporate, etc.)] for seamless movement between systemic levels. Each of these subsystems could then be composed of additional subsystems.[56] Because of interconnectivity between

[54] Donald T. Campbell and Julian C. Stanley, Experimental and Quasi-experimental Designs for Research, Chicago: Rand McNally & Company, 1963, 6.

[55] The Internet is only another component of the GII. Like the GII, the Internet encompasses the world but does not have the breadth and depth of the anticipated GII (Ronald S. Eward, "Telewar: The Physical Vulnerabilities of a Global Electronic Economy," in Schwartau, Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age, 217).

[56] United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future, A Report by the Committee on Information and Communications, National Science and Technology Council, Supplement to the President's FY 1996 Budget, September 1995, 29 and Horton, 14-18.

the subsystems, once a sub-system's vulnerabilities are exploited the results will be transported across the entire subsystem and any connected subsystem(s).[57]

Four categories of potential intruders seem to exist: mischievous, criminal, terrorist, and state. The common lure for the four is the generally relatively slight effort required[58] and the low risk of getting caught. The reward an intruder receives from gaining unauthorized access to a system or degrading a system's capabilities determines his motivation and affects the degree of effort he is willing to expend for a successful attack. Rewards generally are positive (e.g., personal satisfaction, monetary gain, revenge or simply pure curiosity), but may also be negative (e.g., notoriety gained from detection). Each intruder may be expected to apportion his effort optimally according to his view of potential rewards. When the potential for reward is great enough, even absurdly difficult attacks become plausible, e.g., the Hanover Hacker who persisted for over two years to gain unauthorized access to U.S. defense information.[59]

Mischievous agents perpetrate their threat from a sense of thrill seeking, one-upmanship, and a desire to do something forbidden or difficult without being caught. Although their intent is not necessarily malevolent, harm may occur inadvertently or as a

[57]Firewalls, encryption, and procedural and technical measures have been designed to protect the information system but still have not obviated successful exploitation of its vulnerabilities (United States National Security Telecommunications Advisory Committee (NSTAC), Issue Review: A Review of NSTAC Issues Addressed Prior to NSTAC XIX, 8).

[58]Effort is a variable composed of several factors: the attacker's education, skill, and experience as well as time, money and other resources spent by the attacker. Effort should capture the intuitive notion that the more effort invested in attacking the system, the greater the chance of achieving a breach (Olovsson, et.al., "Towards Operational Measures of Computer Security: Experimentation and Modeling" in Randell, Laprie, Kopetz, and Littlewood (eds.), 555-556 and Geer).

[59]The subjective view of one intruder may be different from other intruders' views in similar circumstances leading to different rewards being received from a similar attack by different intruders (Olovsson, et.al., "Towards Operational Measures of Computer Security: Experimentation and Modeling" in Randell, Laprie, Kopetz, and Littlewood (eds.), 555-556 and Geer).

consequence of their action anyway. For this reason, mischievous agents should be considered threats to the information infrastructure system.

Criminals perpetrate their actions for gain. Just like the average citizen, criminals and criminal organizations have become more sophisticated in their use of the current information technology to achieve their ends. Numerous cases of cyber-crime involving electronic theft, money laundering, fraud on line, pedophile rings, extortion, and the theft of information system components (particularly computer chips) are documented in the open press, trade publications, and law enforcement reports.

According to Matthew G. Devost, Brian K. Houghton, and Neal A. Pollard of Science Applications International Corporation, terrorists make demands or gain attention through "the intentional abuse of a digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action."[60] Identified terrorist groups that use or have used the information infrastructure system to their advantage include religious zealots, political groups including U.S. domestic militias, and millennium groups. These groups use the information infrastructure system to help finance their campaigns through criminal activity, to maintain records, to plan their operations, to keep track of their adversaries, or to manipulate information to galvanize support or propagate disinformation as well as to inflict damage on targeted information infrastructure system assets.[61]

[60] Matthew G. Devost, Political Aspects of Class III Information Warfare: Global Conflict and Terrorism, Presentation Notes, Second International Conference on Information Warfare, Montreal, Canada, January 18-19, 1995.
[61] Molander, et.al., "Strategic Information Warfare: A New Face of War," 5.

Like the other three types of agents, state perpetrators can either be individuals or an organization, but a state agent is always state sanctioned. State agents use the information infrastructure system to stay abreast of developments in the targeted nation, to gather data that might give them or one of their strategic industries a competitive advantage,[62] to compel another nation or alliance to do the their will, or to attack another nation or alliance.

The information infrastructure system provides a state with the capability to asymmetrically threaten other states.[63] Offensive use of the information infrastructure system appeals to many states since there is no obvious need to invade the targeted nation's homeland thereby reducing the potential for human losses and the costly acquisition of massive amounts of military hardware. John Deutch, Director of Central Intelligence, has said, "There is evidence that a number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks."[64]

[62] Marian Myerson, Risk Management Processes for Software Engineering Models, Boston: Artech House, 1996, 8.

According to the FBI and CIA, the greatest threat to U.S. security is industrial and technological espionage by foreign powers - foes and friends. The U.S. General Accounting Office reports that five U.S. allies spy on U.S. companies. (Myerson, 20) France, along with the governments of China, Taiwan, Japan, South Korea, and Britain, is spying on U.S. companies to obtain confidential economic information as well as trade secrets. The French government has:

- lodged U.S. business executives and defense officials in bugged hotels;
- seated targets in bugged Air France seats;
- recruited French employees of the U.S. Embassy in Paris;
- placed moles (someone with loyalties to an entity or government other than the one for whom they are ostensibly working or to which they profess loyalty) in U.S. computer firms;
- tapped phone lines;
- looked through stolen garbage; and
- posed as nondefense customers to obtain classified technology secrets (Frank Greve, "French Techno-Spies Bugging U.S. Industries," San Jose Mercury News, October 21, 1992, F1).

[63] Asymmetrical strategies allow a state to indirectly threaten a stronger state that possesses battlefield superiority through indirect use of some combination of nuclear, chemical, biological, highly advanced conventional and strategic information warfare instruments ("Strategic Warfare Rising," 1).

[64] United States Congress, Senate, Select Committee on Intelligence, "Worldwide Threat Assessment," Testimony of John Deutch, Director of Central Intelligence, 104th Cong., 2nd sess., February 22, 1996.

The postulated vulnerabilities of the system can enhance an intruder's anonymity (and reduce the risk of being caught) by allowing initiation of an activity from a distance, through other users' components, or with a time delay, if desired. An intruder can even disguise the activity to resemble an accident instead of an attack. The possibility of discovering the real perpetrator(s) is thus reduced and immediate retaliation forestalled.[65] The result of this anonymity is that the victim does not have a clear idea from where, by whom, or the purpose, scope, and intent of an attack. Such uncertainty impedes the decision making process.

At the time of an event, national decision makers may not be able to determine whether the event is an accident, a system failure, hacking by "thrill seekers, a purposeful attack by terrorist or some other state, or simply the cascading results of a systemic fault or interactive complexity. The foremost consequence of such a situation is that these decision makers may not be able to determine when an attack is under way, who is attacking, or how the attack is being conducted. A further consequence at the national level is the lack of jurisdictional clarity between law enforcement and national security and intelligence entities for assessing, monitoring, and responding to any such event.[66] (See Chapter4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy for a more in-depth discussion of the jurisdictional issue)

In order to verify the vulnerability of the existing information infrastructure system postulated by the research, one would need to provide empirical evidence of a compromise

[65] David Bicknell, "US Defence Calls For Security Testing," Computer Weekly, January 9, 1997, 2.

[66] Molander, et.al., "Strategic Information Warfare: A New Face of War," 4 and 5.

See Molander, Roger, Peter A. Wilson, Andrew S. Riddile and Michelle K. Van Cleave. The Day After...in the American Strategic Infrastructure. The RAND Corp. January 9, 1998 for a simulation scenario for senior government decision makers that approximates the situation just described.

of each of the five information assurance objectives. Given the interconnectivity of the information infrastructure system, effects of an information assurance objective's compromise in one system or subsystem conceptually are able to migrate to other systems and/or subsystems from the initial point of compromise. Therefore, evidence of a compromise of an objective in only one system or subsystem instead of all of the systems or subsystems of the information infrastructure system should be all that is needed to demonstrate the vulnerability.

Conceptually, compromise of the objectives could occur from a variety of sources, e.g., interruption of the power source, lack of attention by the operator, insider abuse, etc. An intruder, however, is singularly capable of compromising all of the objectives. Because of this, an intruder represents the worst case for compromising the security of the entire information infrastructure system (See Figure 1.1. Optimum IA Objectives Research Design below for research design of information assurance objectives' compromise by categories of intruders).

However, given that difference between categories of intruders is only one of intent or of resources available, all one would really need to document the vulnerability of the entire information infrastructure system are compromises of the information assurance objectives by any intruder.[67] For these reasons, an acceptable alternative to the previous research design would be to select a case that incorporates only the least likely conditions. A case that demonstrates compromise of the objectives in a system or subsystem that has (or

[67] Any and all categories of intruders conceptually can perform the same actions. Hackers normally work individually or in loose collaboration with other hackers using only their own resources. However, criminals, terrorists, and states (or their agents) would in theory have much greater resources at their disposal to attack the information system's infrastructure.

should have) an extremely high degree of security by an intruder with the least resources and with the least expectations of gain would be such a case.

Information Assurance Objective		Categories of Intruders		
	Mischievous	Criminal	Terrorist	State
Confidentiality				
Availability				
Integrity				
Authorization				
Non-repudiation				

Figure 1.1. Optimum IA Objectives Research Design

Such a case would logically allow generalization across the spectrum of conditions since all other conditions would be less difficult to obtain than the one selected.

Hackers from anywhere on the GII with successful penetration of the Defense Information Infrastructure would seem to meet these criteria. The Defense Information Infrastructure is singularly critical to the nation's ability to respond militarily to traditional conventional threats and should logically incorporate the most stringent, comprehensive counter-measures to safeguard its sensitive data.[68] Fortunately, classified networks within the DII are physically separated from its open network system component with the result

[68] The Pentagon's own computers were penetrated more than 100,000 times in 1996 alone. Before the Gulf War, someone even stole military secrets, including troop movements, and offered to sell them to Saddam Hussein, who apparently didn't believe they were real ("Computers: World Wide Warfare," ABC Nightline, ABCNews, December 8, 1997).

that an intruder of the open network system theoretically cannot access classified networks.[69] Unfortunately, other federal government systems do not have the foresight or means to separate physically their classified, national security, or sensitive files or systems from the open network system of the GII or NII.

The case of Kevin Poulson demonstrates how a lone hacker without an overwhelming desire for gain can use the system's vulnerabilities to access extremely sensitive information in FBI files (national), business systems and files [to include the banking system (reportedly is the most secure of all business systems) and Pacific Bell (considered by hackers to be among the most secure in the telecommunications industry")],[70] and individuals' files thereby compromising the confidentiality of the data. Poulson also compromised the other four information assurance objectives during his escapades (See the case study at Appendix A for a detailed account of Poulson's exploits). There is little empirical evidence that Poulson used the full extent of the GII to achieve unauthorized access to files, but with the seamless nature of the global information infrastructure there is no doubt that he could have if he either wanted to or needed to.

Poulson was able to compromise all of the information assurance objectives single-handedly because of his extensive knowledge of computers and the telecommunications system. Also, his expertise was so exceptional that he could "hack the computers (switches)

[69] Conversation with Dr. Tom Longstaff, Senior Member of the Technical Staff, Computer Emergency Response Team Coordination Center, Carnegie-Mellon University, February 4, 1998; telephone conversation with Gary "Gus" Guissane, DoD, Office of Information Security, May 18, 1998; and confirmed by Targowski, 144.

Encrypted portals do exist between the separated classified and unclassified networks, but to date no unauthorized intrusion of the classified networks has been acknowledged. Telephone conversation with Gary "Gus" Guissane, May 18, 1998.

[70] Jonathan Littman, The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulson, Boston: Little, Brown and Company, 1997.

of Pac Bell to gain control of the telephone system's switches. As Winn Schwartau says in Information Warfare, "...he who controls the switch wields immense power..."[71]

Poulson took advantage of the switch's maintenance ports normally used to turn phones on or off, reroute calls, or give calls free billing to gain unauthorized access. Since the telecommunications infrastructure is the backbone of the information infrastructure system, once in the system he was able to use other vulnerabilities of the telecommunications system to gain unauthorized access to other components of the information infrastructure system and then use their vulnerabilities and his computer skills to access virtually any sub-system or file he wanted. As Jonathan Littman in The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulson reports, "simply by the force of his hacking, Kevin proved that the communications infrastructure that we rely upon for banking, commerce, and even national security is far more vulnerable than we imagine."[72]

As improbable as it seems, Poulson was able to accomplish this without the benefit of formal education or computer training. His knowledge of computers and the telephone network came from old phone company manuals, observation of phone company equipment, computer programming manuals, and trial and error experiments. If a lone individual without resources or formal technical training could do this, what would organizations or nations with adequate resources and malevolent intent be able to accomplish?

[71] Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway, New York: Thunder's Mouth Press, 1994, 123.
[72] Littman, 276-282.

A special threat to the information infrastructure system deserves mention because of its perniciousness and the degree of damage it produces (or, at least, potentially can produce) to the entire information infrastructure system: denial of service (DOS) or, in its latest contemporary form, distributed denial of service (DDOS). A (D)DOS attack is typically initiated against a server,[73] router,[74] or any number and combination of these by an intruder intent on putting the system at risk. What makes a (D)DOS attack so insidious is that many of them do not even "require direct access to the systems being attacked. Instead, those attacks are able to exploit fundamental architectural deficiencies external to the systems themselves rather than just widespread weak links that permit internal exploitations."[75] Conceptually, it is possible that a (D)DOS attack could be precipitated by one of Perrow's system accidents although to date there is no evidence that such an attack has ever occurred.

In a (D)DOS attack, a server(s), router(s), or buffer(s) (or several of each) are overwhelmed to the degree that they can no longer function. Consequently, connectivity of the information infrastructure system is interrupted thereby disrupting the availability of service to all users of the targeted server(s), router(s), and/or buffer(s). Generally, such an attack is initiated with a virus or worm and is not a direct attack on the server(s), router(s), or buffer(s) but produces secondary effects that effectively overwhelm the target by creating more message traffic than these components have the capacity to service. When this

[73] A server is a basically a computer that serves as the interface to direct data or message traffic between a host and the rest of the information infrastructure system.

[74] A router is a computer that serves to direct data traffic, analogous to a switch in the public switched (telephone) network in the information infrastructure system.

[75] Peter G. Neumann, "Denial of Service Attacks," Communications of the ACM 43, no. 14 (April 2000), 136.

happens, the component shuts down and ceases to function until the flood of incoming messages is interrupted.

There are numerous instances of deliberate (D)DOS attacks beginning with the first documented attack against the system (the 1987 Morris worm) and continuing through today. Several attacks have gained notoriety because of the extent of damage they caused and name recognition of some of the affected customers, e.g., the Love Bug which interrupted service to Yahoo and E-Bay. I will use various cases to illustrate the vulnerabilities this type of attack's targets, the effects such an attack can have, and the damage they can produce to the information infrastructure system (See Appendix B. Denial of Service for a detailed account of DDOS attacks and their effects).

The research so far should provide a comprehensive picture of the information infrastructure system's vulnerabilities and the consequences of their exploitation. Since my primary focus is how the information infrastructure system's vulnerabilities affect the United States' national security, I also examine the Federal government's information infrastructure system's national security policy and IT security research and development over the decade of the 1990s with particular attention on the Clinton administration's efforts. Such a longitudinal examination should provide the continuous empirical evidence of the Federal government's understanding of the information infrastructure system's vulnerabilities and actions taken to compensate for those vulnerabilities. As indicated previously in this section, the inherent vulnerabilities of the open system architecture, interconnectivity, and integration will be enduring as the product of policy and market decisions. Therefore, little can be done to change those conditions and any actions or policy to remedy system vulnerabilities will have to take those conditions into account.

1.4. Research Results.

The research was accomplished using documents from the federal government, industry, and academia, as well as through interviews with government officials and others (e.g., CERT, DoD) with oversight of the information infrastructure system and its security. Since the information infrastructure system is primarily privately owned, much of the research was aimed at those representatives of industry that have knowledge of both the infrastructure and its security implications (e.g., Information Technology Association of America (ITAA), International Computer Security Assoc., Mitre Corp., Assoc. for National Defense and Emergency Resources, etc.). Further details of Kevin Poulson's exploits and the Morris and Love Bug virus attacks can be found from hacker's publications, bulletin boards, federal and state court records.

The research is introduced in this chapter, Introduction, providing the purpose, scope, and theoretical and conceptual foundation along with an overview of the intended research. The framework for analyzing the threat to the United States information infrastructure system is defined, the risks specified, the nature of the threat defined, and the agents who conceptually have the capability and intent to exploit the vulnerabilities established. The notion of system accidents and decision makers' uncertainty of effects' origin and their effects on America's national security through the information infrastructure system is introduced and explained.

Chapter 2. Information Infrastructure System describes and defines the information infrastructure and its boundaries. The description begins with the most elemental components and incrementally aggregates the components to the system's highest conceptual level (Global Information Infrastructure). The concept of an open network architecture is described and illustrated and those system characteristics, to include its connection with other critical infrastructure and progressive integration, are explained.

Chapter 3. Information Infrastructure System's Vulnerabilities, Risks, and Threats analyzes the defined information infrastructure system for inherent structural vulnerabilities. The model of smallest to largest aggregation of components established by the description of the system is used for this vulnerability analysis. Vulnerabilities in individual hardware and software components of the computer system, as well as their integration, the open network architecture nature of the infrastructure, and its interconnectivity within its subsystems and with other critical infrastructure are identified and explained. Any identified vulnerabilities of the open network architecture, interconnection, and integration will be examined for synergy as they combine within the infrastructure system.

The chapter concludes with two studies that are particularly relevant: one of Kevin Poulson' intrusion activities and one on denial of service. Each demonstrates different systemic vulnerabilities of the information infrastructure system and the effects of their exploitation. Intrusion represents the worst case for a system end-user: possible compromise of the sanctity of data through manipulation, change, deletion, or theft. Denial of service represents the worst case for the network or system, whether limited to one end-user or to larger segments of the system itself: compromise of the system's very raison d'etre, the ability to connect with and transmit data to others. Kevin Poulson's case provides an analysis of a lone hacker exploiting the "brains" (public network switches) of the infrastructure system through the vulnerabilities of ease of access, anonymity, and interconnectivity. It affirms the extreme case of a single intruder and leaves little doubt about the possibility and degree of vulnerability exploitation by intruders with support from groups or nations with malevolent intent. The case study of distributed denial of service (DDOS) provides a description of this particular type of systemic risk and its ease of implementation.

Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System National Security Policy provides a longitudinal review, with particular emphasis on the Clinton administration, of the nation's policy response to the information infrastructure system's vulnerabilities and their risks to national security. The policies of the Clinton administration bring into focus the contemporary debate about confidentiality surrounding the security issue and highlight the government's policy efforts during the 1990s. The chapter also analyzes from an organizational perspective why there has been such little policy development in this area.

Chapter 5. Information Infrastructure System Security and Information Infrastructure System Security R&D Funding details the federal government's spending over the decade of the 1990s for both information infrastructure system security and system security R&D. The paucity of both reinforces the lack of commitment by the government to address the national security risk of the system, especially after specific public support for both by the Clinton administration.

Chapter 7. Conclusions and Recommendations suggests that some type of risk management response strategies should be adopted. A mix of mitigation and risk reduction strategies drawn from Wildavsky's "searching for safety" and Perrow's "normal accidents" seems to be both prudent and relevant. Aaron Wildavsky's strategies are founded on the notion that there will always be dangers that cannot be neutralized and the need to develop strategies to cope with that fact. He bases his response to those dangers on strategies of anticipation or resiliency depending on the degrees of uncertainty and risks involved. Charles Perrow's "normal accident" strategies are based on the dangers he see in modern technologies: extremely complex and too tightly coupled which leads to interactive complexity and system accidents. Perrow's strategies prescribe loosening the coupling of the technology and separating complex components so they might be isolated if things begin to go wrong.

CHAPTER 2

INFORMATION INFRASTRUCTURE SYSTEM

> "The information infrastructure is extremely complex. There is no simple way to define it, to establish its bounds, to measure its impact, or to identify clear responsibilities for the evolution, operation, maintenance, and repair of the infrastructure."[76]

2.1. Introduction.

One can be excused for confusion regarding the term "information infrastructure" since there is little consensus even among researchers about much associated with it. However despite the forewarning of the quote, the proposed research compels both a definition and an understanding of the information infrastructure system be provided. In this chapter I will provide a systematic description of the system beginning with the basic components and progressing through increasingly abstruse aggregate levels to the Global Information Infrastructure (GII). I will also include anticipated trends that should shape the infrastructure for the future and, more than likely, introduce new vulnerabilities.

2.2. Infrastructure Basic Elements.

In the broadest sense, the information infrastructure consists of data and information and the means to create, gather, process, store, and transmit or receive that data or information.[77] Even given this accepted scope of what an information infrastructure system definition should include, there is still little consensus on a definition. The major issues thwarting consensus are:

[76] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-15.

[77] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-15-16.

These means are generally acknowledged to include, as a minimum, the equipment, facilities, and telecommunications that manipulate and transmit the data and information.

- the inclusion or exclusion of users and operators as a discrete component in the creation, gathering, processing, storing, transmitting, and receiving of data and information and
- the subsequent organization of the elements selected for inclusion.

Even among those definitions where users and operators are included, there can still be wide variation in the organization of the elements. For example, the Defense Science Board in its 1993 Summer Study, "Information Architecture for the Battlefield," restricted its description to six basic elements: "hardware (computer, entry, output, and display devices, storage media, and facilities), operating software (system), application software (including data base software), communications devices and links, data, and the people who have been trained to operate or maintain one or more of these elements."[78] Forest Horton, on the other hand, includes nine basic elements, including users and operators, in his description.[79]

My own definition relies heavily on Horton's scheme in Towards The Global Information Superhighway: A Non-Technical Primer for Policy Makers. I elected to use Horton's scheme to present the most comprehensive case initially then exclude those elements considered not necessary for this research. My rationale and methodology should become clearer as the systematic description progresses through successive aggregations.

In Horton's construction of an information system, the nine major components of an information infrastructure system are:

[78] United States Department of Defense, Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield, Defense Science Board, Washington, D.C., October 1994, B-14.

[79] Horton, 14-15.

1. **Users**. The producers and consumers of information products and services the system provides.

2. **Operators and providers**. The technical experts who provide and operate the channels, sources of information, system and network functions, and other tasks necessary to keep the infrastructure functioning, and the managers who control and regulate the system.

3. **Computers and microprocessors**. Devices that generate and receive the data that move on the infrastructure. Along with the telecommunications network, these devices and computers are the "hardware," or equipment, of the infrastructure. Computers link users to the information infrastructure system through one or more of the following input-output (I/O) devices:[80]

•• monitor – a device with either a passive or interactive screen that displays the data or information;

•• keyboard – a device similar to a typewriter to manually enter data;

•• modem – a device that connects the computer to a transmission medium;

•• printer – a device that physically transforms electronic data to print;

•• fax – a device that digitizes text or graphics to transmit a replica of an original text or graphic or translates digital data into text to print a replica of a transmitted text or graphic;

•• video and audiotape – media for storing, handling and communicating information on strips of magnetic or optical film material;

[80] The following list of input/output devices is representative of those that are available today. I/O devices are being developed constantly to increase the formats by which data is entered into or extracted from the information infrastructure system, e.g., voice recognition devices.

•• camera – a device for photographing an object onto film from which it can further be disseminated in digital, analog, or photographic form;

•• scanner – a device that transforms printed or photographic data into digital data;

•• microphone – a device to auditorily enter data;

•• speakers – devices that produce audio output from digitally transmitted data; and

•• the entire class of devices that store and input digital data directly into the computer, such as the floppy and compact disks, zip drives and disks, and portable hard drives.[81]

In addition to the terminal computers just discussed, a computer (a "server") manages the technical details of communicating with other domains[82] while yet another computer (a "relay" or "switch") may manage data transmissions between servers.[83]

4. **Software and standards.**[84] Programs and rules that simplify, streamline, and accelerate the interconnectivity and interoperability of the hardware components and the interfaces between the infrastructure, users, and the transmission facilities. Telecommunications or networking standards address such issues as the transmission media between communicating systems, type of interface between a

[81] Horton, 14-15.

[82] A domain is any group of users who use the same suffix in their electronic address, e.g., ".edu, .org, .gov." A domain can be local (local area networks - LANs), sub-regional (MANs or RANs), regional (wide area networks - WANs), supra-regional, sub-global, and global (global area networks - GANs) as long as the grouping uses the same domain address (Horton, 16).

[83] Horton, 16.

[84] A standard is a formally adopted and widely accepted rule that describes an agreed-upon way of doing things at the national (the American National Standards Institute (ANSI) in the United States) and international levels [the International Standard Organization (ISO)] (Horton, 29-30 and Targowski, 225).

computer system and transmission medium, format of transmitted message, length of transmission, and all other aspects of information exchange between two devices with respect to the following five principles:

- •• **Interoperability**: the ability of two or more components of a system or network to interact with each other so applications can work in a heterogeneous environment;
- •• **Portability**: the ability to move applications easily between platforms;
- •• **Scalability**: the ability to downscale or upscale applications;
- •• **Heterogeneity**: the ability to support applications on different platforms, and
- •• **Distribution**: the ability to use resources and processes on any system on the network.

A sophisticated contemporary network to support multimedia communication uses key standards in the following categories:

- •• **Operating system** – determines how the computer operates and locates files that are stored on the computer,
- •• **Application program** – a programming interface designed to let software applications execute over a transmission network,
- •• **Router** – a hardware/software combination that directs messages between local area networks,[85]
- •• **Bridge** – a less powerful software/hardware combination similar to a router that directs all messages received without consideration of priorities,[86]

[85] Horton, 16-18.

•• **Domain** – scheme for translating numeric addresses into strings of word segments denoting user names and locations (See footnote 32 for the definition of a domain),

•• **Finger** – determines whether another user is logged onto the network or finds a user's e-mail address,

•• **Search tools** – present information available from a given source in a hierarchical, logical menu,

•• **Internet relay chats** – make possible real time keyboard conversations online,

•• **Network driver interface and open data-link interface** – allow multiple transport protocols to run on one network card simultaneously,

•• **Wide area information server (WAIS)** – indexes large text files in servers, and

•• **Protocols** – serve as a set of rules to manage all traffic received and sent to ensure host and network compatibility, interconnectivity, and interoperability. Unfortunately, not all protocols (e.g., file transfer protocols (FTP), Internet protocols (IP), network news transport protocols, serial line Internet protocol/point-to-point protocols, mail transfer protocols, network management protocols, transmission control protocol/internet protocols (TCP/IP), and telnets) are compatible.[87]

[86] Mara Lee, "Creating the Ultimate Network," Washington Technology: Tech Business. December 7, 1995.
[87] Horton, 16-18.

5. **Telecommunications networks.** The physical conduits that move messages and data through the infrastructure between end users.[88] The telecommunications media are the single significant component of the information infrastructure system that is not under the direct administrative control of the computer system management for key functions such as maintenance and operation. It is also, obviously, the most geographically diverse and complex element in any networked computer system and, as such, makes accurate quantification of threats and risk assessment extremely difficult.[89]

Over the years, the telecommunications network has evolved from a hodgepodge of wires, mechanical switches and relays to a system dominated by computerized switches and relays[90] with expanded bandwidth and carrying capacity through a combination of the following mediums:

•• Cable: wire, twisted pair (multiple wires bundled together), and optical fiber.[91]

[88] Horton, 15.

[89] Dennis Willets, "Telecommunications Security" in K. M. Jackson and J. Hruska (eds.), Computer Security Reference Book, Boca Raton, FL: CRC Press, Inc., 1992, 732.

[90] Horton, 15.

[91] Glass fibers are considered to be the carrier of choice for the future because of its capacity to carry new, higher-bandwidth applications (such as digitized video) and the promise for reengineering the infrastructure to carry higher quality and more reliable basic telephone service at lower cost (Horton, 15 and 170 and Targowski, 350).

Although fiber is widely deployed between central offices, only a small fraction of the total local-loop network is fiber-based because of the prohibitive costs of installation to the individual retail customer. Very large investments will be required to achieve any substantial upgrade not only in U.S., but also global, communications facilities (Horton, 170 and National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, NII 2000 Steering Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, Washington, D.C.: National Academy Press, 1996, 11 and 13).

A future trend is to look to the power industry as an infrastructure provider. Electric utilities invest in replacing wires on a regular basis since wires carry a risk of failure over time. The industry has observed that the incremental cost of including a fiber-optic cable inside its ground wires is very low which naturally suggests that investment in fiber represents a good risk as a basis for entering new business

•• Satellites: relay stations in orbit above the earth's atmosphere, and

•• Microwave: wireless communications.[92]

The transmission medium for an information infrastructure system in the United States is generally accepted to be the existing public telecommunication system.[93] The more than 1,300 local operating companies, or local exchange carrier (LECs), represent the access point to connect end users at homes, businesses, and other locations to the telephone network, switches, and trunks and interchange carriers (IXCs), or long distance carriers.

There are about 450 IXCs in the United States, most of which resell capacity purchased from other, facilities-owning carriers (e.g., AT&T, MCI, and Sprint). IXC networks form backbones[94] carrying traffic between separate local areas through switches and interoffice trunk lines. Communications that leave the local telephone company's service area must pass over facilities owned by long-distance carriers and terminate on facilities owned by other firms, such as other LECs and wireless (primarily cellular) carriers.[95]

Switches are the brains of the telecommunications system that route the data to the destination(s) the consumer chooses. More importantly for this research, large phone switches are among the most complex systems on earth, using about 10 million lines of software code to make sure calls are handled and billed properly. Within the U.S.,

opportunities. Because it does not carry an electrical current, fiber is a natural means to transport control signals through a utility's power grid (National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 145).

[92] Horton, 15.

[93] Brian Hayes, "The Infrastructure of the Information Infrastructure" American Scientist 85, no. 3 (May-June 1997), 216.

[94] A "backbone" is defined as a central high-speed network (normally understood to be the public telephone network) that connects smaller, independent networks (Horton, 16).

[95] S. Arnold Berger, "Co-Verification Handles More Complex Embedded Systems, Part I," Electronic Design 46, no. 6 (March 9, 1998), 166.

telephone switching is organized into a hierarchy of switching networks that routes traffic first to the lowest level and then to progressively higher levels if the selected level is busy.

•• Class 5 – the lowest level of about 20,000 switching centers called end offices (toll free) that directly serve the customer via a local loop.

•• Class 4 – about 1,300 toll centers that apply higher rates.

•• Class 3 – about 265 primary centers.

•• Class 2 – about 75 sectional centers.

•• Class 1 – 12 regional centers (10 in the United States and 2 in Canada) with approximately 7.9 million numbers that can be potentially assigned to customers.[96]

Even more relevant to the research, the utilities are in the process of converting their switches to asynchronous transfer mode (ATM)[97] technology capable of handling 10,000 data lines to generate huge amounts of new revenue-producing traffic. These ATM switches can be run by outside processors so the switches themselves do not require the millions of lines of expensive, complex software code to provide services such as "call-waiting" and "caller ID."[98] With considerable amounts of complex software and off-site processing, switches are more efficient, but at the same time more vulnerable to intentional and unintentional risks and are, therefore, extremely important to the security of the entire information infrastructure system.

[96] Targowski, 53.

[97] Asynchronous Transfer Mode (ATM) is "fast packet switched" cell relay technology in which fixed 53-byte size packets of data are rapidly routed over a network (much the same way Internet traffic is transmitted) (United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future, 10).

[98] Targowski, 51-53.

6. **Information content.** Information content is all data that are in machine-readable (e.g., binary) or human-readable (e.g., an ASCII text) format regardless of handling, storage, or retrieval medium (i.e., voice, graphic, text, numeric data, multi-media, interactive, etc.) or packaged form (i.e., single messages, packets of messages or data, files, blueprints, etc).

7. **Applications.** Software to create, access, manipulate, organize, store, preserve, integrate, manage, interact and utilize the information content. These functions can be in text only or multimedia format with passive, interactive, or "virtual reality" (television- or movie-like) presentation.

8. **Materials and supplies.** Logistics needed to operate the hardware and software and support the users, operators, and providers of the network and systems.

9. **Financial resources.** Money needed to fund, develop, operate and maintain the infrastructure system on a fully functioning basis.[99]

2.3. An Information Infrastructure System.

Combinations of these components providing communications and connectivity between users create a network to permit data transfer, database inquiry, program development and/or on-line transaction processing that is an information infrastructure system. [100] Although the number, speed, sophistication, and abilities of computers have

[99] Horton, 10-11.

[100] The DSB uses similar conditions to define an information system in its 1997 report on information warfare:

> "An information system is defined as the organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. This includes the entire infrastructure, organization, and components that collect process, store, transmit, display, and disseminate information. It includes everything and everyone that performs these processing, and using the information functions - from a laptop computer to local and wide-area voice and data

increased almost geometrically in the past decade, the greatest change in computer technology has been the proliferation in the number and use of these computer networks. Beginning in the 1970s and throughout the 1980s and 90s, computers increasingly became connected by networks that permitted computer users to share the information and resources of remote computers.[101] Computing power (the speed with which the computer can perform functions), software programs, and domains[102] still dictate the flexibility, - or, the speed, efficiency, and effectiveness – with which one can navigate these interconnected components, but the networks created altered the way computers were, and are, used in society.[103]

Such a combination of components when considered as a network should also be considered a system[104] since it takes a combination of the components to perform the common purpose of data transfer (See Figure 2.1. Archetypical Information Infrastructure System for the simplest combination of the discussed components as a system). With only individual components, the function of data transfer cannot be performed. This distinction

networks, broadcast facilities, buried cable and, most importantly, the people involved in transmitting and receiving" (United States Department of Defense, Report of the DSB Task Force on Information Warfare (Defense), App. C – "A Taxonomy for Information Warfare").

[101] Mark Rasch, "Criminal Methods of Attack on the Internet" in Ruthberg and Tipton, S-343.

[102] 1. power of the user's own computer - the greater the power, the faster, more efficiently and more effectively one can search, organize, retrieve, format, etc. the different software functions and send the data to the desired end location.
2. power of the host computer - the greater the power, the quicker and more efficiently access, navigation and exit of the interconnected components will be accomplished.
3. software packages installed on the user's and host computer - different packages are necessary to allow one to access, navigate, and perform other functions with the interconnected components.
4. domains - rules for entering domains often are different requiring more time and different software to access (Horton, 17).

[103] Horton, 17.

[104] According to Webster's Ninth New Collegiate Dictionary, a system is a group of devices or artificial objects or an organization forming a network especially for distributing something or serving a common purpose, e.g., a telephone system, a data processing system. In this case, the connectivity provided by the combination of components can easily be considered to be a group of devices forming a network to serve the common purpose of distributing data.

of the infrastructure as a system is important to the core of my hypothesis. In a system, a vulnerability in one component affects not just that component but the entire group joined to form a network. Effects spill over, or cascade, to other parts of the system and put the entire system at risk, not just the initial component affected. The speed with and degree to which the effects affect other parts of the system depend on how much slack is built into the system. It is my contention that the effects of the vulnerabilities of the information infrastructure's components produce just such a systemic effect and, as a result, affect the national security of the United States.

For this research, I elect to not include the first two and last two aforementioned components in my definition of the information infrastructure system. The vulnerabilities of and counter-measures for the first two components (users and operators/providers, i.e., people) are already well known. This is not to suggest that the vulnerabilities associated with the people that use and maintain the system are not potentially serious,[105] but only that there is little new I can say about the subject. I elect not to include the last two components (materials/supplies and financial resources) in the defined system since they are primarily indirect support of the system and the vulnerabilities associated with them do not necessarily lead to unforeseen immediate risks.

[105] For an example of the seriousness of humans' vulnerabilities and the consequences of their exploitation, see the LoveLetter denial of service (as well as others that require social engineering to install and/or propagate the DoS tool) incident in Appendix B. Denial of Service.

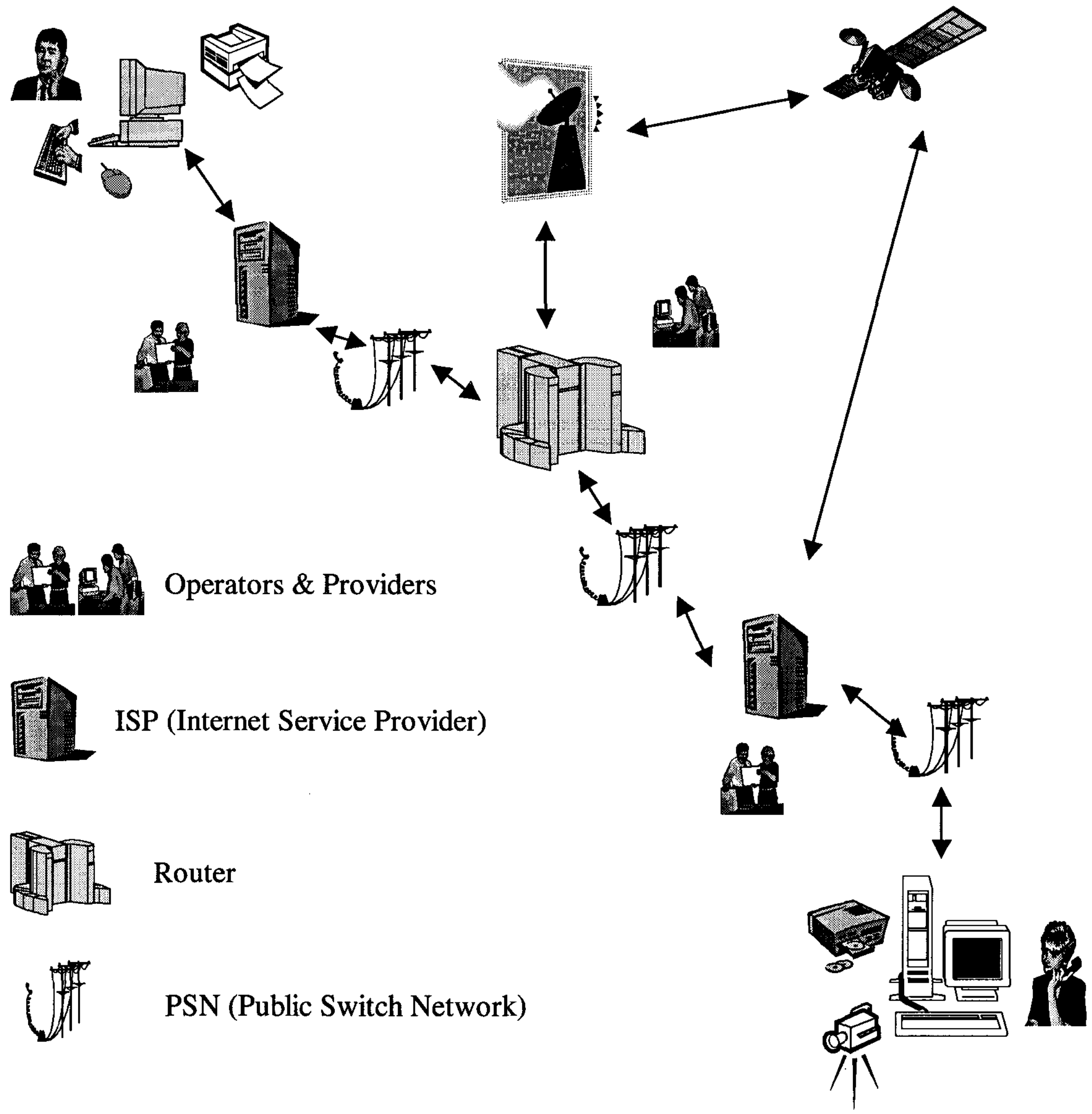


Figure 2.1. Archetypical Information Infrastructure System

I will define the information infrastructure system for this research as comprised of components three through seven (See Figure 2.2. Research Information Infrastructure System):

- the computers (hardware),
- software and standards,
- telecommunications networks,
- information content, and
- applications.

I restrict my definition to those components only since I am most interested in the data; its storage, manipulation, and transmission; and the vulnerabilities of the technology servers and bridges, memory, software, standards, and storage media with a transmission medium to create an information infrastructure system is not without precedence (See The Unpredictable Certainty and Revolution in the U.S. Information Infrastructure, both by organizations of the National Academy of Sciences).

With my definition, the terminal computers enter and receive, store, access, manage, retrieve, and manipulate data. The transmission medium transports packets of data to and from initiating and receiving devices and serves as an access to data stored on computers.[106] Switching, networking, and other communication technologies allow messages to be

[106] The transmission medium may be either the normal public switched network's system assets or, in certain cases, leased lines or private circuits. One needs to carefully consider the threats and risks when discussing leased lines or private circuits. In analogue networks, leased lines are used exclusively by the leaser and in the past have consisted of dedicated transmission plant over a fixed route. However, in digital networks (which are becoming more and more the norm), "leased lines can be provided as Private Virtual Circuits which appear to the customer to have the traditional properties of a leased line, but which for all intents and purposes are part of the switched system implemented in a way that does not require network address information. Therefore, there is negligible physical separation between the leased line and the rest

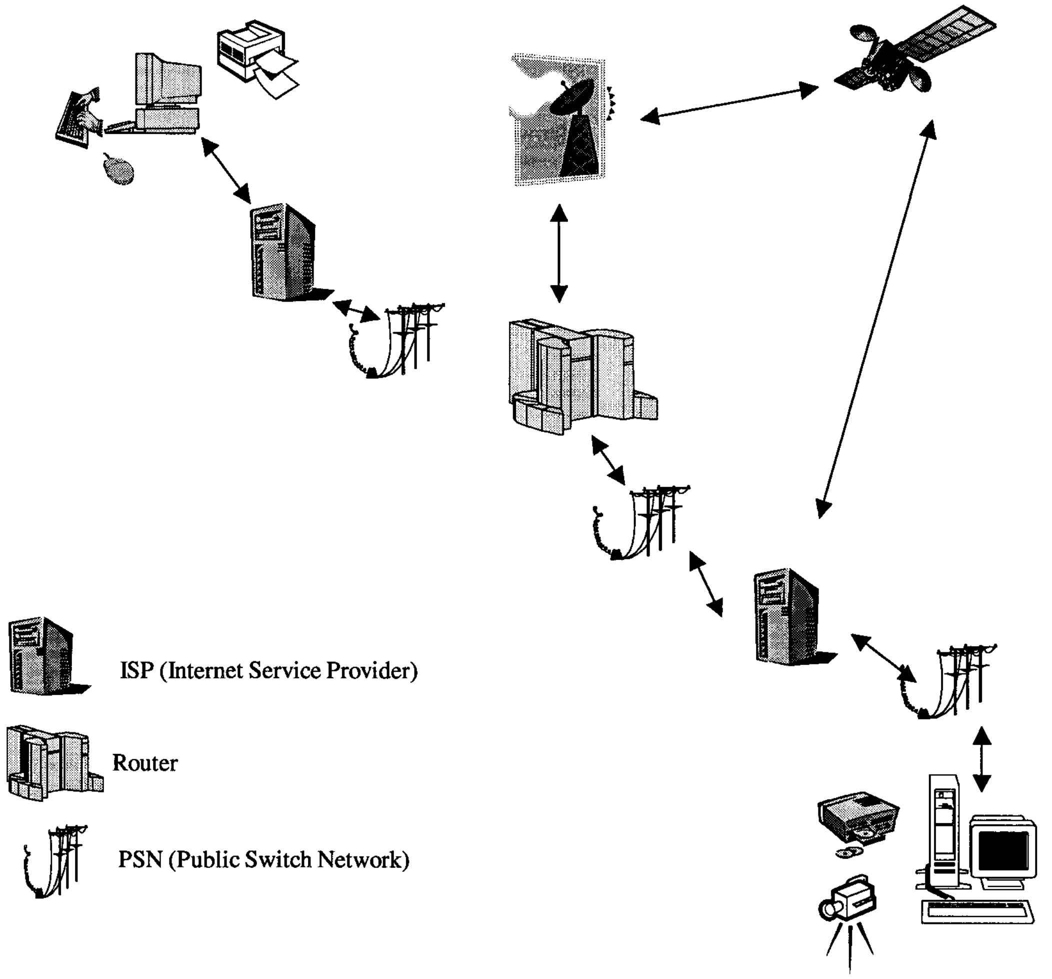


Figure 2.2. Research Information Infrastructure System

of the network” (Willets in Jackson and Hruska, 745).

efficiently routed from place to place.[107] The integration of the two systems (computer and telecommunications) creates a higher order system that is the information infrastructure system.

Admittedly, the information infrastructure system depicted in either Figure 2.1 or Figure 2.2 is the simplest system possible. Neither diagram is meant to suggest that most information infrastructure systems are that simple. They visually show only the minimum combination of components necessary for an information infrastructure system. Most such systems are much more complex making them much more valuable and vulnerable.

Information infrastructure systems evolve into the complex networks we associate with the distributed system today by adding connections between the components of an existing system, to additional computing components, or to other networks or information infrastructure systems through the transmission media to become a network of networks connected to a transmission medium by servers, routers, and bridges. (See Figure 2.3. Typical Distributed Information Infrastructure System for an example of the process of increasing the complexity of a simple information infrastructure system and Figure 2.4. Representative Complex Distributed Information Infrastructure for an example of a representative relatively simple complex information system). As more such connections are added, the degree of complexity increases.

Hierarchy in the form of clustering and levels is a fundamental feature of complex systems. Systems are composed of multiple subsystems, and systems are themselves

[107] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 3-4 and National Academy of Sciences, Revolution in the U.S. Information Infrastructure, iii.

contained within suprasystems.[108] The information infrastructure system illustrates the concept admirably in several different ways. Structurally, the clustering begins with the individual basic elements of a computer system and of a transmission system. The information infrastructure system is a suprasystem formed when the computer system and the transmission system are integrated into one system.

The information infrastructure system also illustrates the systemic concept organizationally. There are two different conceptual schemes to organize information infrastructure systems. An information infrastructure system can exist as a private, public, or some combination of the two in progressively larger Local Area Networks (LANs), Metropolitan Area Networks (MANs) or Rural Area Network (RANs), Wide Area Networks (WANs) or a Global Area Network (GAN). Each one is an information infrastructure system as long as it is capable of integrating the computing components and transmission media to transfer data. The other organizational scheme is to organize all of the local public and private networks into a Local Information Infrastructure (LII), then aggregate those into a National Information Infrastructure (NII), and, finally, into a Global Information Infrastructure (GII). Obviously, these conceptual aggregations are not exclusive. There could possibly be some type of intermediate stage(s) between the LII and the NII or the NII and the GII.

[108] Richard W. Scott, Organizations: Rational, Natural, and Open Systems, Englewood Cliffs, N.J.: Prentice Hall, 1992, 88.

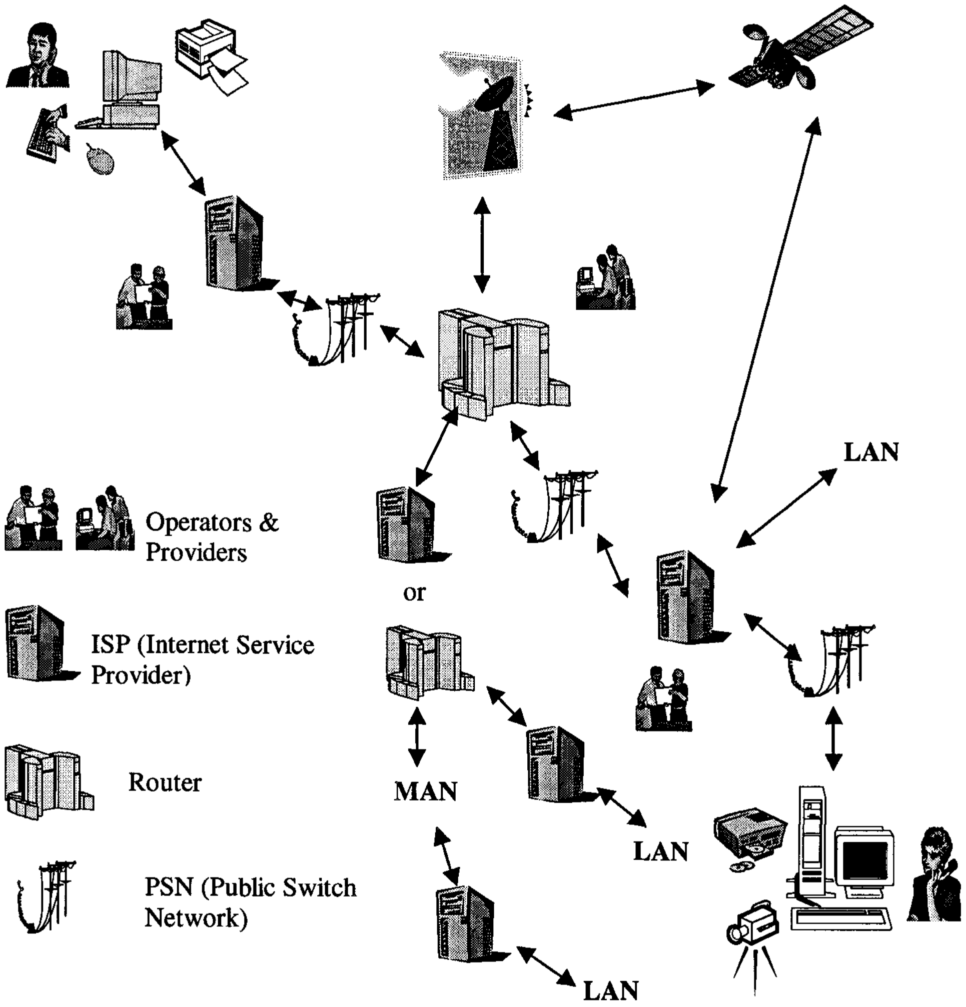


Figure 2.3 Typical Distributed Information Infrastructure System

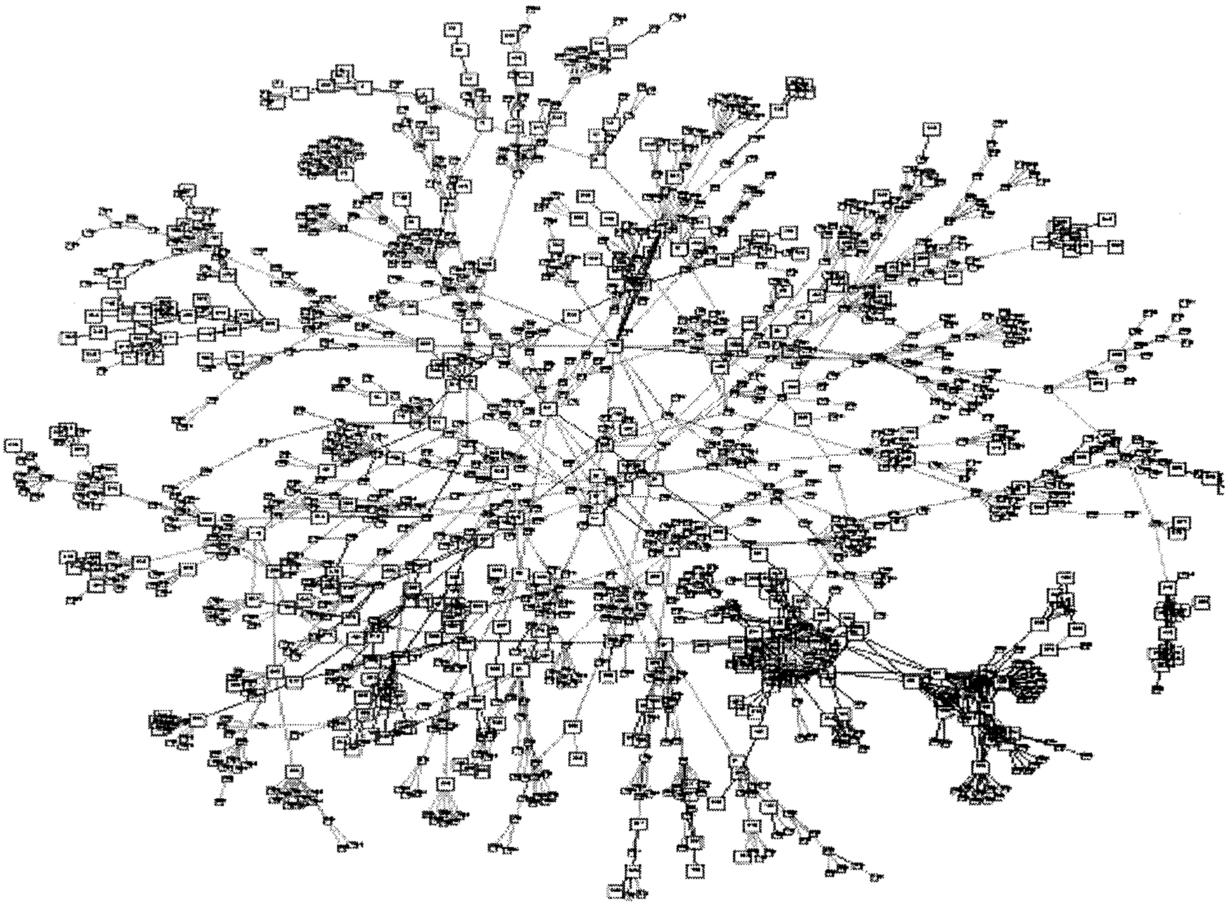


Figure 2.4. Representative Complex Distributed Information System[109]

[109] Elan Amir, Computer Science Division, University of California at Berkeley, http://www.cybergeography.org/atlas, January 1, 2001.

Figure 2.3 is a map of the MBone topology in August 1996. It was arbitrarily chosen only to demonstrate the degree of complexity that information infrastructure systems achieve as connections are added. Obviously, many systems are much more complex (e.g., the Internet) while others are somewhat simpler. The website cited contains many different types of network maps to demonstrate not only the different techniques used for mapping networks but also networks of differing complexity.

As the different infrastructure systems connect with each other, the degree of complexity increases exponentially. That is the reality of the information world today and promises to be even more so in the future as more and more computing components connect to existing networks, create new networks, or networks connect with other networks. Within the United States, the complexity has grown even greater as the information infrastructure system becomes increasingly interconnected with other critical infrastructure systems. The complexity, and hence, the vulnerabilities, are further exacerbated by the combination of applications (e.g., internet conventions, software with its inherent defects and faults, etc.) and the properties of the network itself (i.e., interconnected and open).

The information infrastructure system can be defined as an open system if its boundaries are defined to exclude people as I have done in this chapter. Defining a system as "open means, not simply that it engages in interchanges with the environment, but that this interchange is an essential factor underlying the system's viability."[110] The information infrastructure system is "open to and dependent on flows of personnel, resources, and information from outside."[111] Among the various flows connecting system elements, the flow of information is the most critical. Since the information infrastructure system is about the flow of information, it makes perfect sense from the open system perspective to connect it with other systems. However, some of the other characteristics of an open system should caution designers about making that connection too binding.

As for the information infrastructure system itself, the system cannot function without input from its environment. In addition to the obvious reliance on power and

[110] Walter Buckley, Sociology and Modern Systems Theory, Englewood Cliffs, N.J.: Prentice-Hall, 1967, as quoted in Scott, 76.
[111] Scott, 85.

climate control, it is also dependent upon data or requests for data supplied by people. And, public policy has consciously allowed the system to develop to grant the widest distribution of information to the greatest number of people through easy access to the system.[112] Once easy initial access to the system's flow of information has been gained, navigation within the system between the different levels and different subsystems is intended to be easy also.

2.4. Influences Affecting the System.

Over the years, the dramatic pace of innovation in semiconductor technologies, fiber optics, voice and data communications, and software has changed both the nature and physical structure of the information infrastructure system. Increases in silicon integrated-circuit technology have more than doubled workstation speed and memory size every 2 years increasing speed, flexibility, and generality.[113] These advances combined have

- induced more powerful, facile, and useful computers,
- reduced computing costs 15 to 25 percent annually,
- facilitated technology growth by making the technology more attractive to ever greater numbers of consumers, and
- permitted rapid technology rollover and almost continuous restructuring of the hardware base.[114]

[112] The public policy of maintaining an open system architecture is continued in the United States Chief Information Officers Council, CIO Council Strategic Plan, January 1998, http://cio.gov/content/fy1998.htm.

[113] However, the apparent simplicity and use of natural logic in the user interface to produce flexibility and generality require very complex processes in software and hardware (National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 115-116).

[114] Robert W. Stearns in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 27.

Innovations have also enabled a shift from incompatible analog to interoperable digital technologies facilitating the convergence of computers, telecommunications, and media. Today, digital and analog telephone systems and digital telephone systems with different voice codings (e.g., digital cellular systems) work interchangeably because economical format converters permit greater use of the information infrastructure system.[115]

At the same time, shortened product development cycles and increased price/performance pressures have propelled a fundamental change in electronic system design that allows functions to be transferred from large central computers to the personal computer.[116] Semiconductor process technology is now down to 0.15 microns and the number of gates is now in the millions per die permitting an entire functional system to be placed on a single chip. Embedded system, or system-on-a-chip (SOC), technology replaces some hardware functions (which are frozen once manufactured) with software applications;[117] designers partition the algorithm between the hardware and the code executing in the microprocessor. Such software substitution for hardware permits a function to be modified through software code upgrades instead of manufacturing new hardware.

This flexibility of SOC technology to change a product during its lifetime to correct "bugs"[118] or to meet evolving user application needs is critical to reducing labor and human

[115] Stearns in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 27 and National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 117.

[116] John S. Mayo, "The Evolution of Information Infrastructures: The Competitive Search for Solutions" in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, National Academy of Engineering, Washington, D.C.: National Academy Press, 1995, 6.

[117] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 116.

[118] The origin of the term reputedly goes back to the early days of computing, when a hardware problem in an

error costs.[119] Costs can be reduced by replacing a number of special-purpose or low-level hardware elements with a single integrated processor that then performs all the same tasks as multiple hardware elements by executing a single program. For example, when purchasing is integrated with the accounts payable system, there is much less clerical work and fewer errors since data is entered only once.[120] With SOC technology, the software content of complex electronic systems is now reaching 50 percent of the total software/hardware content of the system.[121]

As a result, the computer will increasingly be only an access, processing, and storage point as the network is increasingly designed and built with a higher and higher percentage of the intelligence lying outside of the devices connected to the network. Typically, systems created by this marriage have the ability to handle large numbers of remote users in a conversational mode and to adapt to a wide range and form of information and communications products and services.[122] Users are able to interact directly with one or more computers, databases, and problem-solving procedures to access electronic transaction

electromechanical computer at Harvard University was traced to a moth (a "bug") caught between the contacts of a relay in the machine (http://encarta.msn.com). In common usage, the terms "error" and "bug" are used to express an incorrect step, process, or data definition in a computer program (Institute of Electrical and Electronics Engineers, Standard Glossary of Software Engineering Terminology).

[119] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 116.

[120] Targowski, 216.

[121] Bernard Cole, "Methodologies Focus on Core Integration," Electronic Engineering Times, no. 1013 (June 22, 1998); Richard Goering, "New Tools Will Force Embedded Designer to Link Hardware/Software Efforts -- Codesign Turns Workplace on Its Head," Electronic Engineering Times, no. 988 (January 12, 1998); and "Mentor Graphics and IKOS Deliver Verification Environment to Accelerate Telecom and Datacom System Design" PR Newswire, March 30, 1998.

[122] Embedded systems products such as Digital Service Providers (DSPs), controllers, and peripherals with greater software content than older products, are now being used for networking, communications, multimedia, consumer electronics, industrial controls, and automotive electronics (Cole; Goering; and Berger).

processing systems and information, communications, and networking services from remote terminals in a multimedia mode.[123]

The dilemma is that system software development has always been the bottleneck in product development, but is even more so with SOC designs. Embedded systems development forces designers to conceive of system-level specification, functional and architectural analysis, high-level estimation, partitioning and software synthesis through task scheduling and synchronization; all new concepts. With the development of soft cores, hard cores, VHDL, Verilog and synthesizable macros, the hardware portion of the project can often be finished in a fraction of the time that software designers can write and debug the necessary programs even when a synthesized version of the design can be provided.

These pressures increase the demand for codesign (the concurrent specification, design, and verification of hardware and software or the merging of functional and architectural design). To assist designers, design-specification language that can represent an entire system and rapid estimation tools are being developed to speed integration of the software and hardware through simulation of a virtual system before committing the design to silicon.[124]

In addition, telecommunications networks as a whole are becoming more and more sophisticated as integrated digital networks of computers, telecommunications, and television create a second tier of the transmission medium: [125] the public data network.[126]

[123] Targowski, 105 and 156-157.

[124] Cole; Goering; "Mentor Graphics and IKOS Deliver Verification Environment to Accelerate Telecom and Datacom System Design"; and Berger.

[125] Network technologies of the future are envisioned to be integrated into a single telecommunication environment based on the Broadband Integrated Services Digital Network (B-ISDN) architecture. However, service installation costs coupled with very high monthly service costs will more than likely limit residential and small-office deployment. Rapid deployment of B-ISDN can be achieved, but only as the price of service approaches that of

For these new technology networks, function and data sharing are combined with a common user interface forming a more powerful, more useful, seamless[127] environment.

New techniques have also been developed to overcome traditional application integration limitations, i.e., the application controlling the communication rather than the preferable obverse. This new technology separates the communication mechanism from the message itself. The result provides a generic mechanism for communicating between all applications and provides for integration of new applications to the system with messages instead of having to rewrite the application itself.[128] Networks created through this technology integrate the transmission and switching equipment with the voice and data communications distributed throughout the telecommunications service provider's Service Control Point (SCP) which directs a Service Switching Point (SSP) to act as the entry and exit points for the system and the Service Management System (SMS) to provide network planning, engineering, provisioning, monitoring, maintenance, and repair.[129]

Electronic Data Interexchange (EDI), the CPU-to-CPU telecommunications exchange of standard business documents such as purchase orders, invoices, and medical claims, is just such an integration of a software application with other software applications. Unlike electronic mail, EDI is meant to be read by a machine, not by a human being. An EDI transmission can go straight from a buyer's purchase order application into the seller's

current telephone service (National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 163; Targowski, 21-24; and Mayo in National Academy of Sciences Revolution in the U.S. Information Infrastructure, 3).

[126] A public data network is an information infrastructure that is publicly accessible for a fee from remote locations. In the United States public data network providers resale circuits from the telephone companies to users of commercial (AOL, Compuserve, etc.), company (VNET (IBM), XEROnet, etc.), and non-profit (Internet, BITNET, etc.) networks and generally provide some value-added services such as transmission, computing power, storage, software rental, private network management, etc. (Targowski, 156).

[127] The user is unable to tell where one application ends and the next begins (Targowski, 231).

[128] Targowski, 231.

[129] Targowski, 54.

order entry application without human intervention. Integration became possible only when EDI standards and translation software allowed access to "flat" data files from a corporate application and translated them into standard EDI formats, such as the (ANSI) X12 format.[130]

Future networks envision the integration of applications across multiple network platforms with transparent user access. These future networks will be composed of various data communication, processing and information management technologies (e.g., video, voice, image) that form an integrated electronic infrastructure to facilitate the efficient exchange of information. Hosting[131] is an example of a service provided by this integration of applications across multiple network platforms.[132]

These trends also act synergistically, as well as individually, to produce advances. For example, data transformations such as the real-time encryption and compression of video or data are now migrating to software.[133] A further example of synergistic benefits is Open Data Networking (ODN). ODN is a software service interface independent of underlying technology options and also independent of specific applications that allows

[130] Targowski, 222 and National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 134-135.

Interfaces allow the EDI software to operate with business software. Translation software must perform a number of different tasks: extract data from internal corporate data sets; contain tables of the particular EDI formatting characters used by the trading partners so that correctly formatted information can be "wrapped around" each data element; and generate EDI files that are ready for transmission. On the receiving end, EDI translation software must perform the obverse functions (Don Steinberg, "EDI Evolution Continues with Integration into Business Applications," PC Week 5, no. 6 (February 9, 1998), 31-32).

[131] Hosting is a function that connects end users to the content they seek. Customers will gain easy and timely access to personal communications, transactions, information services, and entertainment via wired and wireless connections to telephones, handheld devices, computers, and, eventually, television sets (Mayo in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 7).

[132] Targowski, 224.

[133] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 117.

construction of a service built on top of another service.[134] This layered approach to constructing services is a consequence of increased processing power and more modular design with defined interfaces to basic infrastructure facilities.

Because of ODN, networking now often involves a simple, layered model of technology, in which infrastructure components are installed and then used as a foundation for next-level services, and so on in an orderly manner.[135] The Internet is just such a service continuously improving itself with service and infrastructure providers making new services available by layering them on top of existing communications infrastructure.[136]

It is useful to use the Internet as a prototype for the emerging information infrastructure system to demonstrate the concepts just discussed. One key to making this network of networks a true global information infrastructure system for multimedia and other communications is a system of open, user-friendly interfaces and global standards; maximum interoperability and connectivity, and a multi-vendor environment that allows maximum customer choice of equipment and services.[137] The Internet currently possesses all of these conditions, as does the U.S. information infrastructure system. Policy-makers

[134] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 121.

[135] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 119.

[136] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 14.

The World Wide Web (WWW) is an example of a layer service in use on the Internet. It is really only a global, hypermedia information system layered on top of the Internet infrastructure (Micki Krause, "Resolving Internet Security" in Ruthberg and Tipton, S-262).

[137] Stearns in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 9.

However, these same properties exacerbate the other vulnerabilities of the Internet and, by extension, the Information Infrastructure System. "From its inception as a mechanism for the free-flowing exchange of research and development data, the underlying philosophy of the Internet has been strongly entrenched in freedom, openness, and availability. This thinking is certainly not compatible with stringent security policy. This unregimented albeit democratic environment is coupled with a lack of central authority for ruling or regulating the Internet" (Krause in Ruthberg and Tipton, S-249-250).

and the information industry have consistently indicated that the current policy with respect to these conditions for the Internet and the information infrastructure system will not change in any future information infrastructure system.[138]

The Internet is perhaps an extreme example of a system that is open; in fact it is open in a number of ways:

- First, all of its standards and specifications are available for free, and without any restriction on use.
- Second, the Internet is open to providers as well as users. One objective to the design of standards is to make it as easy as possible for networks within the Internet – both public networks of Internet service providers and private networks of corporations, institutions, and individuals – to connect together.[139]
- Third, its internal structure is organized to be as open as possible to new applications. For example, some of its traditional features, such as the TCP protocol that ensures ordered, reliable delivery of data, are not mandatory and can be bypassed if this better suits the needs of an application. This type of openness has made the Internet an environment conducive to new and innovative applications.[140]

[138] The NII 2000 Steering Committee of the National Research Council concluded, "The government in particular need not and should not protect mature products, but that it should move to foster an open, innovative environment in which new services and applications can occur. This approach includes encouraging the deployment of communications infrastructure that is general and flexible, removing regulatory barriers to innovation (for example, making spectrum for experiments easily and predictably available) and competition, and continuing to foster the success of the Internet through R&D and delivery of public services. Government should adopt policies intended to retain the power of a service, and provide a link among many resources for both information and its processing and distribution" (National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 206 and 229).

[139] This is the concept of openness I am advocating when I refer to an "open" system.

[140] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 150-151.

Hindering this integrated open network, and by extension the National and Global Information Infrastructures since both have publicly committed to the same open nature, though are the following technical issues:

- Achieving interoperability. Full interoperability among the thousands of networks, communications devices, and services that will comprise the national and global information infrastructure systems will be very difficult to achieve. To do so, governments, industry and standards-setting organizations must agree on well-defined international standards for rapidly advancing communications technologies, while manufacturers and service providers need to provide products and services conforming to these standards.[141] H.100 and H.110 Interoperability Agreements that detail specifications for a compatible telecommunications bus provide a significant step toward this open-systems environment for computer telephony.[142]
- Encryption and Decryption. Quality and integrity of information are long-standing issues that have been around in the "print world" from the advent of the first printing press. The information infrastructure system creates enormous challenges for both information providers and users to the privacy and confidentiality of data transmitted over networks.[143]

[141] Targowski, 28; See also Mayo in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 9-10.

[142] William H. Matlack, Jr., "Interoperability the Rage at Forum," Electronic Engineering Times, no. 10 (August 24, 1998).

H.100 has a capacity of 4,096 timeslots and supports backward compatibility with all existing standards. Both H.100 and H.110 also define an embedded message channel that can provide for control and maintenance of peripherals that are not bridged to the telecommunications bus (Matlack).

[143] Horton, 26.

Some governments object to encryption on the grounds that it limits their ability to monitor transmissions where they have the will and the authority to do so. Privacy advocates argue that encryption is a private determination and if a person or organization wants to encrypt its data to protect it from unauthorized access, then it should have the legal authority to do so.[144] Although a contentious information infrastructure systems issue, encryption/decryption is outside the scope of this research.

• Reliability of Networks. Public and private networks are increasingly dependent on existing telecommunications networks to meet their personal and business needs. Yet recent outages on these networks have raised reliability concerns and caused economic losses. Moreover, new technologies and industry trends will likely increase network vulnerability, making reliability of the information infrastructure system a key challenge.[145]

In the final analysis, these technical issues and their solutions are only part of the larger mosaic of the information infrastructure system. They, along with the additions of components and software substitutions that are the future evolution of the system, put any system of which they are a part at risk to new and additional vulnerabilities. Just as technical increases in separate components of the information system synergistically lead to the total benefit being greater than the sum of benefits, individual component's vulnerabilities can lead to the same synergistic increase in risk. Off-site functions, in

[144] Targowski, 28.

[145] Targowski, 29.

E-Bay, Yahoo, and others in 2000 are the most recent widely publicized incident.

particular, increase the system's vulnerability to the probability of software integration errors from tighter coupling and less opportunities for human interaction, to interactive complexity and cascading effects, and to easier unauthorized access. In effect, the software integration, open system, and interconnectivity vulnerabilities that are the focus of this research.

2.5. United States National Information Infrastructure (NII).[146]

Just what is the U.S. National Information Infrastructure? What it is not is a uniform end-to-end network developed and operated entirely by government or the commercial sector. As with most other aspects of the information infrastructure system, there is little consensus about much relating to the NII making the task of defining and describing it even more daunting than accomplishing those same tasks for a basic information infrastructure system.[147] The concept of the NII – and the Global Information

[146] The National Information Infrastructure (NII) is a phrase coined by the U.S. government to describe the convergence of telecommunications, information technology, and the entertainment industry. The NII has also been referred to as the Information Superhighway, Infobahn, or the IWay (Yogesh Malhotra, Abdullah Al-Shehri, and Jeff J. Jones, National Information Infrastructure: Myths, Metaphors And Realities, 1995, http://www.brint.com/papers/nii/).

[147] "The NII has been described variously as: a 500-channel interactive multimedia video/cable network; numerous "edutainment" multimedia products and services; the natural evolution of today's telephone system from one that is voice-oriented to one that supports voice, data, image, and video; an electronic marketplace for a commercial version of the Internet; a public network for government information and services, medical information, and education; not a single network at all but a loose aggregate of many different networks and services with common or related access; a public-policy debate about social rights and access to information; a political battle in which the telecommunication and cable industries may attempt to reassert their monopolies in the name of universal service; and a government-funded initiative, created by the Clinton administration and modeled after the National Highway Project of the late 1950s and 1960s, which could easily turn into a new species of high-technology pork" (Stearns in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 26).

"The NII encompasses a wide range of equipment, including cameras, scanners, keyboards, telephones, fax machines, computers, switches, compact disks, video and audio tapes, cable, wire, satellites, fiber-optic transmission lines, microwave nets, switches, televisions, monitors, printers, as well as the physical communications facilities (i.e., transmission lines, switches, and network software)" (Tom Sheldon, Encyclopedia of Networking, Berkeley: Osborne McGraw-Hill, 1998, 728). The DSB Task Force expressed similar sentiment on Information Warfare (Defense) in their report, Report of the DSB Task Force on Information Warfare (Defense), as did Mayo in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 9.

Infrastructure (GII) of which it is a part – involves an incredibly complex, abstruse technological system; simply understanding its behavior is a major task.[148]

The concept of a national data "superhighway" was first suggested in the initial draft of the High Performance Computing Act (HPCA) of 1991[149] by then-Senator Al Gore. This legislation outlined a plan to link US supercomputing research centers together on a high-speed network and to support other work in high-performance computing.[150] As part of its economic reconstruction policy, the Clinton administration (with now-Vice President Gore) in 1993 made the creation and development of the NII a top priority to stimulate the U.S. economy.[151] The strategic and global implications of such an information-based national economy for the United States are evident in the following extract from the Title 47, Chapter 8, Section 901, U.S. Code.

> "Telecommunications and information are vital to the public welfare, national security, and competitiveness of the United States. Rapid technological advances being made in the telecommunications and information fields make it imperative that the United States maintain effective national and international policies and programs capable of taking advantage of continued advancements. Telecommunications and information policies and recommendations advancing the strategic interests and the international competitiveness of the United States are essential aspects of the Nation's involvement in international commerce."[152]

The High-Performance and High-Speed Networking Act of 1993 was passed, in part, to coordinate efforts in defining and building the NII. In FY 94, the HPCC

"Rather than a single coherent technical framework it is more appropriate to think of the National Information Infrastructure (NII) as a concept to focus thinking on connectivity, accessibility, and functionality. The NII has no specification, no overall plan, and no institutional mechanism for reaching consensus about what it is or what it should be" (National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 3).

[148] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 199.

[149] Even though the bill was initially drafted in 1991, it was not introduced until 1993, and then not as the HPCA.

[150] Malhotra, et.al.

[151] Sheldon, 728.

[152] Malhotra, et.al. and U.S. Code, Title 47, http://www4.law.cornell.edu/uscode/47/chp8.html.

Program[153] began expanding its technical scope to include the following technologies to accelerate the development of a National Information Infrastructure:

- microprocessors for scalable parallel computers;
- high speed connectivity technology such as ATM/SONET (Asynchronous Transfer Mode/Synchronous Optical Network) technology and interfacing ATM to HiPPI (High Performance Parallel Interface) and HiPPI switches and cross connects to make heterogeneous distributed high performance computing systems available at high network speeds;
- client/server technology to route information over the networks;
- massive storage systems;
- high bandwidth networks such as all-optical networking; and
- improved software technologies such as network performance measurement technology to identify bottlenecks. [154]

Despite the obvious government involvement, the NII was still intended to be built and operated primarily by the private sector to create new products and services markets. Since the NII was viewed primarily as a private sector economic project, the

[153] The High Performance Computing and Communications Program (HPCC) was considered so critical to the success of the NII, that the reports (also used as supplements to the President's budget submissions) of its oversight organization, the National Science and Technology Council, for FY 1994 and FY 1995 were entitled "Toward a National Information Infrastructure" and "Technology for the National Information Infrastructure," respectively (High Performance Computing and Communications: Toward a National Information Infrastructure and High Performance Computing and Communications: Technology for the National Information Infrastructure).

[154] United States Office of Science and Technology Policy, High Performance Computing and Communications: Toward a National Information Infrastructure, A Report by the Committee on Physical Mathematical and Engineering Sciences, Federal Coordinating Council for Science, Engineering, and Technology, Supplement to the President's FY 1994 Budget, 1993, and United States Office of Science and Technology Policy, High Performance Computing and Communications: Technology for the National Information Infrastructure, Committee on Information and Communications, National Science and Technology Council, Supplement to the President's FY 1995 Budget, May 1994.

Department of Commerce, instead of one of the traditional national security agencies, was given primary responsibility for the NII:

- The National Telecommunications and Information Administration (NTIA) was created within the U.S. Department of Commerce to provide management;
- The Institute of Standards and Technology (NIST) was to tasked for overall supervision; and
- Commerce Secretary Brown chaired the Information Infrastructure Task Force and appointed the NII Advisory Council representing a broad spectrum of private sector, public interest, and governmental views.[155]

Subsequent legislative history of the National Information Infrastructure is almost as indeterminant as the NII concept. The National Information Infrastructure Act, introduced in 1993 in the House of Representatives as HR 1757[156] set forth the following goals and means for information infrastructure systems:

- To promote private sector investments through appropriate tax and regulatory policies,
- To act as a catalyst to promote technological innovations and new applications,
- **To ensure the NII security and reliability** (emphasis added),

[155] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 1-10.

[156] The High-Performance and High-Speed Networking Act was introduced in 1993 also.

- To coordinate with other levels of government and with other nations the standardization of interfaces and removal of obstacles and unfair policies that may handicap the U.S. economy and society.[157]

The bill was passed by the House of Representatives on July 26, 1993, and sent to the Senate where it was incorporated into Senate Bill S.4, proposed national economic competitiveness legislation. At the same time, The Telecommunications Infrastructure Act of 1993 was introduced in the Senate as S.1086. Neither bill was brought to a vote in the Committee on Commerce, Science, and Transportation to which they were referred. A bill similar to the Telecommunications Infrastructure Act was re-introduced in the Senate the next year as the National Public Telecommunications Infrastructure Act of 1994 but was not reported out of committee either.

NII legislation then became even more inextricably integrated with national economic competitiveness. The next reference to the NII in enacted legislation was in Title VII, "Information Technology Applications," of the National Competitiveness Act of 1993, legislation solely concerned with economic issues associated with information systems. The entire information infrastructure system and National Information Infrastructure issue then became absorbed into the Telecommunications Reform Act of 1996, S. 2195, which was much more concerned with competitiveness in the telecommunications industry than structuring and promoting the NII.[158] My research has

[157] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 1-10.

[158] Paul Evan Peters, "National Information Infrastructure Act of 1993 (HR1757) Passes House," Coalition for National Information, July 30, 1993, http://www.cni.org/Hforums/cni-announce/1993/0046.html; United States Congress, Senate, S.1086, National Telecommunications Infrastructure Act of 1993, 103d. Congress, 1st sess., June 9, 1993; and "Conference on the Nat'l Competitiveness Act (HR820/S.4): Inconclusive First Session of Conference," FINS Special Report 2-36, Federal Information News Syndicate

not discovered any legislation ever enacted to implement the NII as originally envisioned in the 1991 HPCA.

What then is the National Information Infrastructure? First of all, it is an organizational concept or scheme: **a conceptual aggregation of all the present and future data networks in the United States, interconnected domestically and internationally into one system.** The NII is a way to organize the nation's information and telecommunications systems into one system; in concept and practice, the previously described information infrastructure system for the nation.

The NII exists in the national communications web of fiber-optic strands, coaxial cables, RF, satellites, and copper wire. It is envisioned as a seamless web government, public, and private information networks (including the Internet, public switched telephone network, public data networks, cellular networks, commercial satellite networks, broadcast TV networks, cable TV networks, commercial firms' private networks, governments' networks and all test beds), computers, databases, and consumer electronics. [159] The interconnectedness and interdependence of these systems and networks are the foundation of the aforementioned critical economic, diplomatic, and military functions upon which our national and economic security is dependent. The geographic

(FINS), September 27, 1994, http://sunsite.utk.edu/FINS/Special_Reports/Fins-SR2-36.txt.

[159] Stearns in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 8-9; Malhotra, et.al.; and United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-15-16.

DoD's information infrastructure is conceptually a part of this larger NII, and also the GII. DoD has over 2.1 million computers, over 10,000 LANs, and over 100 long-distance networks. Much of the Defense Information Infrastructure (DII) is embedded in the public switched and data networks. DoD depends upon computers to coordinate and implement aspects of every element of its mission, from designing weapon systems to tracking logistics. DISA has determined that at least 65 percent of DoD unclassified systems are vulnerable to attack (United States Department of Defense, Report of the DSB Task Force on Information Warfare (Defense), Section 2-3, "The Infrastructure" and Section 6.4 – "Access Infrastructures Dependencies and Vulnerabilities"; and United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-8).

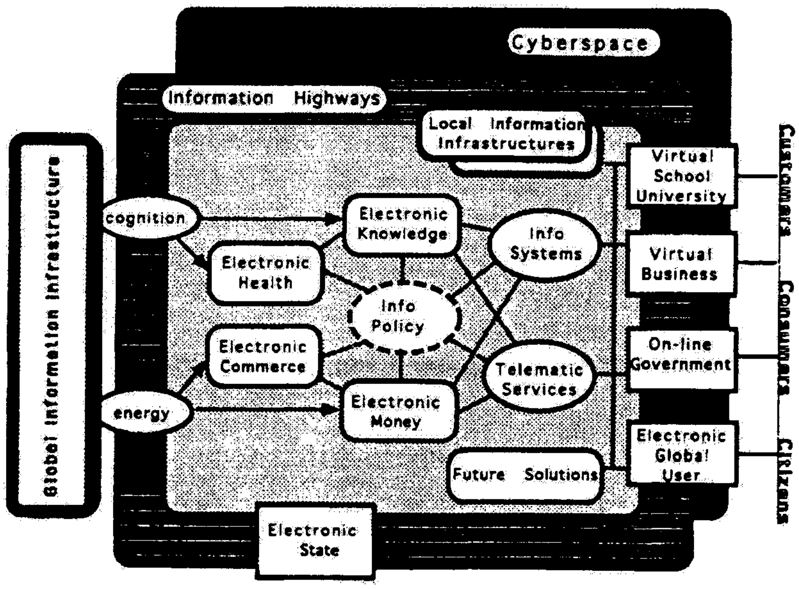
organization of these data carrying networks gives rise to the infrastructural terms: Local Information Infrastructure (LII) at the sub-national level, National Information Infrastructure (NII) at the national level, and Global Information Infrastructure (GII) at the global level.

Figure 2.5. Conceptual View of NII Architecture illustrates the NII concept just discussed. The entire figure represents the world's electronic environment, or cyberspace; the large area in the middle, any and all nations' cyberspace (or, "electronic state" as labeled in the figure). The boxes in the center area represent functional services that might be provided by an information infrastructure system. All of these different functions and any local area networks, to include future developments, are organized into LIIs. The black border represents the different types of networks that might comprise the NII and some typical domains (or functional audiences) to which the infrastructures lead and provide service. The white space outside of the black border represents classes of specific users to which this cyberspace and the NIIs are capable of connecting, including the Global Information Infrastructure (GII) thereby connecting each NII with all other NIIs.

Five key policy issues dominate U.S. NII discussions:

1. Universal service. All Americans should have easy access to the NII, at least for some basic level of services yet to be defined.

2. Interoperability. Legacy and future platform devices, such as computers and phones, software applications, and databases should be able to "talk" to each other easily via the transmission medium or media.



[160]

Figure 2.5. Conceptual View of NII Architecture

3. Security, privacy, and protection of intellectual property. The content and nature of communications on the NII should be carefully protected from eavesdropping, misappropriation, or unauthorized use.[161]

4. Private sector versus public-sector model. Should the NII evolve in a historically unregulated environment that responds to free-market forces, or should the federal government fund and guide its development? Up until now, the prevailing consensus has been that the operating environment be unregulated and free-market oriented.

[160] Targowski, 1-9.

[161] The system's vulnerabilities that prompt discussions about its security have the potential to threaten the national security and are the subject of this research.

5. NII's link to the GII. The prevalent U.S., and most of the rest of the world's, view is that the GII should be a single system, but not all of the world's governments are willing to accept such a concept[162]

Given these policy issues for the NII, a powerful lesson can be learned from the Internet since it approximates the NII and has dealt, and is still dealing, with the same issues. The Internet is an information infrastructure system whose most important use, and indeed the NII's, is to allow individuals to communicate with each other and to access information rapidly.[163] In reality, the Internet is "a collection of public and private information services – both facilities- and content-based – operating as a complex, dynamic system of systems spanning a variety of new and older technologies, always in a state of flux, and, consequently, never embodying the holy grail of developers – a single system appearance." There never was, or is, a central grand plan to direct how the emerging system was to be built. Instead there was a "bottom-up" model of development, characteristic of most competitive technology-driven change such as the internal combustion engine or the telephone, which engendered vitality and legitimacy.[164]

The Internet began in the late 1960s with the development of ARPANET to provide a limited number of researchers with shared, interactive communications at different locations through some key innovative technologies on which it still depends.[165] These

[162] Sterns, "The Promise of the National Information Infrastructure" in Revolution in the U.S. Information Infrastructure, 26-28.

[163] Stearns in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 23.

[164] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 199.

[165] The most important technologies developed by the early users of the Internet and still in use today are:

1. Packet switching which divides a message into packets that are transmitted to their destination and reassembled;

researchers were interested in learning about and compensating for the potential effects nuclear war would have on the United States' commercial telecommunications systems since the military's command and control system resided exclusively on AT&T's telephone network.[166] The ARPANET network was designed to operate even if entire portions of the network were disrupted by using both a newly conceived network design[167] and innovative concept of transmitting discrete packets with their own address and the address of the

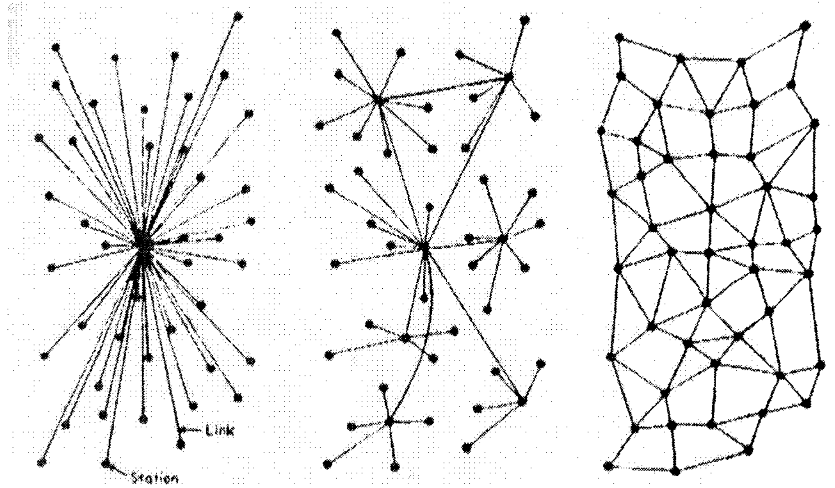
2. A distributed rather than a centralized network which allows the system to continue to function even when some nodes fail;

3. Adaptivity which sends packets to the same destination over different paths of the network based on current network load and connectivity;

4. And the TCP and IP developed to in the 1970s and early 1980s to enable different networks to interoperate (United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future, 10).

[166] The rationale of trying to develop a means of connectivity for the nation's communication systems during nuclear war for founding the Internet is disputed by Robert Taylor, the third Director of the Information Processing Techniques Office in the Advanced Research Projects Agency (ARPA). Taylor was responsible for sponsoring the research based on J.C.R. Licklider's network ideas that led to the Internet. Taylor is adamant that "the project embodied only the most peaceful intentions – to link computers at scientific laboratories across the country so that researchers might share computer resources" (Katie Hafner and Matthew Lyon, Where Wizards Stayed Up Late: The Origins of the Internet, New York: Simon & Schuster, 1996, 10-40).

[167] RAND researcher Paul Baran conceived the distributed network concept to compensate for the "main nerve centers around which links are clustered" of the centralized and decentralized network designs of the telephone system



(a) Centralized *(b) Decentralized* *(c) Distributed networks*

(Hafner and Lyons, 59).

intended recipient of the packet.[168] These packets arrived at the intended designation irrespective of the route traveled.[169]

The network grew exponentially from approximately fifty connected networks to what it is today. By 1973, a nationwide system, ARPANET, was fully operational; by 1981, there were about two thousand individual users and 213 host computers. Partly as a result of the increased number of users, the ARPANET was reorganized into two networks in the early 1980s; the MILNET for classified military applications mainly between military sites in the United States while unclassified applications remained on the ARPANET. The DARPA internet, later shortened to the Internet, initially provided the connection between the two networks.[170]

In the late 1980s, the Internet expanded into overseas networks reaching all continents (including Antarctica); in 1990 the name ARPANET was dropped altogether. Today, from 213 computers in 1981 approximately 181.23 million North American and

[168] The concept of breaking data into "packets" to be transmitted separately over the most expeditious route possible and reconstructing the data into the complete body of data is attributed to both Paul Baran and Donald Watts Davies of the British National Physical Laboratory. Davies, however, is credited with "working out the details of configuring the data blocks" for transmission. To his credit, Larry Roberts, who Robert Taylor had hired to supervise the networking project, synthesized the concepts of both men to make the networking concept work (Hafner and Lyons, 64-67).

[169] The underlying assumption was that if any single link in the network was unreliable; the communications links would have to be redundant and passive (Rochlin, 39 and 44 and Rasch in Ruthberg and Tipton, S-343).

[170] Rochlin, 44-45.

Since both the MILNET and ARPANET would use the TCP/IP protocol, computers on the MILNET would still be able to talk to computers on the ARPANET, but the MILNET network nodes would be more protected. If problems developed on the ARPANET, the MILNET could be disconnected quickly by unplugging the small number of gateways (7) that connected them. According to John Markoff, the Department of Defense did just that during the 1988 Morris Worm incident. As a further safety feature, these gateways were designed to limit the interactions between the two networks to the exchange of electronic mail only (Robert E. Kahn, "The Role of Government in the Evolution of the Internet" in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 16 and John Markoff, "Pentagon Severs Military Computer From Network Jammed by Virus," New York Times, November 30, 1988.

544.2 million individuals worldwide have access to the Internet.[171] In effect, the Internet is the Network of All Networks; an analogue for, but not the actual information infrastructure system even though it is in many cases used as the backbone for both NIIs (to include the National Information Infrastructure of the United States) and the GII.[172] The Internet can be considered the first and most important layer of the information infrastructure system. It was the first network, displays the characteristics ascribed to the infrastructure system, and is the most widely used network in the U.S. and the world. As such, it is the most important component of the infrastructure system; the same events that affect the Internet affect the information infrastructure system.

Beginning in 1985, the U.S. National Science Foundation (NSF) financed the Internet (called the NSFNET) as a joint venture among IBM, MCI, and the nonprofit Merit, Inc. The arrangement was a proving ground for cooperation among government, industry, and academia in the planning, development, and operation of information infrastructure systems. The continued growth and vitality of the Internet demonstrated that commonality of vision can make a decentralized process more efficient and effective and underscored government investment as a catalyst for private investment in both the demand and supply sides of the information infrastructure.[173]

[171] Vibert.

"The art of estimating how many are online throughout the world is inexact at best. Surveys abound, using all sorts of measurement parameters. However, from observing many of the published surveys over the last four years, here is an "educated guess" as to how many are online worldwide as of February 2002. And the number is 544.2 million" (NUA Internet Surveys, NUA.com, http://www.nua.ie/surveys/how_many_online/index.html, January 9, 2001).

[172] Targowski, 144; United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future, 10; Krause in Ruthberg and Tipton, S-262; and Rasch in Ruthberg and Tipton, S-343.

[173] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 199.

Today's Internet points to a future in which the information infrastructure is not a highway but a web, or network, of interrelated public and private networks, platforms, and services.[174] Yet, despite multiple visions and definitions, there is a good chance of attaining a "seamless web" with interoperable facilities and services. However, some components will probably remain disconnected, proprietary, and vertically integrated, i.e., business networks. Many corporations see a need to attach to the Internet as a means of access to a public data network and to take advantage of services such as frame relay provided by carriers. Many commercial organizations also use the Internet as the infrastructure of choice for communicating with counterparts and clients, especially overseas because Internet connections are more reliable than telephone lines.[175]

Most networked personal computers in corporations today are connected to corporate networks (LANs) that are in turn interconnected through the public switched network infrastructure to the Internet.[176] With a projected 75 million networked corporate PCs, private business networks are a very important part of the national information infrastructure and will most likely remain so. However, many of these same organizations opt to maintain their corporate LANs as proprietary, vertical, and closed to outside users [177]

Since its inception there have been concerns about security on the Internet ranging from system penetration to the trustworthy transfer of information and protection of

The Internet is an institution without a real organization, but could be considered a self-organized network of networks. Its existence is predicated entirely on the desire of its participants to perpetuate it; its standardization and coordination are driven entirely by the requirements to adhere to a common set of rules and protocols (Rochlin, 44).

[174] Stearns in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 37.

[175] The WWW, especially, affords a powerful business environment consisting of global connectivity, a user-friendly point-and-click interface, and multivendor, multimedia formats (Krause in Ruthberg and Tipton, 262).

[176] Targowski, 174.

[177] Targowski, 173-174.

intellectual property.[178] The Internet was developed without an overall architectural design to accelerate expansion and not security. Also, in developing the first network the intractability of the technical challenges and the time constraints of the ARPA funding fostered an atmosphere of ad hoc-ness to adopt wherever worked instead of a detailed plan for security. The main concern of the original developers was to produce something that worked, to worry about making it better after demonstrating the concepts feasibility, and to continually improve the performance of the system(s).[179]

In Hafner and Weaver's book, Where Wizards Stay Up Late: The Origins of the Internet (considered the definitive history of the founding of the Internet), the issue of security of the network being created or the data being transmitted across it is not even mentioned, much less seriously discussed. This may sound somewhat strange given that the Department of Defense's research and development organization (ARPA) was the original funding agent for the research and implementation of the origins of what has now become the Internet.

Although security is a concern for all information infrastructure systems, the open nature of the Internet, as well as specific features of its evolving technology, underscore the challenges to Internet security, but advances are being made.[180] And, as is evident, lack of

[178] Neumann, "Denial-of-Service Attacks."

[179] Hafner and Weaver, 247.

The developers and later implementers attitude is aptly illustrated by a comment from a computer scientist involved in the subsequent TCP/IP and OSI internetting protocol, "(choice of technical solutions could be inserted here) should be discovered, not decreed." TCP/IP's eventual acceptance as the networking protocol is considered an "object lesson in technology and how it advances" (Hafner and Lyon, 254).

[180] Because of the increasingly serious security concerns about the Internet, many have proposed a newly structured, industrial-strength, multicarrier, multiprotocol, asynchronous transfer mode, optical fiber-based public internetwork that will be affordable, dynamic, and secure (Krause in Ruthberg and Tipton, 262).

security has not actually halted the expansion of the Internet; individuals and organizations tailor their use to the level and kind of protections available.[181]

A security architecture for the NII (which will have to be built on the architecture of the Internet since it is the predominant network of the NII) seems to be hampered by the same factors that hamper progress toward implementing common architecture generally. John McDonald of MBX Inc. has further identified a number of trends that have led to a **"concentration of `network assets' that increases vulnerability to a single switch failure, line cut, or software system crash,"** notwithstanding the application of a variety of techniques that enhance network integrity. He noted that some of the trends are unintended side effects of strategies to ensure compliance with federal regulations and has argued that integrity and robustness must be "considered from the ground up" and, presumably, in a coordinated manner. Secondly, the fundamental technical approach to network control leads to **"systems that are inherently rigid and subject to failures, requiring heroic efforts to make them robust enough to operate in the real world."** In both instances, McDonald is talking about the same type of systemic vulnerabilities this research addresses and discusses in the following chapter, Information Infrastructure System Vulnerabilities, Risks, and Threats.

In the same way as the Internet, the conceived National Information Infrastructure is not static but is evolving. Virtually all concepts of the NII imply that existing facilities will be used in fundamentally transformed ways. In particular, termination of the network in affordable but powerful computing devices will create an inherently more general-purpose

[181] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 200, 15-16.

communication environment. At the same time, new physical facilities are being built to provide expanded interactive bandwidth to more users.[182] Still to come though is dynamic application deployment; the ability to deploy new applications on the infrastructure without the sort of community-of-interest and standardization problems associated with users having to buy the new software each time a new application is added. Technically, it is possible to deploy applications dynamically over the network itself by downloading new software.[183]

One evolutionary vision for the NII is a single massive upgrade to some chosen new technology. Another advocates a much more incremental process for experimentation and upgrades through smaller staged investments that bring in a series of new technologies. Such incrementalism will most likely establish a pattern of continuous technology improvements justified by proven market demand, but also produce a slower and more measured pace of investment and, consequently, deployment.[184] Regardless of which vision or hybrid of the two is realized, private firms will build it. Therefore, their business plans must justify the investments with the creation of a competitive advantage and/or new markets, not the pursuit of abstract visions or societal goals.[185]

The public policy challenge is to provide a framework in which this evolution may occur (to be discussed in Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy).[186] Addressing security, reliability, recoverability, and associated protections may be the most constructive

[182] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 200, 6-8.

[183] Targowski, 154.

[184] Horton, 10.

[185] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 22.

[186] Mayo in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 6.

areas in which the government can influence overall architecture development in the evolving National Information Infrastructure. If security is seen as a business decision only, public policy will have to impact standardization; the role of governments; electronic signatures and cryptographic key and certificate management; mechanisms for security and other protections; and the need for yet other processes to ensure that a complex and multifaceted information infrastructure, in much the same way as the relatively simpler telephone network in comparison, can meet national security and emergency preparedness needs.[187]

2.6. The Global Information Infrastructure (GII).

> The GII is envisioned as the universal, integrated global telecommunications network serving as the opto-electronic conduit for economic, social, cultural and political exchange in the 21st century.[188]

Although the focus of this research is the U.S. National Information Infrastructure, to describe most completely that infrastructure system, to put it in perspective, and to best address its vulnerabilities it is necessary to describe also the Global Information Infrastructure system. As the Joint Security Commission said in its 1994 report,

> "The network architecture of the future will comprise a seamless global web of unsecured electronic highways linked together to provide a common infrastructure operated as a utility. Subscribers will be a heterogeneous group of individuals and organizations tied into the network to communicate with each other and to obtain various services offered by some portion of the network."[189]

As should be evident from Figure 2.5. Conceptual View of NII Architecture, the U.S. NII (as do all NIIs conceptually) connects to the GII. With the open architecture of most public networks, a user can access their NII through their Local Information

[187] Horton, 210-212.
[188] Horton, 1-6.
[189] United States Joint Security Commission, Redefining Security, A Report to the Secretary of Defense and the Director of Central Intelligence, Washington, D.C., February 28, 1994, Chapter 8, "Information Systems Security."

Infrastructure (LII) and, subsequently, the GII and all other NIIs with little effort or challenge. Therefore, anyone anywhere in the world has easy access to the U.S. information infrastructure system and would be able to exploit its vulnerabilities with relative ease.

The concept of a Global Information Infrastructure, like the NII, corresponds to the Internet as a worldwide network, but is even more chimerical. The envisioned GII can be thought of as a "constellation" of thousands of computer networks used by millions of people located wherever people live; in effect, the worldwide interconnection of telecommunications networks, computers, data bases, and consumer electronics.[190] In reality, the GII is a geographically expanded NII still intended to serve individuals, not institutions. It is similarly perceived as an open, self-organizing, interactive, resilient, interconnected system providing dynamic and democratic means for people not only to find information but also to put forward their own ideas for others to see.[191]

The GII, also, is not intended to be entirely monolithic. Like the NII just described, it will feature interfaces with private and public networks resulting in a matrix of Local Area Networks (LANs), Metropolitan Area Networks (MANs), Rural Area Networks (RANs), Wide Area Networks (WANs), and Global Area Networks (GANs) integrated and aggregated into Local Information Infrastructures (LIIs), National Information Infrastructures (NIIs), or the Global Information Infrastructure (GII).[192] Such a conceptualization visualizes the GII not only as the aggregation of all NIIs, but also of all

[190] United States Department of Defense, Report of the DSB Task Force on Information Warfare (Defense), Appendix C – "A Taxonomy for Information Warfare."
[191] Targowski, 143.
[192] Targowski, 1-6 and 8.

GANs (institutional and private networks that have global reach with no regard for national boundaries, e.g., the Internet and multinational corporations' private internal networks).

The key to unlocking the power of global networking lies in the intelligent signaling capabilities offered by CCS7, ISDN, B-ISDN, and service-specific networks. If designed properly, a global network will accept any interface and interconnection of choice from asynchronous transfer mode and cell relay to X.25 data packet or analog voice or video. These different signaling systems are necessary to achieve functional transparency across multiple national and private networks and to enable deployment of private virtual networks on a global basis.[193]

The envisioned GII is also intended to be responsive to change.[194] Like the Internet, it is envisioned that each country and each region will make its own decisions about the development of the GII. There should be no international mandate for development,[195] but rather each country and society should develop its own system as part of a larger network. The most apparent advantages of such a network is that critical information, no matter where it is located, is available when needed. But it will be possible only if the information infrastructure is transparent for every user and computer and communication technology,[196] i.e., "open."

[193] Targowski, 28 and 85.

[194] Horton, 51.

[195] Horton, 54.

As Martin Bangemann, member of the European Commission, opined at the Telecom Interactive `97 International Telecommunications Union Conference, "There is no blueprint for the Information Society. It is a process that we can shape but not dictate" (Martin Bangemann, "A New World Order for Global Communications: The Need for an International Charter," Speech to Telecom Interactive `97, International Telecommunications Union, Geneva, Switzerland, September 8, 1997).

[196] Targowski, 67.

One characteristic of such "open" networks is that distance is irrelevant. Business and work collaboration and the exchange of information just as easily take place across oceans as within the same city. As a result, there will be a steady increase in cross-border communications, collaboration, electronic trading, and other business.[197]

Much of this electronic business would be conducted via private or institutional Global Area Networks (GANs). Although they evolved originally as private networks with packet switches, multiplexers, and multiprotocol bridges/routers to interconnect local area networks (LANs) serving widely dispersed facilities, GANs today are, for the most part, hybrid public and private systems that take advantage of the explosive growth in undersea fiber, intelligent gateway switches, and highly featured private virtual networks. In most cases, GANs are extensions of domestic applications developed by large corporate users in advanced industrialized countries.[198]

One such GAN is the Electronic Fund Transfers System (EFTS). The EFTS manages an electronic payment system for processing, producing and distributing services incidental and/or related to economic exchanges. It contains a cluster of related practices and information technology that employ electronic impulses generated and interpreted by computers to debit and credit transactions (i.e., an electronic fund transfer) locally, regionally, nationally, or internationally. The EFTS with its transparent standardized procedures and the details of packet assembly, routing, reassembly, etc., is the core financial

[197] Bangemann.

In order for these envisioned activities to succeed, more reliable mechanisms for cooperative authentication, resource allocation, and charging are needed as the various national information infrastructures aggregate into a true Global Information Infrastructure (United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 1997 Implementation Plan, December 1996).

[198] Targowski, 84.

information highway that provides convenience, control, and connections. The EFTS system introduced, de facto, a new electronic financial order that integrates and smoothes a flow of electronic money among nearly 3,000 banks in more than 70 countries since 1989. Only one condition has to be satisfied, the participating institutions must have a gateway to EFTS.

Electronic Data Interexchange (EDI) image technology generates the digital data from checks and other financial instruments to activate the electronic wire transfer of funds, direct deposit of checks, periodic or authorized payments, check verification, and credit card authorizations over EFTS. Point-of-sale (POS) systems, automated teller machines (ATM), and automated clearinghouses (ACH) that access stored information via fuzzy queries represent more advanced methods to activate EFTS and transact business exclusively through electronic signals.[199]

The automated clearinghouse (ACH), created in 1968 by ten California banks' Special Committee on Paperless Entries (SCOPE), has become the true heart of the EFTS. The committee's mission was to develop and implement a system of "preauthorized paperless entries." The first ACH modeled on SCOPE was in operation in December 1974 in San Francisco with Los Angeles, Boston, Minneapolis/St.Paul and others soon following. The National Automated Clearing House Association was formed soon after to facilitate the application of ACHs in all 12 Federal Reserve Districts. The ACHs are now integrated with the national Fed Wire, Bank Wire, the global Society for Worldwide Interbank Financial Telecommunications (SWIFT), and other financial networks (such as CIRRUS, PLUS,

[199] Steven K. Black, LtCol., USAF, A Sobering Look at the Contours of Cyberspace, Ridgway Viewpoints, No. 96-3, Matthew B. Ridgway Center for International Security Studies, University of Pittsburgh, June 1996, 54-56.

CHIPS) that can transfer electronic money and other added value information around the nation and the globe.[200]

The open concept upon which the EFTS depends and the GII is more than likely to manifest makes the interface between the different national information infrastructure systems and the GII of great importance. This gateway function must be able to interact with national and international networks, accepting calls from switching nodes in other countries, performing digit evaluation and transportation, and routing those calls to their destinations. Technically, the biggest problems is supporting multiple interfaces and universal error control systems and dealing with satellite and other processing delays. To carry out these functions, the international gateway switch must be able to recognize and process a wide variety of international trunk signaling and testing protocols, as well as translate dialed digits that differ from country to country.[201]

A global information infrastructure system able to accommodate sophisticated functions such as EFTS and other equally and more advance activities will require massive development around the world. Many countries have only minimal access to communications technologies and very primitive or poorly developed internal and external connectivity. China, for example, will spend $600 billion on information infrastructure in the next 6 years. Without huge spending on such infrastructure, developing nations will experience bottlenecks that impede their economic growth and social progress, leaving them still further behind the rest of the world.[202]

[200] Targowski, 169, 176-177 and 188.

[201] Targowski, 88.

[202] Steven D. Dorfman, "Satellite Communications in the Global Information Infrastructure" in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 42.

Despite the clear intention of the industrialized world to foster building national backbones and the gradual diffusion of connectivity in many developing countries, the traditional state-owned telecommunications operator structure remains a serious obstacle to a truly international information infrastructure system. While technical difficulties can be overcome, the tradition of control over the communications infrastructure and services is more difficult to displace. Although this state-owned telecommunications operator structure has been seriously undermined in the United States, the European Union, and parts of Asia, it remains strong elsewhere.[203]

2.7. Conclusions.

As can be seen from the discussion, the information infrastructure system is not an easy subject to comprehend. Although it is essentially only the integration of computing resources with transmission resources, both are extremely complex systems in their own right. When the two are integrated to produce a unitary system, the complexity only magnifies quantumly. Just as with innovation and vulnerabilities, the two systems have a synergistic effect on the combined product.

As one conceptualizes at each higher abstract level (i.e., from a generic information system to a LAN and the other geographical organizational schemes to a NII to the GII[204]), the degree of complexity further multiplies because of the increase in scope and differences in each system added to the aggregation. This increased complexity only adds to Perrow's admonition about systems:

[203] Targowski, 225.

[204] In actuality, the NII and GII labels are misleading since there are few distinct boundaries in the information environment (United States Department of Defense, Report of the DSB Task Force on Information Warfare (Defense), Appendix C – "A Taxonomy for Information Warfare").

> “Every part of ever system is liable to failure. The more complicated or tightly coupled a system, the more attention needs to be paid to reducing the occasion for failures, but this can never be enough. If we add catastrophic potential, then everyday failures should not go unremarked. They now become significant.”[205]

Because of complexity, any loss of availability, virus infection, unauthorized intrusion, or other breaches of the information infrastructure system’s security objectives should raise concern as Microsoft, Ebay, Yahoo, and countless other commercial and government agencies have unfortunately discovered. Unfortunately, the complexity is not static but increases every time a new innovation for the computing or telecommunication system is unveiled making protecting the infrastructure system only infinitely more difficult. The next chapter discusses in more detail how the vulnerabilities and complexity of the individual computing and telecommunications systems and their aggregation into the information infrastructure system specifically create vulnerabilities that can lead to risks.

[205] Perrow, 43.

CHAPTER 3

INFORMATION INFRASTRUCTURE SYSTEM VULNERABILITIES, RISKS, AND THREATS

3.1. Introduction.

> Networks were created to facilitate ease of use and management of multiple systems and the sharing of resources between computers, with only a minimum of security to hamper users.[206]

All information systems are vulnerable to attack, especially if they are connected to another system, and to completely secure a system, if even possible, would be extremely expensive.[207] The variety of vulnerabilities and the sheer volume and mix of old (legacy) and new software of the information infrastructure system make plugging all of the holes a continuous, impossible task.[208] "As 3Com Corp's Chuck Semeria says, "The only way to be guaranteed 100 percent security is not to be connected,"[209] but even then, system security would be jeopardized by authorized users ("insiders"), threats to system operational requirements (i.e., temperature, power, humidity, etc.), and environmental threats.

However, such an unconnected information system is infinitely less useful than one that is connected. Further, such an unconnected system surely would not be the U.S. information infrastructure system. By the previous chapter's definition, an information infrastructure system is the totality of all computing systems connected by a transmission system within a defined domain, in this case the United States. Since this research is

[206] Pipkin, 97.

[207] Pipkin, 6.

[208] Pipkin, 6 and 61; Sharon Machlis, "Military Beefing Up Its Hacker Defenses; Concerned About Risks to National Security," Computerworld, April 7, 1997, 6; and Robert Ellison, et.al., Foundations of Survivable Systems Engineering, 1.

Also see Foundations for Survivable Systems Engineering for an emerging approach to addressing the effects of exploitation of the system's vulnerabilities from a systemic approach.

[209] Mary Carmen Cupito, "Creating Web Windows May Leave Doors to Data Unsecure," Health Management Technology 18, no. 10 (September 1997), 24.

concerned with the information infrastructure system and its relevance to U.S. national security, I obviously will examine interconnected U.S. information systems connected to the rest of the world's information systems. Unfortunately for the United States' national security, the President's Commission on Critical Infrastructure Protection came to the conclusion that the "computer information infrastructure's security ... is in serious trouble."[210]

Much of the cause of this risk to the United States' national security by the information infrastructure system can be attributed to the integration of the computing and transmission systems into an information infrastructure suprasystem. As defined in Chapter 2. Information Infrastructure System, connection of separate computing functions (the computing subsystem) within a defined domain by a transmission medium (the transmission subsystem) makes the information infrastructure system a suprasystem. A suprasytsem is conceived and designed to maximize the strengths of connected subsystems to produce benefits greater than the benefits of the individual subsystems.

Unfortunately, such a combination of subsystems permits not just the maximization of benefits, but also a "maximization" of vulnerabilities. Each subsystem vulnerability ultimately achieves an effect (or risk) orders of magnitude greater than the original effect because the interconnectivity allows a vulnerability's effect(s) to migrate from the original suprasystem's subsystem in which it occurs to other parts of that particular subsystem or to other subsystems to which the original subsystem is connected in the same way that strengths of subsystems migrate to produce benefits greater than each individual subsystem's benefits. In the case of the information infrastructure system, this

[210] United States White House, Critical Foundations: Protecting America's Infrastructures.

interconnected suprasystemic property allows any effect produced by exploitation of the computing and transmission subsystems' vulnerabilities to imperil one or some combination of the previously discussed five information assurance security objectives[211] of the entire information infrastructure suprasystem.

For the purpose of this chapter's research on the information infrastructure system's vulnerabilities, I choose to focus on those vulnerabilities that are unique to an information infrastructure system: defects in the individual hardware and software (faults and errors)[212] components and those inherent systemic properties ("openness" (open network architecture), interconnectiveness, and complexity) postulated in Chapter 1. Introduction to exacerbate software's vulnerabilities. To be sure, other vulnerabilities associated with physical systems that depend upon human and other inputs for operation exist, e.g., loss of electrical power which may halt a system's operation but can also affect the environmental conditions the system requires to operate, disruption of the physical structures that support the information infrastructure system whether deliberate or inadvertent,[213] "insider" abuse, etc. As discussed earlier, these types of vulnerabilities are classic, knowledge about them and the methodology to defend against them is well known, and little new can be said about them other than how their effects are able to cascade from one subsystem to another threatening the entire system instead of just the initially affected one.

[211] See Chapter 1. Introduction for a discussion of the Information Assurance objectives and their definitions.

[212] See Chapter 1. Introduction for a discussion about the definition of terms that denote software failure.

[213] In Newark, New Jersey, on January 4, 1991, an AT&T crew trying to remove an old cable inadvertently cut another. Approximately 100,000 calls were disconnected and 60 percent of the attempted long-distance phone calls from New York did not get through that day. The New York Mercantile Exchange and several other commodities exchanges were shut down. Air traffic control was also disrupted because systems are interconnected resulting in flight delays from New York, Boston, and Washington, D.C (Wiener, 22).

The intent of the chapter, then, is to demonstrate that those inherent systemic properties of openness and interconnectivity that make the information infrastructure system so useful and appealing contribute significantly to its liabilities. The ever-increasing interactive complexity of the system's interconnectivity further makes it increasingly more susceptible to system accidents. Although the vulnerabilities of the system's software are at the root and troublesome enough as will be shown in the discussion that follows, the synergistic effects produced by interconnectivity are the more serious, pervasive, least understood, and most difficult to address vulnerabilities. It is the combination of effects from all of the types of vulnerabilities, more serious than each individually, that imperils U.S. national security.[214]

I also intend to focus on the most feared exploitation: an unauthorized user, or intruder.[215] Even though software vulnerabilities are susceptible to other exploitations that can also be damaging and, in some cases, devastating (e.g., viruses, worms, overflows, etc.), the unauthorized intruder generally represents the worst-case risk for system users. Intrusions and accidental defects may possibly have the same effects; the improper modification or destruction of sensitive information and/or the disclosure of confidential information,[216] but an intruder, of all the potential threats, is the only one that singularly can directly jeopardize all five information assurance security objectives.

[214] Pipkin, xi-xii.

[215] The security profession recognizes intrusion as the most significant risk to the automated information systems community (Donald L. Evans, and J.A. Morrison, "Penetration Testing," in Ruthberg and Tipton).

[216] Jean-Charles Fabre, Yves Deswart, and Brian Randell, "Designing Secure and Reliable Applications using Fragmentation-Redundancy-Scattering: an Object-Oriented Approach" in Randell, Laprie, Kopetz, and Littlewood, 173-174.

The ARPANET "crash" of October 27, 1980 resulted from bits accidentally being dropped in the time stamp of one status word. The resulting multiplicity of three versions (two corrupted) of the same status word (with different time stamps) broke the garbage collection algorithm, and so degraded the

The deliberately open nature of the infrastructure system facilitates an intruder's relatively easy unauthorized access to and navigation of the system to locate other hardware and software vulnerabilities for further exploitation or a particular sub-system and/or data they are seeking.[217] The Federal Communications Commission mandated an evolution toward open network architectures that have as their goal equal, user-transparent access via public networks to network services provided by network-based and non-network enhanced service providers. **Unfortunately, when implemented, the concept makes network control software increasingly accessible to both users and adversaries** (emphasis added by author). The Telecommunications Act of 1996 also required carriers to collocate key network control assets and to increase the number of points of interconnection among the carriers further facilitating an intruder access.[218]

At the same time, these same vulnerabilities make it easy to execute the current attack du jour: denial of service directed at both single and distributed targets.[219] This type of attack is particularly insidious and difficult to defend against because it is able to exploit not only the "widespread weak links that permit internal exploitations" but also "fundamental architectural deficiencies" of the systems themselves, particularly the routers that "interconnect the networks comprising the Internet.[220] Traditionally, the intent and impact of denial of service attacks is to "prevent or impair the legitimate use of

ARPANET that it was nonfunctional (Peter G. Neumann, "Re: Worm/Virus Mutations," The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 71 (November 6, 1988), http://catless.ncl.ac.uk/Risks/7.71.html).

[217] Vibert.

[218] United States Department of Defense, Report of the DSB Task Force on Information Warfare (Defense), Section 2.3 – "The Infrastructure."

[219] Kevin J. Houle and George M. Weaver, Trends in Denial of Service Attack Technology, CERT Coordination Center, Pittsburgh, PA: Carnegie Mellon University, October 2001, 1.

[220] Neumann, "Denial of Service Attacks" and Houle and Weaver, 14.

computer or network resources." What is especially troubling about this type of attack is the increased frequency and evolution of attack methodology and technology leading to greater systemic impact for each new type of attack.[221] Denial of service attacks will be discussed in greater detail in Appendix B. Denial of Service.

Similar to the chapter on the infrastructure's description, I will initially focus on the individual component's vulnerabilities and then progress to systemic vulnerabilities. I will devote considerable time to detailing the specific vulnerabilities of software since these vulnerabilities truly are the root of the system's technological vulnerabilities[222] and possibly the most intractable to remedy.

3.2. System Components' Vulnerabilities.

It is not the purpose of this research to either document or categorize all of the different vulnerabilities of all components of the information infrastructure system even if that were possible. Known vulnerabilities of the information infrastructure system and their exploitation are well documented in the academic, trade and popular press.[223] Several

[221] Houle and Weaver, 1 and Roger M. Needham, "Security Cyberspace: Denial of Service: An Example," Communications of the ACM 37, no. 37 (November 1994), 44.

[222] "A lot of new computer attacks are based on new programming vulnerabilities. ...software and vendors are mostly to blame for security problems." Peter Bartoli, a "white hat" hacker and Technical Director, for Security Analysis Practice, SAIC (Andrea Siedsma, "Spy vs Spy," T Sector: Everything Tech San Diego, January 2001).

[223] There are numerous articles, surveys, and organizations that strive to keep track of computer-related vulnerabilities by recording incidents as they appear. Two of the earliest articles were by E.H. Spafford, "Crisis and Aftermath," in Communications of the ACM, June 1989, and Levinson and Turner, "An Investigation of the Therac-25 Accidents," of the Information and Computer Science Department, University of California – Irvine in 1992 (Landwehr, et.al., 211).

Peter Neumann at SRI International published some of the earliest comprehensive data on vulnerabilities in a 1995 book, Computer-Related Risks, which contained 1174 examples of computer-related security problems. Neumann also edits and maintains the ever-growing **Illustrative Risks to the Public in the Use of Computer Systems and Related Technology** that summarizes most of the interesting cases of security breeches over the past decades. It can be browsed or *ftp*ed in PostScript or pdf form from ftp.sri.com or from csl.sri.com.

Two of the best-known current surveys are Common Vulnerabilities and Exposures (CVE) (http://cve.mitre.org) and SANS Resources' "How to Eliminate the Ten Most Critical Internet Security attempts at a categorization or taxonomy of security flaws have also been proposed[224] with differing degrees, but without acknowledged consensus, of success. Instead this research intends to illustrate some of the more common and well-known vulnerabilities to demonstrate categories of risks to the system and the ease with which an agent can exploit the information infrastructure system.

Vulnerability issues in hardware concern the design and implementation of processor hardware, microprograms and supporting chips, and any other hardware used to realize the machine's "instruction set architecture." It is not uncommon for even widely distributed processor chips to be incompletely specified, to deviate from their specifications in special cases, or to include undocumented features. Pure hardware failures are rare, but when they do occur generally result in improper synchronization and execution, bit loss during data transfer, or incorrect results after execution of arithmetic or logical instructions[225] leading to loss of system availability or data integrity. Such pure hardware faults are generally easier to fix than software faults since hardware designs are usually

Threats: The Experts' Consensus." Version 1.32. January 18, 2001. http://www.sans.org/topten.html. CVE is a "list of or dictionary that provides common names for publicly known information security vulnerabilities and exposures" CVE's list contained 1510 entries as of May 7, 2001.The SANS document is a list of the ten most critical Internet security problem areas – clusters of vulnerabilities that system administrators need to eliminate immediately.

The best-known organization providing vulnerability incident information is CERT (www.cert.org) but many other governmental and private centers now exist.

[224] Chillarege et. al. in 1992, Florac in 1992, and Brehmer and Carl in 1993 focused on collecting vulnerability data during the software development process for the purpose of improving the process. Landwehr et. al. focused on detected security flaws after software was released for operational use (Landwehr, et.al., 212).

[225] Landwehr, et.al., 224 and 227.

Early versions of the Intel 80486 chip had faulty trigonometric functions, but they were discovered before the chip was incorporated into millions of personal computers. In this case, the fault would possibly have affected both the integrity of the data and not the availability of the system (Wiener, 49).

Also see Case MU9 on p. 239 in 54 for the description of an inadvertently added flaw by the vendor while fixing another problem in a GE –645 "Subverter" that allowed a potential intruder to gain control of the machine. Another example of a hardware security flaw occurred in the VAX Security Kernel on Intel's 80386/8037 Processor/CoProcessor Set when CPUs with access to a clock shared a common bus (Landwehr, et.al., 249).

simpler and incorporate repetitive structures, such as memory, that are less confusing to understand.[226]

However, vulnerabilities of hardware components are more than likely the result of defects and faults in software features (even those frozen into silicon) integrated into the hardware to differentiate it from the competition or to aid in the support and maintenance of the hardware.[227] This tendency to exploit the versatility of software-based systems, at the expense of greater complexity, is understandable in many routine, low-risk applications (e.g., Bell system telephone switches in the U.S. reportedly satisfied the requirement of 3 minutes maximum down-time per year, at least before the large outage on the 15th of January, 1990), but should be avoided in high-risk applications.[228] Most, if not all, of the system hardware components in the earlier description of the information infrastructure system are now dependent upon software to facilitate and enhance their operations.

Some hardware components that have been exploited because of security flaws in the past include:

[226] Wiener, 49.

[227] Landwehr, et.al., 224.

The tendency in IT system development, unmistakedly, seems to be to transfer as much of a component's functionality as possible to software, sometimes with an intent to reduce the hardware unreliability or provide other benefits, such as ease of modification. Even when it is reasonable to use software to overcome hardware reliability limitations, there is usually an irresistible temptation to integrate additional software into the hardware to provide more desired functionality, sometimes at the risk of lower design dependability, but always increasing complexity (Jean-Claude Laprie, Christian Beounes, Mohamed Kaaniche, and Karama Kanoun, "The Transformation Approach to the Modelling and Evaluation of Reliabilty and Availability Growth" in Randell, Laprie, Kopetz, and Littlewood, 474-475).

[228] Jean-Claude Laprie, Christian Beounes, Mohamed Kaaniche, and Karama Kanoun, "Validation of Ultra-High Dependability for Software-based Systems" in Randell, Laprie, Kopetz, and Littlewood, 474-475 and 480.

- terminals with memory (smart terminals),[229]

- X terminals,[230]

- the computer terminal itself,[231]

- modems,[232]

- switches[233], and

- various other input/output devices.[234]

[229] Potential intruders may be able to execute a smart terminal's escape sequence to have the terminal send them the data that is stored in the terminal's memory. They may also be able to send a command string to the terminal and force the terminal to send it to the program that is running on the terminal (Pipkin, 58-59).

[230] An intruder may be able to run terminal software on another person's X terminal or get remote access to the peripherals (e.g., floppies, CD-ROMS, or scanners, etc.) that are attached to another X terminal if the X protocol that executes graphics programs is not properly configured and/or protected (Pipkin, 58-59).

[231] A spoof that simulates the login sequence can be planted by logging onto a terminal and running the program with the "exec" command; the spoof becomes a "virtual" login session. It will appear to be a login session to the authorized user. After the authorized user enters their ID and password, the program will tell them that the login is incorrect. The authorized user will usually exit leaving the real login sequence to reprompt (Pipkin, 47 and 186).

A "spoof" is a program that impersonates another program to gather information by fooling a user or another computer into volunteering information (Pipkin, 47 and 186). Spoofing is such an easy technique for intruders to gain access or additional privileges (that DoD's Advanced Research Projects Agency ARPA) is searching for ways to make Internet addresses less prone to domain spoofing ("ARPA Moves on `Spoofing'," 1998 Exchange Telecommunications Newsletter, September 4, 1998 and John Borland, "Feds Work to Block Domain-Name Hackers" TechWeb News, August 26, 1998, http://www.techweb.com/wire/story/domnam/TWB19980825S0013).

[232] Modems are one of the most common devices an intruder will use. Not only will a modem with dial-out capabilities allow the intruder to "connection launder," (dialing through a system and into another program to gather information) but it also provides opportunities for gaining unauthorized access to another system by connecting to the modem's port, using a login spoof on the port, and collecting passwords from those who dial up the system. If the modem is both dial-in and dial-out, the system may also be subverted by conditions created when trying to dial-in while the system is dialing out (Pipkin, 93-94).

[233] Given the nature of the modern switch with its millions of lines of software code (See preceding chapter on the description of the information infrastructure system's components), one would expect the same degree of faults and defects in a switch as in any other software intensive system to provide vulnerabilities that can be exploited. Despite best efforts, the software that controls the telephone network has approximately one error for every thousand lines of code when it is initially incorporated into the system. Extensive testing and simulation cannot discover these errors (Leonard Lee, 99).

Kevin Poulson was probably the master at exploiting the vulnerabilities of the public telecommunications switch (See Appendix A. Kevin Poulson for a description of Poulson's activities). His exploits are even more remarkable because of the difficulty of identifying which of the many paths are used by any particular customer for a given transmission or connection. The protocols used in digital networks, the extensive multiplexing hierarchy, and the signaling system also present formidable challenges to an intruder (Dennis Willets, "Telecommunications Security" in Jackson and Hruska, 738).

[234] An example of just such a software vulnerability in an input/output hardware component occurred in the

Most of these vulnerabilities will be discussed in greater detail in the next section describing unauthorized access.

As the preceding discussion suggests, software errors and faults are acknowledged as the most widespread cause of information infrastructure systems security failures.[235] When software companies or advisory services such as CERT[236] issue warnings, those warnings are mostly about vulnerabilities in specific software programs. Unfortunately, those exploited vulnerabilities that cause the incident are inherent to the component

summer of 2000. Hewlett Packard was forced by a lawsuit to provide a "patch' for a floppy disk controller defect. The lawsuit claimed that some HP products contained a floppy disk controller, which may, in rare circumstances silently misrecord data due to a design error in controller technology. This may occur when data is being transferred to or from a floppy disk or tape device that utilizes a floppy disk controller while the computer is simultaneously performing other functions (multi-tasking) that place significant stress on the system.

The design error creates the potential for data corruption or data loss (loss of data integrity in information assurance objectives terms) only when the floppy disk controller is transferring the 512th byte of a sector and, in extremely rare circumstances, the subsequent sector of data, but only if the computer is simultaneously experiencing activity on the I/O bus sufficient to cause a significant delay in the transfer of that byte, but no other byte (Hewlett-Packard Company, Floppy Disk Controller Patch Homepage, http://www.hp.com/cposupport/nonjsnav/patch_faq.html).

[235] Security failures are caused most often by software defects, such as the omission of a particular data integrity function in the system. These defects can be accidental, or they can be intentional, these latter may be malicious (Trojan horses, trap-doors) or non-malicious (resulting, for example, from deliberate trade-offs between security and efficiency) (Bev Littlewood, Sarah Brocklehurst, Norman Fenton, Peter Mellor, Stella Page, David Wright, John Doson, John McDermid, and Dieter Gollman, "Towards Operational Measures of Computer Security: Concepts" in Randell, Laprie, Kopetz, and Littlewood, 539-540).

A Trojan horse is a program that looks like a useful program containing hidden code that, when invoked by the user, performs some covert function. The best Trojan horses will do what they advertise as well as the intended covert action. Trojan horse programs generally are used to accomplish some function indirectly that an unauthorized user could not accomplish directly (Pipkin, 50 and 111).

A Trojan horse that replicates itself by copying its code into other program files is commonly referred to as a virus; one that replicates itself by creating new processes or files to contain its code, instead of modifying existing storage entities is often called a worm (Landwehr, et.al., 218).

Although not precisely a Trojan horse, a hidden piece of software code that responds to a special input, allowing its user access to resources without passing through the normal security enforcement mechanism is referred to as a trapdoor. Still another type of hidden software code is the time-bomb or logic-bomb: a piece of code that lies dormant in the host system until a certain "detonation" time or event occurs (Landwehr,et.al., 218).

[236] CERT, a function of the Software Engineering Institute of Carnegie Mellon University, is the oldest and largest of the security incident information sharing programs. It gathers and disseminates information on incidents, product vulnerabilities, fixes, protections, improvements, and system survivability (Karama Kanoun and Jean-Claude Laprie, "Software Reliability Trend Analyses: From Theoretical to Practical Considerations" in Randell, Laprie, Kopetz, and Littlewood, 71 and www.cert.org).

(software) that makes the information infrastructure system possible and functional. Software engineers, designers, and developers reluctantly acknowledge that it is impossible to produce a software program of any size without any errors at this time and that even after the most thorough and rigorous testing, some faults, errors, and contradictions will remain.[237] Faults and errors are inherent in and endemic to the nature of software: complex logic systems, often poorly structured, invisible, abstract, discontinuous, unconstrained by common sense or physical laws, and with so many possible states without real-world analogues that no human mind can grasp them all.[238]

Why would (or should) the component on which the information infrastructure system depends be so unreliable given that most software and the system(s) it inhabits are designed to increase functional efficiency? Software products are among the most complex artifacts that humans produce, and software development is among mankind's most complex undertakings.[239] Security of and in these products (and the system of which they are an integral part) is generally considered too late and, most often, as a separate "thread of project activity" in the development cycle given the other problems involved in software

[237] Leonard Lee, 98; John D. Musa and A. Frank Ackerman, "Quantifying Software Validation: When to Stop Testing," IEEE Software 6, no. 3 (May 1989), 19; and Laprie, et.al., "Validation of Ultra-High Dependability for Software-based Systems" in Randell, Laprie, Kopetz, and Littlewood, 373-374.

[238] Wiener, xi-xii, 39 and 64; Pipkin, 13; and Laprie, et.al., "Validation of Ultra-High Dependability for Software-based Systems" in Randell, Laprie, Kopetz, and Littlewood, 474.

"Large software systems are among the most complex creations of the human mind, " points out the National Science Foundation's William Wulf. Many software systems "have exceeded the ability of humans to comprehend them" (Leonard Lee, 264).

[239] Wiener, 193.

"Software programs," says UNC professor Frederick Brooks, a leading expert on computer programs, "are more complex for their size than perhaps any other human construct" (Leonard Lee, 99).

design and development.[240] Plus, software development is at a very early stage of maturity in comparison with other scientific and engineering disciplines.

Digital systems, in general, implement discontinuous input-to-output mappings intractable by simple mathematical modeling. This last point is particularly important; continuity assumptions cannot be used in validating software, and failures are caused by the occurrence of specific, non-obvious combinations of events, rather than from excessive levels of some identifiable stress factor.[241] Further, software is often used to implement radically new systems, which cannot benefit much from knowledge acquired from previous, successful designs. As a result, many faults and errors, such as those from competition between security and other functional requirements, from missing requirements or undetected conflicts among requirements, or as a byproduct of inadequately defined module or process interfaces,[242] may be inadvertently included in the finished software code. Often, accommodating unplanned and unexpected interactions in the new software means solving some difficult technical problem while still on a tight production schedule.[243]

The average warranty for most commercial software implicitly acknowledges that software is essentially unreliable[244] with major faults, defects, contradictions, and false promises even though it supposedly has been completed, tested, and is now functional.[245]

[240] Robert Ellison, et.al., Foundations for Survivable Systems Engineering, 1-2.

[241] Laprie, et.al., "Validation of Ultra-High Dependability for Software-based Systems" in Randell, Laprie, Kopetz, and Littlewood, 474.

[242] Landwehr, et.al., 222.

[243] Charlotte Adams, "DoD Security Software: Good Year for COTS," Military & Aerospace Electronics 9, no. 2, February 1998 and Wiener, 75-76.

[244] Wiener, 100.

[245] Wiener, x, 4 and William J. Brown, Raphael C. Malveau, et.al. AntiPatterns: Refactoring Software, Architectures, and Projects in Crisis. New York: John Wiley & Sons, Inc., 1998, xxii; 49.

The Microsoft Windows 98 warranty is an excellent example of the warranty provided by most commercial vendors. At no point in the warranty does the company guarantee the software's proper functioning and assigns all responsibility for its proper operation to the user.

"DISCLAIMER OF WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MICROSOFT AND ITS SUPPLIERS PROVIDE TO YOU THE OS COMPONENTS, AND ANY (IF ANY) SUPPORT SERVICES RELATED TO THE OS COMPONENTS ("SUPPORT SERVICES") AS IS AND WITH ALL FAULTS; AND MICROSOFT AND ITS SUPPLIERS HEREBY DISCLAIM WITH RESPECT TO THE OS COMPONENTS AND SUPPORT SERVICES ALL WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY (IF ANY) WARRANTIES OR CONDITIONS OF OR RELATED TO: TITLE, NON-INFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES, ACCURACY OR COMPLETENESS OF RESPONSES, RESULTS, LACK OF NEGLIGENCE OR LACK OF WORKMANLIKE EFFORT, QUIET ENJOYMENT, QUIET POSSESSION, AND CORRESPONDENCE TO DESCRIPTION. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE OS COMPONENTS AND ANY SUPPORT SERVICES REMAINS WITH YOU."

"EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL MICROSOFT OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR: LOSS OF PROFITS, LOSS OF CONFIDENTIAL OR OTHER INFORMATION, BUSINESS INTERRUPTION, PERSONAL INJURY, LOSS OF PRIVACY, FAILURE TO MEET ANY DUTY (INCLUDING OF GOOD FAITH OR OF REASONABLE CARE), NEGLIGENCE, AND ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE OS COMPONENTS OR THE SUPPORT SERVICES, OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS SUPPLEMENTAL EULA, EVEN IF MICROSOFT OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES."

An even more explicit example of commercial vendor's shirking of responsibility for software is the disclaimer included as part of Microsoft's "patches" for identified software vulnerabilities:

> "**Disclaimer:** The information provided in the Microsoft Knowledge Base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply" ("Cumulative Patch for IIS.").

Reinforcing the negligible value of the warranty, a printed copy of the warranty is generally not prominently displayed on the product for the consumer to read before purchasing the product.[246]

Software errors generally occur in operating system programs,[247] support software, or application programs[248] when a program encounters a situation the designer did not

[246] Software's warranty is generally located in the front of the user's manual, if the purchased software is accompanied with one. In many cases today, a printed user's manual is not included with the software; in many cases, it is included as a CD or is on-line. For my own personal computer, purchased with the Windows 98 software already installed, finding the warranty proved to be a task of several hours. I finally located it somewhere in the Microsoft data files that accompanied the software after searching those files for hours; no index or link was prominently displayed to guide me to it. However, the End User License Agreement (EULA) detailing the restrictions of the consumer's use of the software is imminently prominent and cannot be missed.

[247] The software that controls access and authorizes actions (the software that should be the most secure since that is what permits an user access to and manipulates the data).

[248] A fault in Microsoft's NT utility program when issued could be used by a remote user to unscramble encrypted information, including the entire registry of user passwords and display it as plain text. The revelation makes both the NT utility program and anything using Microsoft networking vulnerable to unauthorized user attacks. The potential intruder could access the password file either with a "sniffer" program or with a Trojan horse program designed to extract the file. A software code available on many "hacking" bulletins allowed potential intruders to "break the hashing algorithm via a reverse-engineering technique," then dump out the password database and run a "dictionary attack" (See footnote 407 for an explanation of "dictionary attack") against it. In this particular case, it was extremely easy to develop the code to reverse-engineer the hashing algorithm because Microsoft did not use "salt" data that avoids duplicate passwords. NT instead used a very simple password-hashing algorithm (Larry Lange, "More Microsoft Security Woes," TechWeb News, March 28, 1997, http://www.techweb.com, 1-5).

Faults or defects in proprietary software comprising security functions are not exclusive to only Microsoft. Cisco also discovered that its Internetwork Operating System (IOS) contained an error that breached the security of most of its router products. An unauthorized entry could cause Cisco networking devices running IOS to crash and reload without having to log in to the router providing a potential intruder open access to networked systems (Kimberly Caisse, "Cisco Software Bug Exposes Routers to Hackers," TechWeb News, August 24, 1998, http://www.techweb.com/wire/story/TWB19980824S0010, 1-3).

[248] Leonard Lee, 258; Landwehr, et.al., 224; and Laprie, et.al., "Validation of Ultra-High Dependability for Software-based Systems" in Randell, Laprie, Kopetz, and Littlewood, 481.

In trying to develop a seamless software integration of a simple client/server database application a team at PC Week found that although all of the individual parts worked correctly separately and when put together, the resulting function did not integrate smoothly and took too long to be practical. The new application was to use an X86 server running Windows NT using Oracle as the database server with a new piece of custom software as the front end. Unfortunately, when the new piece of software was implemented each insertion request for a database transfer took at least 7 seconds or more to complete (much too long for the number of databases to be transferred). The culprit was turned out to be the way the insertion procedure verified that each new record was unique. Instead of checking the name index that the database developer had created, Oracle had to search every existing record to verify uniqueness. Once located, a workaround was developed so the system worked as envisioned (Mark L. Van Name and Bill Catchings. "Seamless Doesn't Always Mean Smooth." PC Week 14, no. 50 (December 1, 1997).

adequately anticipate during development, particularly with a novel design.[249] The unanticipated situation then causes the computer either to shut down, produce an erroneous result, or otherwise not perform satisfactorily. Even the tiniest error can have an enormous effect; a simple typographical error can ruin an entire program,[250] and software is rapidly growing in complexity beyond its ability to be properly tested.[251]

Software designers must try to abstract all the real-world factors that could ever matter and to capture accurately how they matter; all the paths that can ever be executed; every situation anticipated; every contingency planned for, while ensuring both the pace and order in which instructions are executed are correct.[252] Such an abstract model is difficult to construct since designers nearly always must rely on highly indirect measures to anticipate what happens when programs execute and nature cannot be relied on to eliminate the physically absurd since software is not constrained by physical laws.[253] To make the task even more difficult, the designer has to anticipate and constrain unwanted behavior that accompanies any intended activity. This complexity is so great that the absence of design

[249] Leonard Lee, 258; Landwehr, et.al., 224; and Laprie, et.al., "Validation of Ultra-High Dependability for Software-based Systems" in Randell, Laprie, Kopetz, and Littlewood, 481.

[250] On July 22, 1962, NASA destroyed the Mariner 1 space probe before it could endanger populated areas because of a missing hyphen in one of its software programs (Leonard Lee, 103-104).

[251] Wiener, 8.

The use of embedded microprocessor cores in system-on-a-chip designs aptly illustrates the task faced by testers in coping with increased complexity and sophistication. SOC designs increase the challenges of effectively emulating and debugging on-chip hardware and software in a real environment once the silicon is available. Embedded CPU cores become increasingly more complex as they attain higher performance (Walter Bacharowski, "EJTAG Port Can Simplify Prototyping," Electronic Engineering Times, no. 992, February 9, 1998).

For example, embedded systems are built into systems or machinery that are intended to control or to substitute for humans in a hostile environment, e.g., on-board satellite control, production process control in a chemical plant. The embedded system is often subject to stringent space, weight, and/or cost requirements. It is thus specifically tailored to be small so that as many of the system resources as possible are available for the application and to provide only the most essential functions for timely execution of hard real-time tasks, task interaction, synchronization, and interaction with the environment (Werner Shutz, "Testing Distributed Real-Time Systems: An Overview" in Randell, Laprie, Kopetz, and Littlewood, 291).

[252] Wiener, 33 and 64-65.

[253] Wiener, 64.

faults simply cannot be postulated, generally at the expense of conventional reliability unfortunately.[254] One missed situation, whether from an omission or mistake, presents the possibility of an unanticipated effect.

This inherent underlying algorithmic complexity is amplified, all too often, by poor implementation resulting in a computer program of considerably greater actual complexity than the base algorithms themselves. However, the difference between this algorithmic complexity and the resulting program could be minimized by close attention to the algorithm during design of the program. Both types of complexity (algorithmic and programmatic) will affect the maintenance costs of software throughout its life cycle so minimizing either or both as much as possible is beneficial.[255]

Past experience indicates that the difficulties in building software increase with the size of the system, with the number of independently modifiable subsystems, and with the number of interfaces between them. As computer programs become larger, they grow in complexity at a rate greater than their growth in size. For example, a single tiny section removed from one computer program taking up a mere ten lines of code may hypothetically have three possible outcomes. Put two of those small sections together to form a slightly larger program, and the number of possible outcomes triples to nine. By the time you get to six sections, the number of possible outcomes grows to 756; sixteen small sections together,

[254] Wiener, 64

"Each time a program is run, different answers can appear -even with identical inputs" (Wiener, 59).

[255] Wiener, 86.

more than forty million.[256] Each increment of added complexity increases the difficulty of changing a part of the system without affecting many other parts.

Additionally, the more situations to which a software system is exposed, the more flexible it must be. The more flexible a system becomes, the more complexity the designers must master and encode in a logical structure, and the greater the number of errors that can be expected in it.[257] In a concurrent software system, each thread could be accessing different data at any given moment, or executing different instructions.[258] Parallel processing, on the other hand, uses two software programs at the same time to execute the same task. Problems arise in load-balancing and dependencies within the task while dividing the work. Consequently, parallel processing is often nondeterministic; given the same inputs, the same program can nevertheless behave as it never has before or events can occur in a different sequence. Results are therefore unpredictable.[259] Problems further worsen when the interfaces themselves can change, modifications make the software even more complex, the software has evolved from older legacy systems, or it incorporates code from many sources written by many different authors.[260] (Problems associated with each of these conditions will be further explained later in this chapter).

At the same time, software is also a component of the real-world physical network. And, the real world presents an infinite set of unique situations from user inputs; from the

[256] Leonard Lee, 100.

[257] Wiener, 59-61 and Kopetz, 22, 25, and 100.

[258] Wiener, 58-59.

[259] Wiener, 59-61; Lee, 3; and R. M. Suresh babu, B.B. Biswas, and G. Govindarajan, "Developing Highly Reliable Software," IEEE Micro 17, no. 5 (September/October 1997), 59.

[260] Wiener, xi-xii, 3, and 47 and Pipkin, xi-xii.

naturally noisy, busy, messy, physical environment; and from other distributed system[261] components to which it is connected.[262] User inputs can be wrong, too fast, too slow, too forceful, or not forceful enough; people are unreliable, make mistakes, change their minds, get impatient, or can be mischievous, hostile, or criminal. I users, especially, do things that designers do not anticipate; even experienced users can be absentminded. Too much noise, dust, heat, cold, humidity, dryness, or electromagnetic radiation from the environment can also affect how a software system functions at times. Since connected software, in many cases, provides data to initiate or sustain operation, other components can transfer their inherent defects and faults, faulty inputs, or the effects from malfunctions to the software to which they are connected.[263]

Time, likewise, can cause problems. Although the user sees only one path through the system, the system may actually be executing many paths concurrently, even if only some of the software is executing. This provides for many different potential states of the system. Each of these conditions can affect how software functions, at times producing effects not originally anticipated or for which programmed.

[261] Distributed systems are characterized by the existence of several loci of control (processors, nodes) that are interconnected by a network. Each node is a self-contained computer, consisting of a CPU, local memory, access to the network, a local clock, and other (optional) peripheral devices. Each node executes a set of parallel processes concurrently with the other nodes with all of the concurrent problems previously discussed for parallel processing. Processors (or processes) may communicate or synchronize themselves by messages in order to achieve their common mission. This requirement for interaction and synchronization provide additional opportunities for errors to occur or to be made (i.e., not only in each sequential process, but also in process interaction or synchronization). Finally, distributed systems tend to be larger in size than sequential ones (Shutz, "Testing Distributed Real-Time Systems: An Overview" in Randell, Laprie, Kopetz, and Littlewood, 285-287).

[262] Wiener, 36-47.

[263] Wiener, 49-50.

Software itself may be inherently unreliable, but the typical software development process is not apt to improve matters.[264] Software programs are still written the same way they were forty years ago in the dawn of the computer age. A small program can be written by one person, but large, complex programs can quickly become so large and unwieldy[265] no one person can understand the entire program. Large, complex programs have to be written by teams of programmers who somehow must share the common vision of what the program must do and how to achieve that goal.[266] These teams laboriously hack out perhaps six lines of code per person every hour. The average new business software program takes thirty-two thousand workdays to write requiring a team of thirty-six programmers almost three years to complete.[267] Then, as software becomes more complex, more sophisticated, and contains more integrated systemic functions, a fault's and/or defect's effect becomes ever riskier and more difficult to detect.[268]

Most software development organizations in the United States have not institutionalized the necessary software development practices to consistently produce reliable programs. This is not due to fraud, negligence, or incompetence, but is a result of market pressures, the structure of the development organization itself, and the software development process.[269] In a March 2001 Software Engineering Institute (SEI) Capability Maturity Model[270] assessment of 1380 organizations, 43.2 percent were still at level one of

[264] Mickey Williamson, "The Science of Software Development," CIO Magazine, April 15, 1996, 62 and Wiener, 69.
[265] The space shuttle holds over twenty-five million lines of code (Leonard Lee, 104) and, by now, many programs to control extremely sophisticated functions probably exceed the size of the space shuttle's program.
[266] Leonard Lee, 100 and Pipkin, xi-xii.
[267] Leonard Lee, 104 and 121.
[268] Leonard Lee, 3
[269] Wiener, 73.
[270] Theoretically, each maturity level in the CMM indicates the level of risk; the lower the maturity level,

the model (the ad hoc/chaotic Initial process). Only 4.3 percent reached level 4 (Managed process) and only 2.8 percent of the organizations assessed successfully advanced to level 5 (Optimizing process).

As dismal as these figures appear, there has been a tremendous improvement in the number of organizations exhibiting an orderly, managed process of software development over the 13 years SEI has been conducting the assessment. In the first assessment in 1987, 80 percent of the organizations were still at the Initial level 1, 1.4 percent were determined to be at the Managing level 4, and only 0.8 percent (one

the greater the risks to the software development processes. Improvement (or lowering the risks of inherent faults or defects) is accomplished by introducing, in sequential steps, techniques and methods such as configuration management, project management, explicit process definition, quality control, and product evaluation (Marian Myerson, Risk Management Processes for Software Engineering Models, Boston: Artech House, 1996, 102).

THE BASIC STRUCTURE OF THE CARNEGIE-MELLON CMM FOR SOFTWARE

Level	Characteristic	Key Challenge
5 (Optimizing)	Improvement fed back into the process	Still human intensive Maintenance of optimization
4 (Managed)	(Quantitative) Measured process	Changing technology Problem analysis Problem prevention
3 (Defined)	(Qualitative) Process defined & institutionalized	Process measurement Process analysis Quantitative quality plans
2 (Repeatable)	(Intuitive) Process dependent on individuals	Training Technical practices Process focus
1 (Initial)	(Ad hoc/chaotic)	Project management Project planning Configuration management Software quality assurance

(Les Hatton, Safer C: Developing Software for High-integrity and Safety-critical Systems, London: McGraw-Hill Book Company, 1995, 20).

organization) was at the Optimizing level. As encouraging as the 2000 Update data seem though, it also found that an improvement in management levels takes an average of about 24 months. The 596 organizations at the Initial level 1 stage in 2000 (43.2% of 1380 organizations) will take six years to reach the level 4 Managed stage although any increase in levels will be an improvement in these level 1 organizations' software development process.[271]

In too many instances, the rush to get the product to the market quickly through this hurried, ad hoc if not chaotic, software development process is responsible for many of the defects in the software.[272] Market pressures on software development are extreme; "The need to adapt to market changes is so great that time-sensitivity outweighs cost-sensitivity....." Many software companies are more interested in making a quick profit and managers are pressured to trim budgets and schedules to meet unrealistic targets.[273] These pressures can manifest themselves through inadvertent defects because of the rush to complete the project.

Further exacerbating the pressures on software developers, hardware technologies are now evolving faster than newer software engineering models and countermeasures needed to protect assets from adverse threats.[274] Software developers scramble madly to

[271] Carnegie Mellon University, Process Maturity Profile of the Software Community 2000 Year End Update, Software Engineering Institute, March 2001, http://www.sei.cmu.edu/sema/pdf/2001mar.pdf.
[272] Mickey Williamson, 65.
[273] Wiener, 73-74 and Siedsma.

"The goal is to embed information security in the corporate culture..., but whenever tradeoffs arise, the bias is towards speed not safety (or security (added by author)). The challenge for the IT sector and its customers is to provide security at the speed of business" (Kanoun and Laprie, "Software Reliability Trend Analyses: From Theoretical to Practical Considerations" in Randell, Laprie, Kopetz, and Littlewood, 4).
[274] Myerson, 4 and 14

"Computer power has increased from the days of the VAX-11/780 with its 1 MIPS (million take advantage of the latest technological advance (such as client/server improvements) even though each advance tends to increase the risk and the likelihood of a new cycle of faults, defects, market pressures, and further technical advances in hardware. As a consequence, many companies, both new and established, routinely underestimate how long or how difficult developing new reliable software is.[275]

Also, because the pace of change is so fast, new products are continuously being offered to the market but not all consumers opt to buy the new products. Therefore, at any given time a mix of old (legacy) and new technology makes up the information infrastructure system. Generally, network software has originated from a number of sources with differences in networking and management utilities. Many computer vendors started with proprietary operating systems and expanded them into networking software before standards were available. As these vendors moved into open network architecture systems, proprietary protocols that generally granted greater permissions with less authentication than current protocols were used to allow connectivity.[276] The vulnerabilities of the old technology are generally well understood and can serve as a gateway to the new technology if the new has not specifically been structured to preclude such a vulnerability[277] (which is difficult for all of the software-related conceptual reasons discussed earlier).

instructions per second) processing power, to 1Ghz (gigahertz) Pentium III processors, an increase of over 800% (Vibert). Comparatively, software efficiency is growing at a comparative crawl: just four percent a year. Computers have also improved a thousand times in the last twenty years while the improvements in software productivity has been merely ten times" (Leonard Lee, 264).

[275] Brown, et.al., 19.

[276] Pipkin, 104.

[277] Dr. Tom Longstaff, senior member of the technical staff in the Networked Systems Survivability (NSS) Program at the Software Engineering Institute (SEI), Dissertation Committee Overview Meeting, University of Pittsburgh, Pittsburgh, PA., February 1, 1999, suggested that this issue was a source of

The case of Kevin Poulson (See Appendix A) dispels the market model of letting technological advances remedy vulnerabilities because even though the advances may correct the vulnerabilities of older components, some old technology with its known vulnerabilities will still be in use. Exploiting those known vulnerabilities will still allow an intruder to manipulate the system. Poulson himself wrote to Judge Manuel L. Real prior to his sentencing in the Southern California Federal court case (CR 93-376R) that he found

> "the network to be a complex, fractal landscape: intricate and diverse.... One segment of the network might run off the latest in high-speed digital computers, while another runs on antique electro-mechanical equipment that predates the invention of the transistor."[278]

One-way software developers try to overcome the pace of hardware development is through "cosimulation and coverification," or developing new hardware and the software to operate on it concurrently. Cosimulated development utilizes a virtual CPU environment to simulate the functioning of the developing hardware so programmers can develop software to operate on the new hardware. This technique seems to work well for peripheral device-driver development. Coverification links software to a hardware simulator by taking advantage of C hooks provided in many HDL simulators.[279]

defects not widely publicized or acknowledged.

Microsoft made an intruder's password cracking task easier by making Windows NT compatible with earlier Microsoft products, including LANMAN from the 1980s. LANMAN's passwords were only seven characters (all in the upper case) for a total of only eight billion possible passwords. With today's PCs, an intruder can guess all of the eight billion in a matter of days (Doug Thomas, "Why Hackers Hate Microsoft," Online Journalism Review, Annenberg School for Communication, University of Southern California, April 29, 1998, http://www.ojr.org/ojr/technology/1017969479.php).

[278] Kevin L. Poulson, Letter to the Honorable Manuel L. Real, United States District Judge, Los Angeles, CA., Re: United States v. Kevin Poulson, CR 93-276R, February 9, 1995.

[279] Ron Pluth and Taimur Aslam, "Cosimulation Targets Early Integration," Electronic Engineering Times, no. 1013 (June 22, 1998) and "At Nortel, Coverification Is an Ongoing Effort," Electronic Engineering Times, no. 989 (January 19, 1998).

Another technique for speeding the process is to use already existing code in a new program.[280] In theory, this process is simple: copy the program onto the new machine, change a few well-insulated places that depend on specific aspects of the machine, compile it, and run it. In practice, such practice is never quite so straightforward. People typically link pieces of software together by putting the pieces on the same network or by grouping then on a single computer system, stitched together by means of system application programmer interfaces, network protocols, or dynamic libraries. The trouble is that these component boundaries can be weak and threaten an entire system through cascading effects by a failure in just one element.[281]

Still another variation to speed up the development process described above is use of "commercial off the shelf" (COTS) components. This process of developing systems through integration and reuse rather than customized design and coding is a cornerstone of modern software engineering, primarily for economic reasons. Today, practical, affordable IT systems are almost never 100% custom-built, but rather are constructed from a variety of commonly available commercial components. Unfortunately, these commercially

[280] Using code from existing or different sources is sometimes called "component-based development (CBD)." It is thought of as "bits" of software that can be replicated and, often with only minor modifications, assembled repeatedly to form any number of applications. An example of CBD without change is the user-interface component (Yes/No/Cancel dialog box of general utility interfaces). A drop-down list is an example of CBD that requires minor modifications in only the new list of available choices each time it is reused. Use of a word processor, a spreadsheet, and an e-mail program in a larger application is another example of CBD which is more complicated because it requires modification of the larger application to accommodate these reusable resources, especially if they are from different vendors (Miryam Williamson, "Special Report: Software Reuse – Technology," CIO Magazine, March 1, 1997).

A similar process is called "porting." A program is fully portable if it can be taken from one machine, compiled without change on another machine and run without any change in the output. Portability becomes increasingly significant as the growth of open systems continues to expand networks (Hatton, 75).

Another version of CBD is "system-on-a-chip" (SOC) design. With SOC design, engineering teams use verified "virtual components," or existing large functional blocks consisting of both hardware and/or software, to produce complex system chips and chip sets [Frank Schirrmeister and Timothy Rhodes, "Felix Ties System Behavior, Architecture," Electronic Engineering Times, no. 1013 (June 22, 1998)].

[281] Adams; and Wiener, 75-76.

available components contain errors and defects for the reasons discussed previously in the chapter and are, therefore, transported to any new program in which they are used. Adding to this unfortunate situation, most acquiring organizations lack access to the "artifacts of the software engineering process" used to create the COTS components. Even if the customer were interested in assuring the security of the system being created, it would be hamstrung since "analysis of engineering artifacts is the traditional means for verifying custom-built systems."[282] These transported errors and defects can often cause failure of system operations from both inadvertent, unintended interactions[283] and from purposeful intrusions.

When systems are built using the off the shelf components, they become vulnerable to attack strategies based on the known vulnerabilities. With COTS components in the public domain, their internal structures are widely known and available for analysis making it easier to discover their vulnerabilities. Popular commercial and public-domain components, therefore, offer potential intruders a ubiquitous set of targets with well-known and typically unvarying internal structures making successful penetration even easier. The lack of variability among components translates into a lack of variability among systems

[282] Robert Ellison, et.al., Foundations of Survivable Systems Engineering, 2 and 3.

[283] The USS *Yorktown*, one of the Navy's new "Smart Ships," suffered a widespread system failure off the coast of Virginia in September 1997 after a crewmember mistakenly entered a zero into the data field of an application. The computer system proceeded to divide another quantity by that zero. The operation caused a buffer overflow and the error eventually shut down the ship's propulsion system. The *Yorktown* was dead in the water for more than two hours. Experts differed on the cause of the failure. One explanation of the failure was that the mistakenly entered zero triggered a commonly known defect of the Microsoft Windows NT deployed on the ship.

Other experts argued that custom designed applications operating on the Windows NT system instead of a production version of a custom designed operating system for which the applications were designed caused the failure. Regardless of the exact cause, the result is illustrative of the problems of integration whether of commercial off-the-shelf components or customized software with commercial off-the-shelf components ("Rough Sailing for Smart Ships," Scientific American 279, no. 5 (November 1998), 46). The incident also illustrates Perrow's notion of interactive complexity and system accidents.

and creates vulnerabilities common to all potentially allowing a single attack strategy to have a wide-ranging and devastating impact.[284]

As if all of this was not enough, it's difficult to control costs. The main budget item for a software development project is educated, trained, well-paid professional brainpower of which there is a shortage.[285] And, the final insult, once the product is complete and copies sold, it is very easy to make copies of it without paying for the product. The result is that no one ever wants to pay what it costs nor wait as long as it takes to develop a piece of software.[286]

As a consequence of all these pressures, the project is likely to be behind schedule, over budget, and not quite what was originally planned. As successive project deadlines are missed, anything that appears to work is considered acceptable, regardless of quality.[287] Under these circumstances, the usual victim of a slip in project delivery is rigorous, thorough testing.[288]

Ideally, testing should catch the errors created during development. Testing software thoroughly is simple, but impossible.[289] Because of the discrete nature of computer memory and processing, the difference of a single input bit out of thousands may be all that separates an input combination that runs successfully from one that does not.[290]

In practice, testing is never complete as it is not possible to exercise a piece of software with each possible data item from the input domain. You must determine all

[284] Ellison, et.al., "Survivability: Protecting Your Critical Systems."
[285] Wiener, 76.
[286] Wiener, 73.
[287] Wiener, 75-76.
[288] Brown, et.al., 19.
[289] Musa and Ackerman, 19.
[290] Musa and Ackerman, 19.

possible inputs and for each input test all possible sequences of instructions correcting each fault as you find it. The subsequent rewritten program has changed the software, thereby invalidating all previous test results. The complete testing cycle, then, must be begun again.[291] Each successive cycle has a lower failure rate thus taking longer for faults and/or defects to appear.[292] You continue this process for somewhere between forty and forty thousand years, depending on the size of the systems, how much help you can afford, and how reliable you want the program to be,[293] and this is only for single faults.

When the focus of testing is fault removal, the question of how to select a test input set well-suited for revealing real, but unknown, faults is difficult to answer.[294] Most current test input generation is deterministic: input test sets are built by selecting one element from each subdomain to be tested. Unfortunately, exercising only once each subdomain defined is far from being enough to ensure that the corresponding test set will expose faults, since a real limitation is imperfect correlation of test criteria with faults.[295] Probabilistic generation of test data using structural or functional criteria with the proper definition of an appropriate probability distribution over the input domain could better serve to define an input profile

[291] Retesting a program after errors have been corrected or after the software has been changed due to enhancements, optimizations, or for other reasons is called regression testing. It is intended to ensure that

1. errors have been truly corrected, and/or
2. modifications did not introduce new, undesired effects or errors (Shutz, "Testing Distributed Real-Time Systems: An Overview" in Randell, Laprie, Kopetz, and Littlewood, 288).

[292] Kopetz, 9 and Wiener, 98, 103-104 and 106.

[293] Musa and Ackerman, 19.

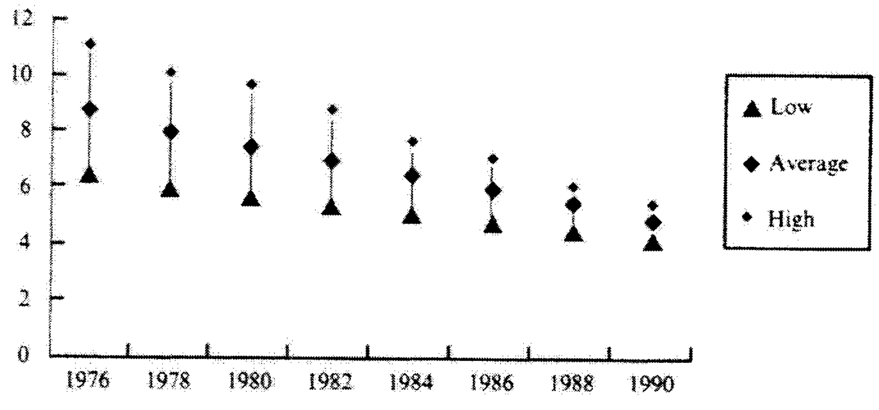
Given a common industry average of one error for every thousand lines of code, a software program of one million lines of code would contain one thousand errors. If testing were to correct ninety percent, that would still leave one hundred errors in the program (Leonard Lee, 102-103). And, remember the space shuttle has over 25 million lines of code!

[294] It is difficult to model the effects of computer failure on complex environments, plus there may be no explicit statement of desirable levels of risk (Laprie, et.al., "Validation of Ultra-High Dependability for Software-based Systems" in Randell, Laprie, Kopetz, and Littlewood, 489).

[295] Bruno Marre, Pascale Thevenod-Fosse, Helene Waeselynck, Pascale Le Gall, and Yves Crouzet, "An Experimental Evaluation of Formal Testing and Statistical Testing" in Randell, Laprie, Kopetz, and Littlewood, 273 and 276.

and a test size for reliable testing,[296] but such a process is generally much longer and more costly than the developers are willing to accept.

NASA's efforts over the last 20-some years are illustrative of the problems intrinsic to eliminating software errors. NASA's efforts only slowly paid dividends as reported by a study conducted by the University of Maryland's Software Engineering Laboratory of 80 ground-based space mission tracking software projects at NASA's Goddard Space Center. As can be seen by the figure below, the average number of software errors per year has declined from ~ nine at the beginning of the study to less than six per year at the end of the study.



Errors per 1000 lines at NASA Goddard 1973-1990 297

Figure 3.1. NASA Efforts to Eliminate Software Errors

Most of the improvement came from improving the errors that occur at a really high rate (from about 11 per year at the beginning of the study to a little more than six per year at the end of the study) rather than those that occur at a low rate (from a little more than six

[296] Pascale Thevenod-Fosse, Helene Waeselynck, and Yves Crouzet, "Software Statistical Testing" in Randell, Laprie, Kopetz, and Littlewood, 253 and 239.
[297] Hatton, 3.

per year at the beginning of the study to a little more than four per year at the end of the study). These results verify the conceptual software failure process model: a program starts life with a finite number of faults, and these are encountered in a purely unpredictable fashion. Different faults contribute differently to the overall unreliability of the program: some affect the reliability of the program more than others, i.e., they would show themselves (if not removed) at a greater rate. Thus different faults have different rates of occurrence.

If faults are "fixed" at each failure and each fix attempt is successful, then as debugging progresses a fault with a larger rate will tend to show itself before a fault with a smaller rate. Large faults will get removed earlier than small ones that will lead to the law of diminishing returns. As debugging progresses and the program becomes more reliable, it becomes harder to find faults (because the rate at which the program is failing is becoming smaller), and the improvements to the reliability resulting from these fault-removals are also becoming smaller and smaller. E.N. Adams demonstrated that about one third of the faults only caused errors at the rate of about once every 5000 years of execution.[298]I

With such a diminishing rate of returns, errors in the above example for NASA should be pretty rare by about 2050. It is a sobering thought that the progress is so slow, even with NASA's resources and experience. The reader is referred to Keller, TW. "Achieving error-free man-rated software" in 2nd International Software Testing, Analysis,

[298]"Optimizing Preventive Service of Software Products," IBM Journal of Research and Development, 28 (1), 2-14, January 1984 in Laprie, et.al., "Validation of Ultra-High Dependability for Software-based Systems" in Randell, Laprie, Kopetz, and Littlewood, 478.

Another investigation showed that over 30 percent of all faults reported for a particular widely used operating system caused a failure on average of only once every 5000 years of system operation (Wiener, 98 and 106).

and Review Conference. Monterey. CA. 1993 for an excellent account of the extraordinary efforts NASA shuttle engineers employed to eliminate error and risk.[299]

To develop highly reliable software, one must test for multiple faults since they cause most serious failures. To test for multiple faults, one first identifies all the single faults that can take place, and what their effects on the system could be. Then one considers what would happen if any two of those faults occur at the same time. Then three simultaneous faults are considered and so on until all possibilities are exhausted – the more complex the software system, the more the number of possible situations proliferates.[300] And consistent with the preceding discussion, one must begin the process anew upon correction of each different set of multiple faults or defects or the discovery of any new faults or defects. Even for small simple systems, the number of such sequences is enormous; as a system increases in size and complexity, testing becomes more complex and more costly.[301] Testing typically consumes in the order of 50% of the total project costs.[302]

Even such thorough testing as just described does not guarantee complete removal of all defects.[303] Software testing traditionally is based on the paradigm of "penetrate and patch." Additional defects always seem to appear because:

- the fix introduces new defects;

[299] Hatton, 3

[300] Wiener, 128.

[301] Wiener, 4 and 96-97.

[302] Shutz, "Testing Distributed Real-Time Systems: An Overview" in Randell, Laprie, Kopetz, and Littlewood, 284.

[303] Landwehr,et.al., 213.

- identified defects cannot be repaired because system operations depend on their original configuration;
- dependency between defects may mask other defects;
- defects that have already been corrected can possibly get reintroduced because of a lack of version control and configuration management, especially in those organizations at lower levels of the Carnegie-Mellon CMM (which still comprise the overwhelming majority of software development organizations);[304]
- of variation in the testing effort during debugging;
- of change in test sets;
- addition of new users during operational life; and
- a host of other changes in the software's environment can cause defects to escape detection.[305]

Then the process of removing faults or defects can also leave detritus. In an effort to track down a fault, programmers will frequently insert instructions to make events inside the program more apparent. These instructions can themselves cause serious problems if not removed before the system is placed into operation.[306]

Finding the cause of a fault or error is at least as hard as fixing it. A fault or error is often the result of such a precise, subtle set of interactions that it is difficult or impossible to

[304] Mickey Williamson, 65 and 69.

[305] Kanoun and Laprie, "Software Reliability Trend Analyses: From Theoretical to Practical Considerations" in Randell, Laprie, Kopetz, and Littlewood, 374.

[306] During the first lunar landing on July 20, 1969, Neil Armstrong was distracted in the final critical seconds before landing by two computer alarms that were left in the code by software engineers eliminating problems with the original Apollo 11 software. Although the alarms were initially indicators of malfunctions in the system, they no longer were accurate indicators of any problem with the Apollo system. The situation was eventually overridden by human decision-making (Wiener, 7 and 9).

replicate. Theoretically, information about either is available from reading the program itself. Such information would allow the testers to use the specification to define test criteria in a formal framework. For each property expressed by a formula of the specification, test data would be selected from strategies derived from hypotheses chosen by the tester. This strategy permits tests to determine whether all the properties specified in the specification are actually processed by the program.[307]

However, most commercial programs are sparsely documented, if at all (even though complete documentation should be the norm), so little help is available there. Pragmatically, even if the documentation can be found it can be exhausting to read more than a few pages of code that you yourself have not written recently; other people's code can be impenetrable. [308]

Too often developers wait until software is nearly complete before bringing humans into the testing process. People can spot errors in logic and misunderstandings of requirements that a computer is likely to miss. The person most likely to grasp what is happening is the person who wrote the program, but, unfortunately, they are the least likely to be still working with the software being tested for two reasons: prestige and job mobility.[309] Software maintenance is an unglamorous job with few opportunities for advancement. Consequently, software production facilities often experience high personnel turnover rates.

[307] Marre, et.al., "An Experimental Evaluation of Formal Testing and Statistical Testing" in Randell, Laprie, Kopetz, and Littlewood, 274.
[308] Wiener, 101-103 and Landwehr, et.al., 219.
[309] Wiener, 104 and Landwehr, et.al., 223.

Programmers who perform well often wish to move from project to project because each move offers a promotion, a raise, or at least the opportunity for fresh challenges. Sometimes a member of the development team, knowing how valuable they are, becomes a consultant. As a consultant, the person is available to provide answers to questions about the program for a price, but, in many instances, commercial companies do not want to pay the price consultants demand for their services. Consequently, the person maintaining the program is often the most recently hired or someone just graduated from college.[310]

If no one is left who remembers how the system was designed, those assigned to maintain it respond to faults and/or defects with patches – inadequate local fixes and makeshift accommodations.[311] The error rate for a program maintained with patches initially decreases, reaches a minimum, and then begins to increase again as the modifications accumulate.[312] Each patch synergistically disturbs the system's structure making the next fault harder to find and fix as the system grows larger and less understood. Also, programmers cannot predict all of the effects a patch will have, and a patch that seemingly has no undesirable effects today promises nothing certain about the future. Under these circumstances, fixing a fault or adding a feature is quite likely to introduce another fault, if not several. Eventually, the program succumbs to the accumulated patches

[310] Wiener, 104.

[311] Kopetz, 106.

[312] Kopetz, 95 and Laprie, et.al., "The Transformation Approach to the Modelling and Evaluation of Reliability and Availability Growth" in Randell, Laprie, Kopetz, and Littlewood, 390-391.

Such reliability behavior is not restricted to the operational life of a system, but also applies to the development-validation phases of a system (e.g., during incremental development, or during system integration) (Laprie, et.al., "The Transformation Approach to the Modelling and Evaluation of Reliability and Availability Growth" in Randell, Laprie, Kopetz, and Littlewood, 390).

with erratic, unpredictable behavior. The only answer then is to throw out the entire system and start over again.[313]

Common-mode failures (a single defect that causes more than one of several supposedly independent components to fail) pose an even more difficult problem. They are less common than multiple failures (the process just described), but are the worst case. They require an analyst to consider unintended connections and unplanned interactions to find the fault or error and its effects.[314]

One classic way to guard against common-mode failure is to use diversified design, i.e., the production of two or more variants of a system or equipment intended to fulfill the same implementation function through different technologies, such as:

- recovery blocks,[315]
- N-version programming,[316]
- N self-checking programming,[317]

[313] Wiener, 106 and Kopetz, 95-96.

[314] Wiener, 127.

[315] In the recovery blocks (RB) approach, variants are named as alternates and the main part of the adjudicator is an acceptance test that is applied sequentially to the results produced by variants. The variants are organized in RB in a manner similar to the standby sparing techniques (dynamic redundancy) used in hardware, and may be executed serially on a single processor. The execution time of a recovery block is normally that of the first variant, acceptance test, and the operations required to establish and discard a checkpoint. RB is highly efficient since this will not impose a high run-time overhead unless an error is detected and backward recovery required or if the test is complex. Limitations of the RB method are primarily related to its acceptance test that is usually derived from the semantics of a given application. Close dependency between the test and variants may impact reliability of the whole system (Jie Xu, Andrea Bondavalli, and Felicita Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in Randell, Laprie, Kopetz, and Littlewood, 157).

[316] N-version programming (NVP) is a direct application of the hardware N-modular redundancy approach (NMR) to software. A voting mechanism determines a single adjudication result from a set or sub-set of all the results of variants (Xu, Bondavalli, and Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in Randell, Laprie, Kopetz, and Littlewood, 156).

[317] N-self-checking programming (NSC) provides fault tolerance through parallel execution of N self-checking components. Each self-checking component is constructed from a pair of variants plus a result comparator (or from a variant associated with an acceptance test). One of them is regarded as the active component, and the others as "hot" standby spares. Upon failure of the active component, service delivery is switched to a "hot"

- t/(n-1)-variant programming,[318] and
- some intermediate or combined techniques.

Each of the diversified designs requires a decider (or adjudicator)[319] to switch system functions from a defective process to a non-defective one thereby providing reliable computing, not the complete absence of design faults but only no similar errors in variants.[320]

The systems architecture in diversified design is also based on the federation of components each implementing one or several subfunctions of the system. This federated approach generally leads to a very large number of processing elements, larger than what

spare (Xu, Bondavalli, and Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in Randell, Laprie, Kopetz, and Littlewood, 157).

[318] The t/(n-1)-variant programming scheme is based on the system diagnosis technique developed for hardware. This approach uses the t/(n-1) diagnosability measure to isolate the faulty variants within a set of (n-1) variants. By applying the diagnosis algorithm to results produced by variants, a result is selected that has the highest probability of being correct as the system output (Xu, Bondavalli, and Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in Randell, Laprie, Kopetz, and Littlewood, 157).

[319] Adjudicators are usually based on a combination of majority voting (in one of many forms possible) and self-checking by the design replicas (acceptance tests). One technique for adding an adjudicator is to include replicated hardware and/or software components. A modular-redundant component is substituted instead of an ordinary component consisting of a set of sub-components (called replicas), each one implementing the same function as the whole component, plus some mechanism that obtains a single result (the adjudged output) from the set of results produced by the replicas (replica outputs) to be used as the output of the replicated component (Xu, Bondavalli, and Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in Randell, Laprie, Kopetz, and Littlewood, 141).

[320] Jean-Claude Laprie, Jean Arlat, Christian Beounes, and Karama Kanoun, "Definition and Analysis of Hardware-and-Software Fault-Tolerant Architectures" in Randell, Laprie, Kopetz, and Littlewood, 104 and Xu, Bondavalli, and Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in Randell, Laprie, Kopetz, and Littlewood, 155-156.

The computer-controlled part of the flight control systems of the Airbus A-300 and A-310 and the Swedish railways' interlocking system are based on the parallel execution of two variants whose results are compared, and they stop operation upon error detection. The flight control system of the Airbus A-320 is based on two self-checking components, each of them being in turn based on the parallel execution of two variants whose results are compared; tolerance to a single fault needs four variants (Laprie, et.al., "Definition and Analysis of Hardware-and-Software Fault-Tolerant Architectures" in Randell, Laprie, Kopetz, and Littlewood, 105).

The space shuttle uses four identical computers using identical software programming to operate all critical flight operations. Each time a decision is needed, the computers vote. If one of the computers disagrees or has a fault, the other computers vote to ignore it. If two or more computers fail, control of the shuttle is handed over to a fifth "standby" computer that uses a completely separate set of software commands (Leonard Lee, 105).

would be necessary in terms of the computing power required, e.g., the Boeing 757/767 flight management control system is composed of 80 distinct functional microprocessors (300 when redundancy is accounted for). However, conceptually such a design for partitioning the system global function into subfunctions would confine a failure of any component and still permit the global function of the system to be performed, possibly in a degraded mode.[321]

However, there are two fundamental problems with design diversity:

- First, the cost of developing the variants and adjudicator may be many times more than that of programming a single version. Even with the high cost, design diversity still has some difficulties in ensuring a routine-based improvement in software reliability; and[322]
- Secondly, most of the methods for software fault tolerance are not particularly efficient,[323] still an important aspect of software quality. Since the applications that require software fault tolerance are often also likely to have stringent efficiency requirements good use of space[324] and time[325] is highly desirable. All fault tolerance approaches require some extra space or extra time, or both.[326]

[321] Examples of this approach may also be found in nuclear plant monitoring (e.g., the SPIN system of Merlin Gerin) (Laprie, et.al., "Definition and Analysis of Hardware-and-Software Fault-Tolerant Architectures" in Randell, Laprie, Kopetz, and Littlewood, 103-104).

[322] Xu, Bondavalli, and Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in Randell, Laprie, Kopetz, and Littlewood, 156.

[323] Efficiency is defined as the good use of system and hardware resources, such as processors, internal and external memories, and communications devices that result in economic savings and timely use of resources (Xu, Bondavalli, and Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in Randell, Laprie, Kopetz, and Littlewood, 156).

[324] Space is defined as the amount of hardware (e.g., the number of processors) needed to support parallel execution of multiple variants (Xu, Bondavalli, and Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in Randell, Laprie, Kopetz, and Littlewood, 157).

[325] Time is viewed as the physical time needed to execute one or more variants sequentially (Xu, Bondavalli, and Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in

Also, to be somewhat evenhanded towards software developers, new testing tools are continually being developed to keep up with and take advantage of advances in hardware/software integration, embedded systems development, and added security:

- JTAG (Joint Test Action Group), EJTAG, or on-chip debugging for rapid prototyping on MIPS-based processors. The on-chip debugging logic in the embedded CPU core includes the necessary logic for hardware breakpoints, debugging exceptions, memory and register display/modification, and program counter trace.[327]
- Cosimulation (discussed previously in this section). Utilizes a virtual CPU environment to simulate the functioning of the developing hardware thereby allowing programmers to develop software to operate on the new hardware [328]
- Coverification (discussed in previous section). Verifies the software and hardware of an embedded system at the same time. Generally, a translation and communications software package takes software instructions as its input and turns those variables into test vectors that are compatible for hardware description language (HDL) simulators.[329]
- Logic emulation. Emulates the logic of the software at less than full clock speed. Most of the new integration and testing techniques require either simulation or emulation of the hardware, software, or both that can lead to other problems. For software, simulation at full clock speed is important because many program-routine

Randell, Laprie, Kopetz, and Littlewood, 157).

[326] Xu, Bondavalli, and Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in Randell, Laprie, Kopetz, and Littlewood, 156.

[327] Bacharowski; and Goering.

[328] Pluth and Aslam; Cole; and Goering.

[329] "At Nortel, Coverification Is an Ongoing Effort"; Cole; Goering; and Berger.

executions depend on precise clock timing. But, simulations of the whole system with full accuracy and at the clock rate of the actual hardware take a lot of time and resources (simulators can contain 200,000 instructions per second while logic simulation of complex designs rarely exceeds 10 instructions per second). Developers will sometimes circumvent full simulation by reducing the clock rate at which the simulation is being modeled, by reducing the accuracy of the model since not all aspects of a system need the same timing accuracy, or by substituting an emulator providing the simulation conditions for the CPU on the simulation host thereby reducing the time and resources needed to execute the full simulation.[330]

- Fragmentation-Redundancy-Scattering (FRS). The aim of FRS is to tolerate both accidental and intentional faults by fragmenting a confidential object using its composition structure, i.e., a hierarchy of sub-objects each with its own subsidiary operation or "methods." The fragmentation process continues until the resulting sub-objects are individually non-confidential, i.e., no isolated fragment contains any significant information. Redundancy is added to the fragments (by replication or use of an error correcting code) in order to tolerate accidental or deliberate destruction or alteration of fragments. These replicas of non-confidential objects are then scattered in a redundant fashion across a distributed system, which more than likely contains both trusted and untrusted stations so that an intrusion into any part of the distributed system only gives access to unrelated fragments. A complete information item can only be re-assembled on trusted sites of the distributed system. By such means

[330] Cole; Goering; and "Mentor Graphics and IKOS Deliver Verification Environment to Accelerate Telecom and Datacom System Design."

much of the processing of object methods, as well as the storing of much object state information, can be carried out safely on untrusted equipment.[331]

Eventually a point of diminishing returns is reached. Testing software, then, becomes an exercise in trying to take out as many faults or errors as possible while acknowledging that all will never be found.[332] Recognizing the futility of the entire process, Peter Neumann says, "It is impossible to guarantee your system is going to be dependable. No matter how much testing you do, you're still going to have vulnerabilities."[333] Realistically, actual use finds more faults than any testing program ever does.[334] Users will exercise the software, both intentionally and unintentionally, much more rigorous and fully than any testing program ever will. Remaining in use for a long time is the only sure

[331] Fabre, Deswart, and Randell, "Designing Secure and Reliable Applications using Fragmentation-Redundancy-Scattering: an Object-Oriented Approach" in Randell, Laprie, Kopetz, and Littlewood, 173-174.

[332] Wiener, 8, 98 and 106.

"It is only possible to completely verify programs up to 2000 lines of code in length - beyond that it become very difficult." Neil Storey, secretary of the British Computer Society's specialist group on safety-related computer systems after British Nuclear Fuels found 2400 faults in software that would monitor and control its nuclear processing plant at Sellafield (Paul Marks, "Faults Highlight Problems of Nuclear Software," New Scientist 135, no. 1836 (August 29, 1992), 19).

The software that IBM (the only organization to achieve a level 5 (optimizing) on the Software Engineering Institute Capability Maturity Model) wrote for the space shuttle flight control system was supposed to be just about as good as it gets. That software cost about $1000 per line, while the industry average was between $25 and $100. It had undergone over two thousand hours of simulation testing and had uncovered more than two hundred errors before the first shuttle ever took off. The software was deemed "stable," meaning it performed its functions reliably enough to be used. But it was not perfect, either; based on bugs found on previous versions, IBM itself estimated that the released software contained about fifty bugs. On the first shuttle flight, twenty-four more errors were found, four of which were judged to be "critical" or "major" (Wiener, 124 and Leonard Lee, 103).

[333] Wiener, 98 and 106.

[334] Microsoft issued Service Pack 2 for its Windows 2000 on May 16, 2001, even though the operating system only debuted in early 2000 (Service Pack 1 was issued on July 31, 2000). (Service packs are conveniently bundled updates for system reliability, program compatibility, system administration tools, drivers, security, and other components. Service Pack2 for Windows 2000 specifically pertains to:

- operating system reliability,
- application compatibility,
- windows 2000 Setup,
- security issues, and
- includes 557 fixes for new faults and defects as well as the 279 fixes previously issued with Service Pack 1 (http://www.microsoft.com/technet/security, June 19, 2001).

way for software to attain high reliability, but faults still appear, at times suddenly causing some unanticipated, unintended result even in old heavily used software.[335]

As an added ignominy, information system developers generally do not use security failure or attack data to improve the security and survivability of systems that they develop. Most other disciplines' systems engineers design system architectures to survive known faults in building materials, construction methods, and the environment. Information

[335] Leonard Lee, 3 and 121.

Defects were found in a piece of the original COBOL language program after 20 years of use in the West Drayton air traffic control system.

Defects are also still being detected on the 25-year-old UNIX language. UNIX was developed under the assumption that security did not need to be addressed; that the operating environment was benign. What are today considered security "bugs" were deliberately placed in the code to make network operations more convenient when dealing with other trusted machines. The original documentation reputedly even contained instructions that detailed "how to bring UNIX to a halt...." (Landwehr, et.al., 230; Peter da Silva, "Re: 'UNIX' Worm/Virus," The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 71 (November 6, 1988), http://catless.ncl.ac.uk/Risks/7.71.html; and Brad Templeton, "Risks of Getting Opinions From Semi-Biased Sources," The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 71 (November 6, 1988), http://catless.ncl.ac.uk/Risks/7.71.html).

Entire organized efforts are devoted to listing and providing fixes for UNIX flaws, e.g., Internet/Network Security, http://netsecurity.about.com/compute/netsecurity/cs/unixsecurity/index.htm; Incomplete List of UNIX Vulnerabilities, http://www.cs.iastate.edu/~ghelmer/unixsecurity/unix_vuln.html; A Taxonomy of UNIX System and Network Vulnerabilities, http://citeseer.nj.nec.com/138786.html/; Douglas G. Conorich, "End-User Security in UNIX" in Ruthberg and Tipton; and UNIX Insider, http://www.itworld.com/Comp/2378/UnixInsider, as well as others. Classic software vulnerabilities of UNIX include:

1. path variable attacks that can take advantage of programs that use a relative path or no path. If an intruder has access to the read permission of binaries and scripts, he can execute those programs;
2. file name attacks initiated by creating a file whose name will be interpreted by the system as something else by embedding command delimiters into the file name;
3. vulnerabilities found in the UNIX sendmail function on an almost regular basis;
4. access to the system name, phone number, UNIX to UNIX Communication Protocol (UUCP) login name and passwords for other systems by using the "systems" file of the UUCP if not configured correctly. Even though most systems today use a point-to-point access protocol (SLIP or PPP), most systems still have the UUCP software loaded and enabled providing the potential intruder an open door into their system.
5. execution of the "L.cmds" and "USERFILE" file to obtain a list of commands that can be performed by the specified remote system and the directories to which the system has access, respectively;
6. browsing a system to locate the password file;
7. the ability to update a system's configurations remotely in a machine not properly configured (Pipkin, 31 and 60-61; Lange, 3; and Wiener, 105).

systems are still being built and managed today susceptible to the same or similar vulnerabilities that have plagued them for years.[336]

Finally, a classic security dilemma is that the more security added to a system, the less secure it sometimes becomes because those responsible for the security become too reliant on the added security measures and are not as vigilant as before.[337]

3.3. Systemic Structural Vulnerabilities.

The information infrastructure system (See Chapter 2. Information Infrastructure System), like all systems, is characterized by an aggregation of parts whose relations make them interdependent. The system is a set of components interacting under the control of a design (which is itself a component of the system). Clearly, the system model is recursive in that each component can itself be considered as a system in its own right and thus may have an internal design that can identify further sub-components.[338]

This does not mean, however, that all relations between the components are constant or the same. Norbert Wiener, the founder of cybernetics, notes that conceptually "organization must be considered as something in which there is an interdependence between the several organized parts but in which this interdependence has degrees."[339] Sometimes the interdependence is highly constrained and limited, or tightly coupled (e.g., in mechanistic systems), resulting in structural rigidity and determinant behavior, while in other instances, the connections among interacting parts may be relatively weak with less

[336] Ellison, et.al., Foundations for Survivable Systems Engineering, 8.

[337] Tom Longstaff, Senior Member of the Technical Staff in the Networked Systems Survivability (NSS) Program at the Software Engineering Institute (SEI), Carnegie Mellon University, Dissertation Committee Overview Meeting, Feb. 1, 1999.

[338] Xu, Bondavalli, and Di Giandomenico, "Dynamic Adjustment of Dependability and Efficiency in Fault-Tolerant Software" in Randell, Laprie, Kopetz, and Littlewood, 88.

[339] Norbert Wiener, I Am a Mathematician, New York: Doubleday, 1956, 322 in Scott, 77.

constraint placed on reactions of one element by the condition of the others, or loosely coupled (in organic systems), resulting in greater response flexibility.[340] This connectivity and type of coupling is a property of any system, but becomes even more critical as the system becomes more and more distributed, as the information infrastructure system seems to be evolving.[341]

The information infrastructure system as it now exists is a mechanistic system controlled by programs, or “any prearranged information that guides subsequent action,”[342] in this case, software. Such a system provides a standardized predetermined, predictable response to an external action.[343] Organizational concepts like the National and Global Information Infrastructure and software/software and software/hardware integration are attempts not only to increase efficiency and effectiveness but also to remove uncertainty from the system so outcomes can be predicted better.

One only has to look at the infrastructure system described in Chapter 2. Information Infrastructure System and the interconnectivity of the vulnerabilities described earlier in this chapter to find examples of tight and loose coupling and programmed actions in the information infrastructure system. The system is itself now more tightly than loosely

[340] There is an opportunity for human intervention to delay or stop the system's operations (Scott, 77 and 88).

[341] Wiener, 64.

The telephone switching system probably represents the most highly connected computer network in the world, and the most complex distributed system. One of these days, the phone system will reach the point where a problem in Tokyo will bring down the telephone system in Des Moines (Wiener, 64).

[342] James R. Beniger, The Control Revolution: Technological and Economic Origins of the Information Society, 39 in Scott, 79.

Programs control by determining decisions; the process of control involves comparison of new information (inputs) to stored patterns and instructions (programming) to decide among a predetermined set of contingent actions (possible outputs) (James R. Beniger, The Control Revolution: Technological and Economic Origins of the Information Society, 48 in Scott, 79).

[343] "A well-organized system is predictable - you know what it is going to do before it happens.... A perfectly organized system is completely predictable...." (George A. Miller, "What is Information Measurement," American Psychologist 8, 1953, 3-12 in Scott, 84).

coupled,[344] but examples of both relationships do exist. Most software is tightly coupled (especially when integrated with other software, e.g., consider shell software and its responses to actions) but password software is an example of loose coupling.[345] The challenge facing the information infrastructure system's designers is how to create structures that will overcome the limitations and exploit the strengths of the different types of coupling.[346]

One of the contentions of this research is that this increasingly greater software/software and software/hardware integration discussed in the previous section exacerbates the risks to the U.S. information infrastructure system and, therefore, to U.S. national security. Software developers and industry managers continually search for their Holy Grail: completely automated, or autonomous, systems – those with no human beings involved in their operations. By definition, to create such systems designers and developers must combine and integrate many separate functions to perform more complex functions.

Within man-made complex systems, these connections and interdependencies within and between a system(s) are likely to be tighter and greater than those between simpler or natural system components. Within the information infrastructure system, this implies that the interdependencies between the components of a computer system are more tightly coupled than the interdependencies between the computer system and other components of a network, or the information infrastructure system is more tightly coupled than its connection

[344] Lee Badger, a principal computer scientist with Trusted Information, reinforces this point; "General-purpose systems like Unix and Windows don't provide the controls for restricting and controlling interactions" between software components, and software components depend on data produced by other software. Consequently, there is tight coupling between the software components linked together with no or little opportunity for human intervention (Adams).
[345] In the password software case, humans not only have the opportunity to intervene, but that intervention is necessary to produce subsequent action.
[346] Scott, 88.

with other critical infrastructure systems.[347] I suspect the looser coupling between the information infrastructure system and other infrastructure systems is more a result of a lack of "progress" in this area than intent. I further suspect designers are attempting to tighten the coupling between the information infrastructure system and other critical infrastructures for greater predictability of the interactions between them (which will also theoretically increase efficiency and effectiveness of both systems).

There is no dispute that integration of computers and information systems makes rapid decisions possible thereby increasing the efficiency of the operation, but the rapidity with which actions can take place and the increasingly tight coupling[348] between and among them may prove to be destabilizing. Further, the new products add to the complexity of an already complex system even more and designers cannot assure the new products will do only what they are designed to do.[349]

The engineering solution for these potentially problematic integration conditions is often to provide for additional redundancy through diversified design – providing multiple and overlapping systems to monitor or control critical activities. But reliability in systems

[347] Scott, 85.

[348] Rochlin, 104.

[349] For example, Cisco Corp.'s Eudora e-mail software program was discovered to contain a flaw that could let even "relatively unsophisticated computer programmers foist viruses or other malicious programs on the software's users." Eudora's flaw is in its ability to read e-mail messages as if they were Web pages, letting its users embed active HTML links and live JavaScript applications inside a piece of mail. Someone intent on malicious activity can place an innocent-looking Web link inside a message that, if triggered, actually runs an attached program that has been hidden from the user's view (John Borland, "Trojan-Horse Security Flaw Found in Eudora," TechWeb News, August 7, 1998, http://www.techweb.com/wire/story/TWB19980807S0007, 1-3).

In January 1999, Microsoft's widely distributed Excel spreadsheet software was found to contain a fault that makes the program vulnerable to intrusion. Excel's CALL function that normally is used to divide Websites into sections known as frames can be manipulated to download code (a Trojan Horse) into a user's computer when visiting what appears to be an ordinary Website. The fault does not require that users take any more active steps to be vulnerable to an unauthorized user than visit a booby-trapped Website [David Clark and Joseph Pasquale, et.al., "Strategic Directions in Networks and Telecommunications," ACM Computing Surveys: ACM 50th Anniversary Issue: Strategic Directions in Computing Research 28, no. 4 (December 1996)].

depends not only on technical redundancy against possible equipment failures and human redundancy to guard against single-judgment errors, but also on that wonderfully scarce resource of slack – that sometimes small but always important excess margin of unconsumed resources and time through which an operator can buy a little breathing room to think about the decision that needs to be made, and in which the mental map can be adjusted and trimmed.[350]

However, in many cases human requirements such as slack, excess capacity, trial-and-error, and shift overlaps are often assumed to be wasteful; an inefficient use of resources to be engineered away. Of particular concern is the degree to which what is destroyed or discarded in the relentless pursuit of technical and operational efficiency is not waste or slop, but "slack." In the extreme case, those humans who are retained are increasingly put there to correct the outcome of the process if something incorrect happens or to reconstruct the automated system if it fails. Such a situation contributes to system collapse much more quickly in the case of extensive failure (Perrow's system accidents).[351]

Another important characteristic of exceedingly complex, probabilistic systems[352] is that the whole is more than the sum of its parts. The information network exhibits just such a property; it is built with independent application, transport, network, data link, and descending operational layers with the upper layers concealing the lowers ones from "view."[353] These "stacked" layers perform their functions without having to know or

[350] "Slack serves to provide the human and material buffering capacity that allows organizations and social systems to absorb unpredicted, and often, unpredictable, shocks" (Rochlin, 126-127).

[351] Rochlin, 127, 213.

[352] The most complex of Beer's classification of systems. See Stafford Beer, Cybernetics and Management, New York: John Wiley, 1964, for a discussion of his classification of systems based on complexity.

[353] Hayes envisions the information infrastructure as a stack of functional layers with each layer "concealing the lower ones from view":

account for the details of the other layers. This combination of parts provides the autonomous links that allow the user to find, retrieve, and transfer data through an information network (i.e., the Internet). Each layer has a specific function to perform and provides the data necessary for the part of the system above or below it to perform its function but alone will not perform the function of the network.[354]

This stratified architecture is also means of dealing with complexity. Each layer needs only the correct input from the layer it interacts with to perform its intended without being concerned with how that layer performs its function. Therefore, the complexity of each layer is "walled off" from all other layers.[355] This boundary setting provides some defense against system accidents since the layer above or below must recognize the data provided by its adjacent neighbor to function. However, if the data is recognizable, even if corrupt, the next functional layer will pass the corrupted data to its neighbor layer to cascade throughout the system. Although each layer has slack built in to interrupt this flow of corrupted data (essentially discontinue the operation of the particular layer until the corrupted data can be corrected), it has to be recognized as corrupted before it is interrupted.

Just such an incident occurred on April 25, 1997. MAI Network Services, a small Internet service provider headquartered in McLean, VA., released a routing table update

- Application layer – software instructions the end user employs for content to be transmitted over the infrastructure;
- Transport layer (TCP) – instructions that breaks the data into packets and prepares them for transport over the infrastructure;
- Network layer (IP) – directs data packets to their destination;
- Data-link layer – instructions to hardware for dealing with flow control and correction of transmission errors; and
- Physical layer – machines that translate the data from software code to voltage levels, modem tones, or pulses of light or back to software code (Hayes, 214-215).

[354] Hayes, 214-215.
[355] Hayes, 214.

for its routers. Routing tables periodically provide updated information about available routes for packets to travel to their destination in the constantly changing world of the Internet. At 8:30 AM MAI broadcast the updated routing information to it own routers but because of an incorrect configuration the update also rewrote the routing tables of a large number of routers owned by Sprint and UUNet to which they were connected. The updated routing tables instructed the Sprint and UUNet routers to send all traffic to several MAI routers.

Suddenly, all Internet traffic was suddenly redirected towards MAI. Because it never had the capacity to handle even a fraction of this flood, MAI began absorbing packages at an incredible rate. Forty-five minutes later the company was forced to shut itself down to stop the damage. In the meantime Internet providers helplessly watched all their traffic being directed to MAI where nothing ever reappeared. Sprint recovered only after it manually changed all the routing tables it owned, as did many of the big and small Internet providers affected by the problem. Within minutes of its release, the misconfigured routing table was part of several large networks, triggering a classic cascading failure[356] and, at the same time, a classic system accident. Corruption of the entire Internet was prevented only by human intervention, however, at great costs to those involved.

This property of aggregating a large number of discrete individual parts into an information infrastructure system appears to provide a degree of slack that prevents a complete collapse of the system. At the time of a catastrophic malfunction, the affected parts can always be disconnected from the rest of the system until the cause be determined

[356] Albert-Laszlo Barabasi, Linked: The New Science of Networks, Cambridge, MA.: Perseus Publishing, 2002, 153-157.

and corrected or system can be re-built. As the case study on denial of service at Appendix B. Denial of Service demonstrates, this is exactly what the managers and administrators did when faced with overwhelming systemic malfunction from attackers. In fact, the normal protocol to assess and correct a systemic malfunction of any kind seems to be to disconnect the part of the system suffering the malfunction from the system until the cause can be determined and corrected. This would seem to indicate that the information infrastructure system is not so tightly constructed at the present to allow for human intervention. The more immediately pressing problem currently is the recognition of data that will cause systemic malfunctions to allow more timely intervention to disconnect the affected parts of the system before the malfunction is cascaded to other interconnected parts.

Given the properties of all of the parts of the information infrastructure system and the laws of their interactions, it is not a trivial matter to infer the behavior of the entire system. For the information infrastructure system, complexity increases as the network sends and receives data on diverse platforms designed to perform ever increasing diverse functions across organizational and geographical lines. As more functions are added to such a system it develops more and more complex interdependences between the parts. These complex systems cannot be understood by an analysis that attempts to decompose the system into its individual parts in order to examine each part and relationship in turn. This approach "gives us only a vast number of separate parts or items of information, the results of whose interactions no one can predict. Many of the more recent software defaults (e.g., Microsoft's NT and Internet web browser and Cisco's Internet Operating System (discussed in footnote 248)) are a result of this phenomenon. If we take such a system to pieces, we find we cannot reassemble it!"[357]

Because of their great complexity, exceedingly complex, probabilistic systems (such as the information infrastructure system) defy conventional mathematical modeling approaches and often exceed engineering capabilities for intellectual control. Instead, the most widely employed technique of analysis is to simulate the operation of the system. All the variables and relationships of interest (to include security) are linked as understood into a model and then certain ones are manipulated and the resulting action observed as the simulation of the system plays itself out, e.g., cosimulation techniques in software development.[358]

As a consequence, it is virtually impossible to predict and protect against all the ways in which exceedingly complex, probabilistic systems can fail. Failures will occur both in software and hardware, from a low-level network link or router to higher-level service elements such as a name server or web server. Although technologists have a set of tools that mitigate failures to some extent, neither is there a full understanding of how to address the problem of complex failures in distributed systems, nor has an adequate job of preparing programmers and users for the fact that, despite our best efforts, failures will occur.

As networks grow to connect millions of nodes, and as these nodes all communicate in unpredictable patterns, the resulting overall behavior becomes very difficult to model or predict. Large highly connected systems can show aggregate behavior with complex characteristics: they can become chaotic, show self-organizing features, or oscillate. Large

[357] Ashby, "The Effect of Experience on a Determinant System," Behavioral Science, 1, 1956, 35-42 in Scott, 87.

[358] Ellison, et.al., Foundations of Survivable Systems Engineering, 2.

networks such as the Internet have these tendencies, but the tools or methods to explore this eventuality, to model how this might happen, or to control the resulting behavior, if necessary, are not currently available.[359]

When systems are characterized by high levels of interactive complexity and tight coupling then, Perrow argues, accidents should be regarded as “normal.”[360] “Normal accidents” is meant to signal that, given those system characteristics, multiple, complex, unanticipated, unperceived, and incomprehensible interactions of components that could lead to failures are inevitable.[361]

Different environments also place differing requirements on systems; specifically, environments characterized by uncertainty and rapid rates of change in conditions or technologies present different demands – both constraints and opportunities – on systems than do placid and stable environments. The more varied the types of environments confronted by a system, the more differentiated its structure needs to be. Moreover, the more differentiated the system structure, the more difficult it will be to coordinate the activities of the various subunits and the more bases for conflict that will exist among the components. Hence, more resources and effort must be devoted to coordinating the various activities and to resolving conflicts among components if the system is to perform

[359] Clark, et.al., 686-688.

One technique used in sequential systems that is not applicable for distributed systems is an interactive debugger program to find and correct software defects. The main concern is possible interference with the relative timing between processes in the distributed system, which may either prevent certain timing or synchronization related errors from occurring, or may introduce new errors which would not occur with the probe (Shutz, "Testing Distributed Real-Time Systems: An Overview" in Randell, Laprie, Kopetz, and Littlewood, 288).

[360] Scott, 87-88.

[361] Charles Perrow, Normal Accidents: Living with High-Risk Technologies, New York: Basic Books, 1984, 5 in Scott, 87.

effectively.[362] An uncertain and rapidly changing environment can contribute to Perrow's normal, or system, accidents by prompting responses that are not predetermined by the programs controlling the system.

An example of just such systemic added complexity is the current organizational state of the information infrastructure system as "unbounded."[363] Such networks are created to increase effectiveness and efficiency of communications and services but obviously not for security. These organizational schemes are typically found in the commercial environment to integrate previously fragmented operations into coherent processes open to many organizational participants. In such unbounded systems, each participant has an incomplete view of the whole, must depend on and trust information supplied by its neighbors, and cannot exercise control outside its local domain.

Other than the just described general increase in the information infrastructure system's organizational and functional complexity, an example of increasing complexity through technological advance is the Defense Department's Advanced Research Projects Agency's (DARPA) wrapper efforts. Wrapper software is thin layers of code that system designers can place at the boundaries of an operating system or program to offer a high degree of control over software interactions and data flows. Wrappers promise advances in access control, intrusion detection, encryption, auditing, and data labeling through a "kernel-loadable" module that attaches itself to and extends the kernel without permanently changing the kernel's code at runtime. Wrappers insulate programs from each other and

[362] Scott, 89-90.

[363] "Unbounded" is defined in Ellison, et. al., "Survivability: Protecting Your Critical Systems," as "computer system or systems characterized by distributed administrative control without central authority, limited visibility beyond the boundaries of local administration, and lack of complete information by the network, e.g., the Internet. This same state is also referred to as a "distributed" system by other authors.

make it possible to impose security on large, patchwork applications by intercepting calls from a network and making access control decisions or re-routing calls to a security decision-making engine.[364]

Several commercial companies have developed wrappers that act as a "micro-firewall"[365] to prevent access by rogue Java applets, JavaScripts, Netscape plug-ins, and Activex components to portions of the system the user has declared off-limits and to allow users to describe the files to which a browser will be allowed access. Research is also being done to "harden firewalls" by limiting damage if the firewall service is overrun and to provide a "runtime support system" that loads into the operating system before the wrapper loads. Despite all of the publicity, wrappers only add the ability to save data and, by dealing with the boundary of the operating system, to control only a limited amount of the operating system. The wrapper cannot really know what is going on deep inside the operating system.[366]

Of course, the previous discussion on "patches" and complexity suggests that such wrappers may not always perform as intended. There are also assurance issues to be addressed. "The problem with ... programs is that when you plug the components together, you don't know what you've got," (the previously discussed issue of joined software programs not always operating as logic dictates they should because of some missed outcome or effect) says Lee Badger, a principal computer scientist with Trusted Information. There is also the possibility of damaging the operating system kernel and,

[364] Adams.

[365] A firewall is a system designed to defend against unauthorized access to or from a private network (United States National Security Agency, National Information Systems Security (INFOSEC) Glossary).

[366] Adams

particularly important in situations where time is a critical factor, a decrease of about 30 percent in efficiency in current network transactions.[367]

Finally, the information infrastructure system is at risk, as is all other networks, from structural vulnerabilities inherent in its network topography. Existing empirical and theoretical evidence indicate that complex networks can be divided into two major classes based on their connectivity distribution: exponential and scale-free (See Figure 3.2. Exponential and Scale-Free Networks following).

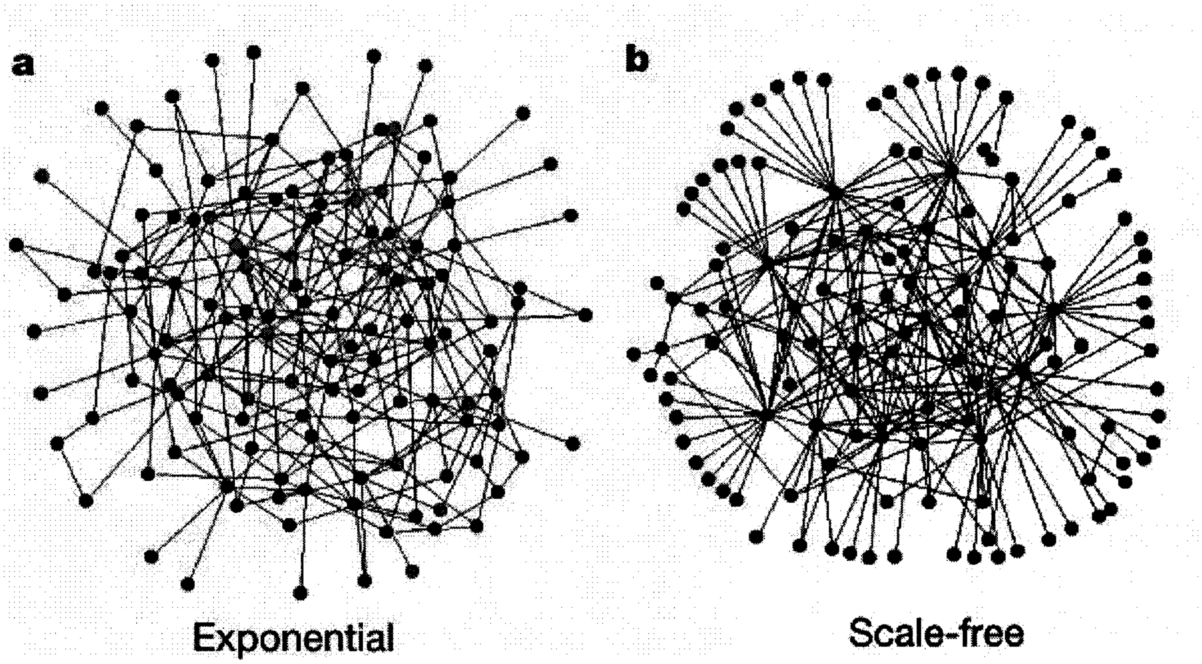


Figure 3.2. Exponential and Scale-Free Networks[368]

[367] Adams.

[368] Reka Albert, Hawoong Jeong, and Albert-Laszlo Barabasi, "Error and Attack Tolerance of Complex Networks," Nature, no. 406 (July 27, 2000).

The tolerance of a given network to different types of disturbance depends critically on the structural difference of these two classes of networks.

Given a set of nodes and links (130 nodes and 215 links in the exponential and scale-free networks, respectively, in the figure above), a simple network (exponential) can be built by linking pairs of nodes at random until all available links are used. Such a random network has roughly the same number of connections; it is statistically homogeneous. In the visual illustration above, the five most connected nodes in the exponential network reaches 27 percent of the nodes in the network.

But most natural and man-made networks have much more intricate hierarchical structures. These more complex systems belong to a class of inhomogeneous scale-free networks that follow power laws. This means most nodes will have one or two links, but a few highly connected nodes will have a large number of links and so play a key role in the behavior of the network. In the illustrative figure, the five most highly connected nodes reach 60 percent of all the other nodes in the network. These highly connected nodes are statistically significant to the scale-free network's operation as opposed to exponential networks where the probability that any node has a very large number of connections is practically prohibited by definition.

Research has shown that in any network, regardless of class, the deletion of a node increases the distance between the remaining nodes by eliminating some paths that contribute to the system's interconnectedness thus degrading the network's functionality. Also, when nodes are removed, clusters of nodes whose links to the system have disappeared may be fragmented from the main cluster. Accumulation of fragmented nodes has a deteriorating effect on the network's performance by making it increasingly difficult for the system's remaining nodes to communicate with each other since some direct connecting paths between the remaining nodes of the networks are eliminated. These remaining nodes then will have to use increasingly more indirect paths to communicate with each other. Theoretically, nodes can be removed from a network either randomly or by an intentional attack that generally is, or most certainly can be, aimed at the most connected nodes. The removal choice has dramatically different results for the two types of networks.

In an exponential network, owing to the homogeneity of the network, there is no substantial difference whether the nodes are selected randomly or in some attack scheme based on the order of connectivity. With network homogeneity, all nodes contribute equally to the network since all nodes have approximately the same number of links. Removal of any node causes the same amount of damage and destroys some local paths. Both random and selective attack node deletion will have the same degree of network degradation.

In contrast, all scale-free networks display an unexpected degree of robustness under random node deletion. The network is deflated by nodes breaking off one by one leading to isolation of single nodes only, not clusters of nodes. Remaining connected network nodes are still able to communicate unaffected under an increasing level of unrealistically high failure rates. Thus even when as many as 5% of the network's nodes fail, the connectivity between the remaining nodes in the network is unaffected; the largest cluster's size only decreases. The network will fall apart only after a main cluster has been completely deflated. The immunity of the free-scale network's performance to random error suggests two features about the network structure:

- most of the nodes are just "end users" not connected to other nodes, the removal of which does not affect the paths between the remaining network's nodes; and

- there are some "degenerate paths" between nodes which implies the existence of highly connected nodes.

These phenomena can be explained by the scale-free network's extremely inhomogeneous connectivity distribution: the power-law distribution implies that the majority of nodes have only a few links, therefore nodes with fewer connections will have a much higher probability of being removed in a random node deletion. The removal of these less-connected nodes does not alter the path structure of the remaining nodes, and thus has little impact on the overall network topology or functionality.

However, the inhomogeneous structure that makes the scale-free network superior to the exponential network in the case of random node removal becomes its Achilles' heel under a targeted deletion attack. By definition, scale-free network connectivity is structured through a few highly connected nodes. When these vital nodes are eliminated, the network topology is altered (unlike the exponential network), and the paths of the remaining nodes to other nodes are greatly diminished. And, if a vital (or, a highly connected) node is deleted or vanishes, catastrophic fragmentation of the scale-free network into many isolated clusters is swift.

The information infrastructure system behaves in just such a fashion. Such maps as there are confirm the information infrastructure system to be a scale-free network.[369] Figure

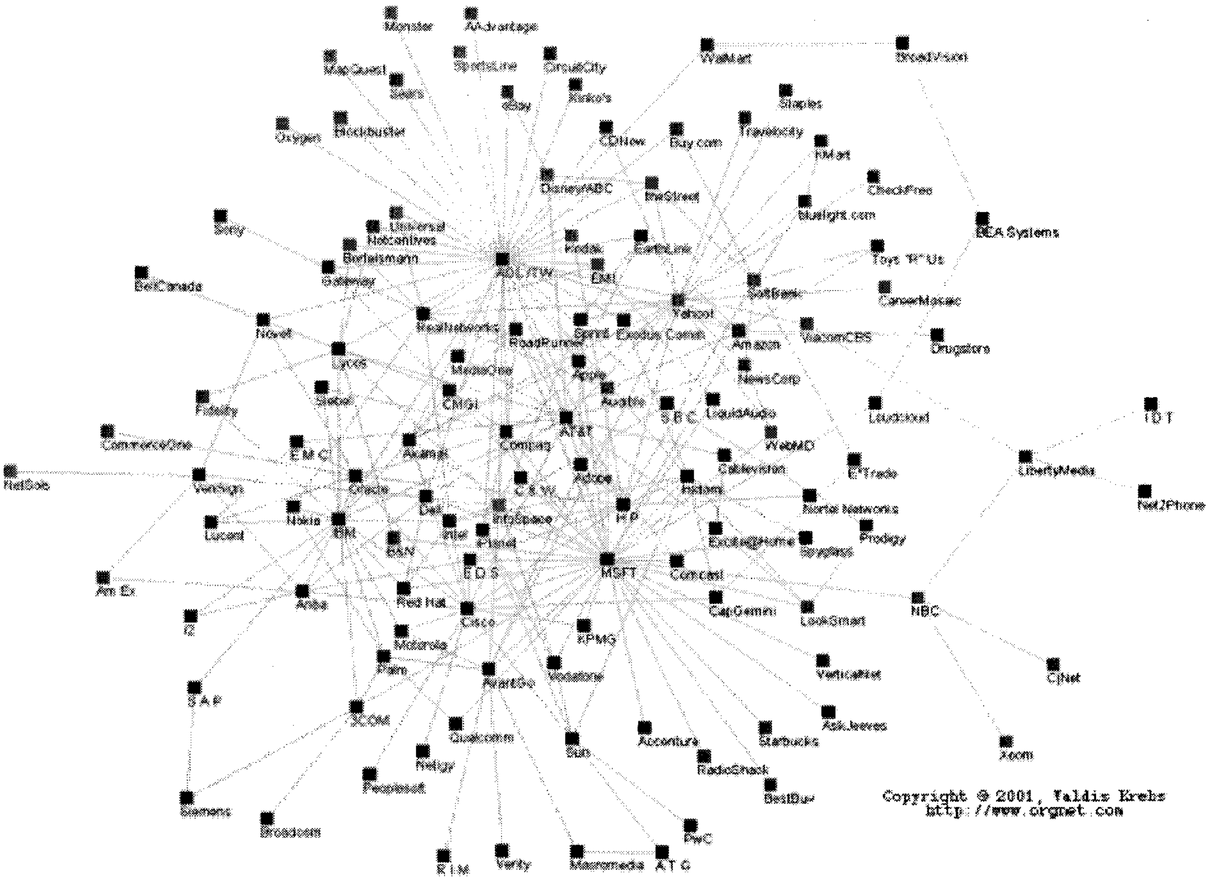
[369] Obviously, because of the extent and complexity of the Global Information Infrastructure (GII) and some National Information Infrastructures (NIIs) (e.g., the U.S. and European) maps are not able depict the entire information infrastructure network in a single complete map that can be viewed on a single sheet of 8x11 paper. Such maps as do exist generally depict either only the major connections (backbones) or a picture of all connections for only a small portion of the total network. (See http://www.cybergeography.org; http://www.geog.ucl.ac.uk/casa/martin/atlas/isp_maps.html; http://www.girardin.org/luc//cgv/; http://www.ckdhr.com/dns-loc/; http://www.ckdhr.com/dns-loc; http://hawk.fab2.albany.edu/webmaps/srchengn.htm, for examples of different types and forms of cybermaps).

3.3. Map of Internet Industry Partnerships, Strategic Alliances & Joint Ventures (following) is a graphic representation the connections between selective industry relationships that clearly demonstrates the scale-free nature of its network. This should come as no surprise given the original network connecting computers at distant locations (ARPANET) evolved into today's information network's structure.

The solutions chosen by the developers of the original data network (ARPANET) to difficult technical networking issues practically foreordained the scale-free network of today's information infrastructure system. The developers conceived of "gateways" (intermediate computers called Interface Message Processors (IMPs)[370]) to link Computers to and to control the envisioned network. This concept effectively left "host computers out of the network as much as possible and created a smaller subnet by inserting a small computer between each host computer and the network of transmission lines." The concept solved the technical problems of connecting computers with different hardware, software and operational functions, but at the same time effectively created a scale-free network of characteristic highly connected "gateway" nodes.[371]

[370] These gateway IMPs "interconnected the network, sent and received data, checked for errors, retransmitted in the event of errors, routed data, and verified that messages arrived at their intended destinations." The original Interface Message Processors (IMPs) are the equivalent of today's servers and routers. "Gateways were the internetworking variation on IMPs, while routers were the mass-produced version of gateways, hooking local area networks to the ARPANET" (Hafner and Lyon, 244).

[371] Hafner and Lyon, 72-75.



Copyright © 2001, Valdis Krebs
http://www.orgnet.com

Figure 3.3. Map of Internet Industry Partnerships, Strategic Alliances, & Joint Ventures[372]

[372] Figure 2.3, Representative Complex Information Infrastructure, represents a portion of the Internet Mbone connections clearly shows the network to be a scale-free network. Each node in the network represents a company that competes in the Internet industry. The map distinctly shows examples of nodes that are end users and both most-connected and vital (highly connected) nodes. "Two firms, AOL-TW and Microsoft are in positions of power in this network. (Positions of power are calculated from the overall pattern of connections in this network)." These "positions of power" equate to the highly connected, or, vital, nodes of the conceptual discussion and from the graphic display of the map, it is easy to see what would happen to the network if these nodes are removed (orgnet.com, Logic Programming Associates (LPA) Homepage, November 21, 2001 (Last Updated: June 21, 2001), http://www.orgnet.com/netindustry.html).

As the original ARPANet network sites grew from four sites in 1969to what it is today, not only the number of network connections increased but locally and regionally connected networks (LANs) based on authenticated technology, browsers, the World-Wide Web, e-mail, and other applications evolved. The one constant was the original gateway concept and structure for connecting to the ARPANET and its successors (CSNET, NSFNET, INTERNET (the collection of all connected networks), etc.[373] These "gateways" (servers and routers) then represent the highly connected and most-highly connected nodes of a scale-free network.

This evolved information infrastructure system survives as a large cluster under high rates of random failure, but abruptly falls apart under attack[374] of the most-connected nodes. When the researchers tested the Internet and World Wide Web, they found that the error tolerance of the two networks has exactly the same characteristics as that of the scale-free network. The function of the Internet is unaffected by the random removal of as high as 2.5% of the nodes whereas if the same percentage (2.5%) of the most connected nodes are eliminated the failure rate more than triples.

Similarly, large connected clusters persist for high rates of random removal, but if nodes are removed selectively in a decreasing order of connectivity, the size of the fragments that break off completely increases rapidly. This exhibited behavior of a scale-free network explains why, despite frequent router problems, the global network rarely experiences total outage or, despite the temporary unavailability of many web pages, the ability to surf and locate information on the web is unaffected.

[373] Hafner and Lyon.

[374] See Appendix B. Denial of Service for a more detailed examination of and explanation of activity that unintentionally or deliberately targets highly connected nodes.

Although it is widely thought that attacks on networks with distributed resource management such as the information infrastructure system would be less successful than an attack on a network centrally managed, empirical results indicate otherwise. Distributed resources management in itself creates vital nodes and has the properties of a scale-free network, e.g., system administration, different types and classes of servers, etc., and the connections to those vital nodes that are then susceptible to selective attack. The inherent structural weaknesses of a scale-free system, rooted in inhomogeneous connectivity distribution, could, thus, still be exploited by those seeking to damage the information infrastructure system by attacking these most connected or vital nodes to seriously reduce its survival probability.

Any informed agent that attempts to deliberately damage a network will not eliminate even the most-connected nodes randomly, but will preferentially target them in descending order of connectedness or some other criteria of importance to more effectively jeopardize the system even more. The performance of the Internet is reduced by a factor of two if just 1% of the most connected nodes are destroyed; and with only 4% of its most important nodes destroyed, the Internet loses its integrity, becoming fragmented into small disconnected domains.[375]

The information infrastructure system would appear, on the surface, to some to be impervious to this type of directed attack given its complexity and the scope of the system. An attacker seeking to conduct such an attack would need some way of detecting these most-connected or vital nodes. Currently, maps depicting the structure and topology of this

[375] Albert, Jeong, and Barabasi; and Yuhai Tu, "How Robust is the Internet?" Nature, no. 402 (July 27, 2000).

amorphous global network are non-existent or severely limited. However, ominously rudimentary depictions of portions of the information infrastructure system and tools to better map it now exist and are being further developed. **Skitter**, the primary tool for determining node connectivity, and **traceroute** (another tool) send out packets of data from a source to many different destinations throughout the information infrastructure system and record the paths these packets take to:

- Acquire infrastructure-wide (global) connectivity information (what's connected to what?) and
- visualize network-wide connectivity (what does the network look like?)

By analyzing skitter's data, critical paths, pivotal roles of specific backbones, traffic exchange points, and individual routers can be identified. Using data from skitter in 1999, the criticality of CerfNet/AT&T, Cable & Wireless (the old MCI backbone) Sprint, and UUNET (part of MCI/Worldcom) in transporting packets across the infrastructure from San Diego was revealed.[376]

The information infrastructure system can also be considered as the cyber equivalent of a natural system. Just as in an evolutionary natural network, the Internet exhibits growth of and preferential attachment in its inhomogeneous connectivity distribution. At the system's heart is a mesh of interconnected backbone networks containing, in scale-free network terms, the most connected, or vital, nodes. The most vital nodes are probably the "peering points" where networks come together to exchange traffic. In 1997 the largest two peering points on the East Coast were the New York Network Access Point (NAP) and the

[376] K. Claffy, Tracie E. Monk, and Daniel Mc Robb, "Internet Tomography," Nature: Web Matters, January 7, 1999, http://www.nature.com/nature/webmatters/tomog/tomog.html.

Metropolitan Area Exchange (MAE)-East. MAE-East was an enormous hub and spoke structure where 100 networks carrying more than half of the traffic on the Internet at the time converged on a single point.[377] Obviously, degradation of this node would affect the functionality of the network tremendously. I would suspect that such vital nodes still exist and are relatively easy to locate in cyberspace as well as physically. Once located, an intruder with malicious intent potentially could affect the operation of the node leading to degradation of the network. Obviously, physical location of the node makes it vulnerable to physical attack that will also lead to degradation of the node.

There is no dispute that the system is rapidly evolving. New connections among core Internet backbones are made hourly, ranging in capacity from T1 copper cables (1.55 megabytes per second) to (OC48 fiber optic pipes (2.48 gigabytes per second). The last mile connections from the Internet to homes and businesses are supplied by thousands of small and medium sized Internet Service Providers (ISPs) resulting in a complex array of telecommunications carriers and providers.[378] However, given the system's preference for a scale-free architecture for greatest efficiency, vital nodes will always exist unless purposefully engineered out of the system for security reasons.

In natural evolutionary systems, error tolerance is not just a passive property of the network structure; rather it is part of the driving force by which evolution selects the network structure for maximum survivability. One key component of this desire for survival is redundancy; achieved through preferential attachment for naturally occurring organic systems and the antithesis of efficiency. Unfortunately, such natural evolutionary

[377] Hayes, 216-217.

[378] Albert, Jeong, and Barabasi; and Claffy, Monk, and McRobb.

forces are not at work with the information infrastructure system, or many, if any, systems designed by humans. The paramount force for the U.S. information infrastructure system, governed by the laws of the free market system since its assets are predominantly privately owned, is efficiency, not survival. Competitive providers, all operating at fairly low profit margins, consider redundancy to be a luxury they cannot afford and remain in business. As a result, today's information infrastructure industry lacks any ability to evaluate trends, identify performance problems beyond the boundary of a single ISP, prepare systemically for the growing expectations of its users, and, in the long term, to deal with systemic errors.[379]

As the discussion suggests, software vulnerabilities are not limited just to providing easy access for intruders. Software's vulnerabilities are also instrumental in cascading effects; defects in one software system affect any other system to which it is connected and will more than likely cause that system to malfunction as well. Whether the malfunction merely causes the succeeding system(s) to fail (a loss of availability), to produce inappropriate output (loss of data integrity), lose confidentiality, or not provide the assurance that a message has been received or is from the indicated sender (nonrepudiation and authentication) is extremely significant in the integrated software and infrastructure systems of today and the future.

Buffer[380] overflow is just one such effect where the effect of a problem cascades beyond the original piece of hardware or software. Buffer overflow occurs when the

[379] Tu; and Claffy, Monk, and McRobb.
[380] A buffer is a device or storage area that serve as a temporary waiting and staging location to compensate for differences in rates of data flow, time of occurrence of events, or amounts of data that can be handled by the devices or processes involved in the transfer or use of data (Institute of Electrical and Electronics Engineers, IEEE Standard Glossary of Software Engineering Terminology (Std. 610.12-1990); and Hafner and Lyon).

buffer is written beyond its intended capacity and is generally associated with a loss of availability (the denial of service phenomenon is discussed more fully in Appendix B. Denial of Service). Not only do the resulting effects affect the buffer or the device in which the buffer is physically located, but they extend to the entire system as well because of interconnectivity.[381] In many cases, buffer overflow results in the operational cessation of the computer or application that has suffered the overflow. Not only does this cause a denial of service, but a savvy user can also insert malicious code in the data that causes the overflow that may enable the code to execute on the computer, unbeknownst to the owner. Such code can introduce a virus or Trojan horse designed to steal passwords, to stop the system, delete files, or even gain administrator-level control over a local network if the overflowed application has "superuser" status. Overflow problems can be notoriously difficult to correct because C++ and other programming languages used to create the bulk of applications today don't have adequate boundary checking.[382]

[381] Microsoft's Internet Explorer 4 was discovered to have a buffer overrun defect that could threaten Windows 95 after it had been marketed. By feeding Internet Explorer 4 a URL that contained more than 265 characters with the "res://" prefix, the HTML interpreter would crash. By adding executable binary code to the end of the long URL, Windows 95 would run the executable code after the HTML engine crashed. Amazingly, the hacker that reported the error had discovered it six months earlier while previewing the beta version of Internet Explorer 4 and was amazed that Microsoft did not catch the error during beta testing (Brian McWilliams, "Hacker Reveals Serious Security Hole in IE4," PC World News Radio, November 12, 1997, http://www.pcworld.com/news/article/0,aid,5605,00.asp).

Microsoft still has not solved buffer overflow problems; Microsoft Security Bulletin MS01-033 was issued on June 18, 2001 alerting users of Windows NT 4, Windows 2000, and Windows XP beta to a vulnerability in the "idq.dll extension that is a component of Index Server and provides support for administrative scripts and Internet Data Queries." Microsoft considered the vulnerability a "serious vulnerability" because an intruder who successfully exploited the vulnerability could gain complete control over an affected web server. This would give the intruder the ability to "take any desired action on the server, including changing web pages, reformatting the hard drive, or adding new users to the local administrator's group (Microsoft Corporation, Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise).

[382] Andy Eddy, "Buffer Overflow Bugs Here to Stay: Recent Microsoft, Netscape Software Problems Nothing Out of the Ordinary," Network World, August 10, 1998.

Software's acknowledged complexity also supports my contention that complexity, in both software systems and the overall information infrastructure system, breeds "system accidents" for which there is no discernible empirical reason and for which designers cannot plan. Still, an intrusion is probably the most disconcerting and worst case security failure of all.[383]

Intrusions are deliberate attempts at transgressing the security policy assigned to the system. They can originate from external intruders, authorized users trying to exceed their privileges, or privileged users, such as administrators, operators, security officers, etc. who abuse their privileges to perform malicious actions.[384] Such an agent can manipulate the system to compromise completely any and all of the information assurance objectives through deliberate action unbeknownst to authorized users. Even more insidious, intruders always seem to be able to develop a new means of attack to circumvent new technology solutions to a particular vulnerability. It is not clear that even in principle it is possible to identify all possible attacks a priori. [385] Therefore, trying to safeguard the information

Buffer overflow has have gained even greater notoriety recently with the growing use of communications software and the Internet. Both the e-Bay and Yahoo loss of availability in Spring 2001 were caused by buffer overflow (See http://cert.org and http://catless.ncl.ac.uk/Risks/20.87.html#subj3.1 for more detailed account of both incidents).

[383] The security profession recognizes intrusion as the most significant risk to the automated information systems community (Evans and Morrison, "Penetration Testing." in Ruthberg and Tipton, S-65).

[384] Fabre, Deswart, and Randell, "Designing Secure and Reliable Applications using Fragmentation-Redundancy-Scattering: an Object-Oriented Approach" in Randell, Laprie, Kopetz, and Littlewood, 173.

[385] As the intruder gains familiarity with a system a kind of learning process takes place until entirely new attacks, initially completely outside the imagination of the attacker (and system owner), are invented which exploit peculiarities of the system. If this is the case, then it represents a kind of enlargement of the scope of potential attacks over time, or at least a drastic shift in the operational profile resulting in attacks that were initially unimagined (i.e., 'impossible') acquiring an increasing probability of occurrence as time and effort are expended (Littlewood, et.al., "Towards Operational Measures of Computer Security: Concepts" in Randell, Laprie, Kopetz, and Littlewood, 545-546).

infrastructure system is analogous to an ever escalating arms race where one party is continuously trying to gain the advantage over the other party.[386]

As discussed earlier, almost any person or organization can now possess the capability to initiate a malevolent action over the information infrastructure system with very little investment. If such a person or organization exists and he "wants on a system, he will eventually get there,..."[387]

3.4. Intruders.

> "Any computer network automatically introduces the risk of unauthorized access to a system. Hackers most likely exploit the weaknesses in software access controls to enter the system itself."[388]

As previously stated in Chapter 1. Introduction, four types of perpetrators seem to exist: mischievous, criminal, terrorist, and state. The common lure for all four is generally the minimal effort required and the low level of risk involved. The system's vulnerabilities can enhance anonymity by allowing intruders to conceive, plan, invisibly reconnoiter, clandestinely rehearse, and execute an action without any detectable logistic preparation in a matter of minutes or even seconds from a distance without revealing their identity by obfuscating the route of an activity, or even disguise the activity to resemble an accident instead of an attack if that is their intent. This inherent anonymity further reduces the

[386] Kanoun and Laprie, "Software Reliability Trend Analyses: From Theoretical to Practical Considerations" in Randell, Laprie, Kopetz, and Littlewood, 9.

[387] Pipkin, 5.

"Of the hackers that were discovered, some 40 to 60 percent of them think maybe they were actually into corporations that had computer security systems and firewalls in place and the hackers still managed to get past them," Forrest Sawyer (ABCNew, "Computers: World Wide Warfare").

[388] Myerson, 146.

possibility of discovering the real perpetrator(s) and immediate retaliation by a system's proprietor.[389]

However, even with all of the system's vulnerabilities just discussed a potential intruder still has to gain entry into the information infrastructure system to exploit it. The remainder of the chapter details how intruders could possibly do that and then use this unauthorized entry to do as they wish with not only the system to which they have gained access but to any component of the entire infrastructure system.[390] The different techniques discussed that an intruder may use are not meant to exhaust the possibilities for gaining access or exploiting a system, only to illustrate that there is not a dearth of ways for intruders to achieve their goals.

3.4.1. Beginning: Gaining Unauthorized Access.

> "Computer break-in can occur in various ways because systems connected to the Internet almost always have certain vulnerabilities."[391]

In this section, I will focus on the first, and most difficult, obstacle a potential intruder has to overcome to exploit any system component's vulnerabilities: gaining access to a system. Once the user has gained access to the system, he then becomes just another user trying to gain access to the system's data.[392] It may take an intruder some time to gain access to the targeted system, but if he is persistent, he will eventually get there. The Hanover Hacker persevered for over two years to find a path from Hanover, Germany, to

[389] James Glave, "U.S. Computer Security Called Critical Mess" (Original article written October 28, 1997), Inforwar.Com & Interpact, Inc. WebWarrior@Infowar.Com, March 22, 2001, http://www.infowar.com/civil_de/civil_103097a.html-ssi, 2.

[390] See Carolyn P. Meinel, "How Hackers Break In...," Scientific American 279, no. 4 (October 1998), 98-105, for a excellent fictionalized scenario based on real incidents of how a potential intruder uses the techniques described (and others) to gain access to a system which has excellent and vigilant security measures to protect against unauthorized access.

[391] Meinel, 98.

[392] Pipkin, 27.

Berkeley, California, to White Sands, New Mexico. As reported by Evans and Morrison, "his intent was to steal military secrets, and he was very determined to succeed."[393]

Although the most difficult task the potential intruder must overcome, gaining access is still not that terribly difficult. Increased availability of easy to use hacker tools over the Internet makes the potential intruder's job even easier. The explosive growth of and dependency on networked computers and the ever-increasing connectivity of these networks provide the potential intruder plenty of opportunities to gain unauthorized access. With the size and complexity of the networks and the number of users, an intruder has a better chance of gaining unauthorized access and exploiting the data than ever before.[394]

The majority of successful attacks on information systems can be traced to a few software vulnerabilities.[395] Intruders are opportunistic; they exploit the easiest, best-known, and most convenient vulnerabilities with the most effective and widely available attack tools. They depend on administrators and users not fixing problems thereby allowing these legacy vulnerabilities to remain within systems for a long time.[396]

Evolving social and business practices further increase the potential intruder's probability of gaining access. Business today requires greater sharing of information with individuals who are not employees. Organizations provide their employees with portable

[393] Donald L. Evans and J.A. Morrison, "Penetration Testing," in F.H. Tipton and Z.G. Ruthberg (eds.), Handbook of Information Security Management (1995-95 Yearbook), Boston: Auerback, 1995, in Kenneth Boulding, "General Systems Theory: The Skeleton of Science," Management Science 2, 1956, 19-20.

[394] Pipkin, 97, 104, and 106.

[395] The SANS Institute has sponsored cooperation among industry, government, and academia to identify the ten most exploited Internet security flaws. See SANS Institute, "How to Eliminate the Ten Most Critical Internet Security Threats: The Experts' Consensus," Version 1.32, SANS Resources, January 18, 2001, http://www.sans.org/topten.html.

[396] Many administrators report that they do not know which of over 500 potential problems are the ones that are most dangerous, and they are too busy to correct them all (SANS Institute, http://www.sans.org/topten.html, September 11, 2001).

computers for "mobile computing" to continuously stay abreast of activities and operations while at the same time, opening new opportunities for a potential intruder to exploit.[397]

Even trusted system networks are vulnerable to unauthorized access. Generally, all systems in a trusted host group are similarly managed, often by the same administrator. An intruder can find the list of trusted hosts, especially the added trusted hosts since they have been added by users and not the system manager. The intruder then only has to define a user ID of another trusted system to use the current system since trusted systems are generally reciprocally trusted. An intruder may use other techniques (e.g., RUPTIME, ARP Cache, RPCINFO, RUP, etc.) to locate information about the system, including trusted systems, to which he is trying to gain unauthorized access.[398]

The first piece of equipment that serious potential intruders must have is a computer of their own. The falling price and the increasing performance of computer equipment have made it possible for almost any potential intruder to afford a powerful computer system. Potential intruders will spend many hours using their computer observing the system to which they are connected and the other users connected to that system. A serious potential intruder is in control of his own computer system's permissions and privileges and can appear as anyone they want to another system to further guarantee anonymity. A computer and a system will also give the potential intruder invaluable experience at managing and securing a system and, therefore, insight into the practices used on a targeted system.

A serious potential intruder will begin with a great deal of acquired knowledge. He will already know, for example, as much as he can about the common operating systems for

[397] Pipkin, xi-xii.
[398] Pipkin, 94-96.

networking (VMS, UNIX, OS/2, and LINUX) and the different networking tools and protocols. There is an abundance of information about all of the operating systems in the public arena, especially LINUX since it was and still is developed in the public domain and is not proprietary. With the advent of distributed networks, desktop operating systems such as Windows NT and OS/2 have gained greater popularity, usage, and disbursed documentation in the public arena making these programs easier for a potential intruder to abuse also.[399]

The truly serious potential intruder will also know how to write C code and shell scripts to modify tools for his needs and to automate access techniques When the serious potential intruder finally decides to try to gain unauthorized access to a system, "It is almost a given he will know more about the internals of the operating system of the targeted system than the system administrator or security manager."[400]

Any information about information system security can be used by the potential intruders to their benefit. Many of the same tools used by system managers are also used by intruders. He will have read the latest security bulletins from the different security monitoring organizations (e.g., CERT, the National Institute of Standards and Technology (NIST)), vendors, the hacking underground, security news groups, and e-mail lists) to learn about the latest security bugs and patches and to locate new tools to use. Not only will a serious potential intruder know the details of how the operating system works, but he will

[399] Pipkin, 6.
[400] Pipkin, 1-7 and 25.

also know what auditing and security tools are in use on the targeted system and how to use them to his advantage. [401]

A potential intruder has different options for gaining unauthorized access depending upon the configuration of the targeted machine and whether it is connected to a data-sharing network. If not connected to a data-sharing network, the potential intruder is constrained to operating on the same network as the targeted system. However, most systems today connect to other networks.

Regardless of whether the targeted machine is connected to a network or not, to gain access to another system a potential intruder must use an ID and password the targeted system recognizes. Trying to guess login Ids and passwords is the most dangerous and unproductive way for the potential intruder to attempt to gain unauthorized access to a system. Attempts to log in will be logged, whether they are successful or not, by the system's accounting system and eventually noticed by the system administrator.[402]

This generally though is not an insurmountable problem for someone who is intent on gaining access to a system. First, the potential intruders will have the data they acquired from monitoring the targeted system and as wide a variety of sources as possible. System users themselves will give up more data. Potential intruders will also take every opportunity to acquire personal private information from individuals, e.g., phone card numbers, ATM PIN numbers, system passwords, etc.[403] This may be no more innocuous than looking over

[401] Pipkin, 25.

[402] Pipkin, 28.

[403] Not only will this personal information help a potential intruder circumvent the usual security measures for personal accounts, but it can also be used in an equally sinister scheme to steal one's identity to gain access to financial and other assets. Identity theft has increased significantly because of the ease with which one can access individuals' personal private data with information technology, even the famous and celebrities. Tiger Woods recently testified at the trial of Anthony Lemar Taylor who used his personal

someone's shoulder, striking up a conversation with someone, "social engineering,"[404] visiting the target's facility, going through the trash, or it may involve more sophisticated high tech means of electronically intercepting conversations, wireless connections, or monitoring a computer system.[405]

Electronically obtaining a password is relatively simple for a potential intruder. Many proprietary systems will offer help at the login prompt that will explain the login syntax and options simply by typing "help" at the login prompt.[406] And although encrypted, a system's password file is readable to all even without logging on to the system. The potential intruder can then easily copy it to his own system to decipher.

information to obtain a driver's license and credit cards in Woods' name. Taylor eventually used the credit cards to obtain more than $17,000 in merchandise (Dave Anderson, "Sometimes a Nickname Has a Price," New York Times, May 3, 2001).

Even more audacious was the case of Abraham Abdallah. Abdallah was able to gain access to the personal data of 217 of the Forbes magazine 400 richest people in America including Oprah Winfrey, Michael D. Eisner, George Lucas, Ronald O. Perlman, Michael R. Bloomberg and Paul Allen. Investigators have yet to determine how much Mr. Abdallah was able to steal from his victims before he was arrested (Jayson Blair and William K. Rashbaum, "Man Broke Into Accounts of Celebrities, Police Say," NY Times, March 21, 2001).

However, this is not a problem of just the rich and famous. The Privacy Rights Clearinghouse "estimates that between 500,000 and 700,000 Americans were victims of identity theft last year." (Jenny Lyn Bader, "Ideas & Trends; Paranoid Lately? You May Have Good Reason," NY Times, March 25, 2001).

[404] Social engineering is a term used to describe the process of getting a person to divulge information through intimidation or persuasion. Many social engineering attempts will go unnoticed since the potential intruder will ask one individual only a few specific questions and then move on to another individual. There are also software techniques of social engineering such as Trojan horses (Pipkin, 20).

A particularly egregious example of social engineering was perpetuated on Microsoft and Verisign, Inc. early in 2001. An individual who fraudulently claimed to be a Microsoft employee convinced Verisign to issue "two Verisign Code 3 code-signing digital certificates" with the common name of "Microsoft Corporation" to him. The person with these two certificates could digitally sign programs, including ActiveX controls, Office macros , and other executable content signifying that they were genuine Microsoft programs. Such digital signatures would probably convince other users to run an unsafe program (spoofing) to most likely distribute malicious code widely (Microsoft Corporation, "Erroneous Verisign-Issued Digital Certificates Pose Spoofing Hazard," Microsoft Security Bulletin MS01-017, March 22, 2001, http://www.microsoft.com/technet/security/bulletin/ms01-017.asp).

[405] Pipkin, 19-24.

[406] Pipkin, 24.

An encrypted password file is not actually deciphered since the encryption algorithm cannot be reverse engineered, but passwords are guessed by processing the password through the potential intruder's personal password cracker dictionary.[407] Studies have shown that between 25 and 30 percent of all passwords can be guessed using this method even though there are over 300 quadrillion possible passwords based on the standard encryption algorithm. Users generally select passwords from only a minuscule percentage of all possible passwords to keep the password simple in order to be able to remember it. Therefore, most user passwords will normally be a word, term or phrase that is important to them, or some derivation of that.[408]

A potential intruder may also check the system's "/etc/btmp" file for passwords that users have inadvertently entered instead of their login name. By comparing bad and good

[407] Pipkin, 38 and 43-44.

A password cracker dictionary is an idiosyncratic software program a potential intruder writes to guess passwords for user IDs captured from the targeted system. Each potential intruder's dictionary is different and will normally be built on the potential intruder's experience and his knowledge of the targeted system. The dictionary generally will include common first names; characters, titles, and locations from works of fiction, television, and film, cartoons, and computer games; sports terms; terms based on the industry in which the targeted computer is being used; and all known information about the user, (e.g., the user's name, initials, account name, etc). All of the above words will be permuted by:

- varying upper- and lowercase letters,
- reversing the spelling,
- substituting the numerals 0,1,2 and 5 for the letters o, i, z and s in the word,
- appending a single digit to the word,
- pairing two words and separating them with a special character; and
- any other logical scheme of simple encryption the potential intruder might think the user would use to make their password harder to guess.

Depending upon the desire of the potential intruder to gain access to the targeted system and their perseverance, selected data will continuously be provided to the dictionary program until a usable password is provided (Pipkin, 39).

[408] Pipkin, 39.

See D. V. Klein, "Foiling the Cracker; A Survey of, and Improvements to Unix Password Security" (original paper), Proceedings of the United Kingdom Unix User's Group, London, July 1990, for an early discussion of the issue.

login attempts from the same terminal, he may be able to determine if a user inadvertently used his password instead of his login name at the login prompt.[409]

The potential intruder may further try to determine a user's ID and password with a Trojan horse program. By getting a user to execute the Trojan horse, the potential intruder can covertly capture the ID and password, as well as any other function the intruder has programmed the Trojan horse to perform.[410]

The potential intruder may also check common multiplayer games to see if a player has entered his system's login password to join the game. Many common multiplayer games let a user suspend his session and return to it later. Many of these games ask for a password so the player can be authenticated when he returns. The passwords are usually stored as clear text.[411]

In many cases, a potential intruder can access a system simply by connecting to the modem or network server[412] without even having to use a password. Some terminal servers will allow connection to a port on the server from over the network. If this port is connected to a direct-connect terminal (such as fiber optic or DSL), an intruder can use a login spoof on the terminal and collect passwords since the modem is always "open" when the hardware connected to it is activated.[413] Some network servers may allow the potential intruder to

[409] Pipkin, 47.
[410] Pipkin, 50.
[411] Pipkin, 47.
[412] A server is a hardware/software integration that provides a transparent connection directly between separate functions, e.g., a terminal and one or more host computers. It may provide multiple terminals with access to a host or it may provide terminals with the capability of switching between sessions on different host machines (Shafer, 576).
[413] "ARPA Moves on `Spoofing'" and Borland, "Feds Work to Block Domain-Name Hackers."

With the spread if DSL and fiber optic technology, more and more servers and individual computers will be connected to the infrastructure system with an "open" modem further facilitating an intruder's task.

connect to the modem that is attached to the port and dial in or out thereby facilitating "connection laundering" (see footnote 232).

The Serial Line Internet Protocol (SLIP) or Point to Point Protocol (PPP)[414] will extend the network to users on the road or at home by giving Transmission Control Protocol/Internet Protocol (TCP/IP) connectivity to any user that dials into it with valid IP address information. With the valid IP address information, a potential intruder can access the system as easily as any other authorized user.[415] Once connected to the modem or server, the potential intruder may then be able to connect to any computer on the same network or any system on which there is routing information.

Data entry systems connected through serial port direct-connect terminals provide a potential intruder an even easier route for unauthorized access if not correctly attended. An unattended session with the computers logged on and left alone allows the potential unauthorized user to gain access to a system to use as they see fit.[416]

The potential intruder may also be able to capture or watch keystrokes, the Windows program, and more on a user's computer if the system's programs are not configured or secured correctly. By using a software program to monitor the terminal port to which the keyboard is attached, a potential intruder can watch what a user types into the computer, including login ID and passwords.[417] Or, by electronically connecting to the X server's port,

[414] SLIP is an Internet protocol designed to run Internet Protocol over serial lines that connect two network systems. PPP is a protocol enabling point-to-point transmissions of routed data from router to router, or from host to network, on local area networks by using synchronous or asynchronous serial interface (Shafer, 461 and 527).
[415] Pipkin, 32.
[416] Pipkin, 28-30.
[417] Pipkin, 49.

the X Windows server can be compromised if not properly protected by a "magic cookie"[418] or the "xhost" mechanism.[419]

Intruders may also be able to gain unauthorized access to the public switch telecommunications network providing the ability to eavesdrop on communications, reroute calls, or steal a phone conversation from a user if the intruder is connected to the phone network during the conversation.[420] Kevin Poulson was probably the most accomplished unauthorized user to use the public telecommunications network to gain unauthorized access to different information networks. He was able to exploit the vulnerabilities of the public switch telecommunications network because through his detailed study of the system's mechanics. (See Appendix A. Kevin Poulson for a detailed description of Poulson's methodology and activities).

3.4.2. Exploiting the Information Infrastructure System.

Once intruders have gained access to a network, they then will look for ways to achieve their ultimate goals. If the goal involves only the network hey have accessed, then they will exploit various vulnerabilities of that system to achieve the goal. More than likely though, the goal will involve gaining access to another or other networks in the information infrastructure system.

Finding other systems on the network to exploit is the easiest part of the process. Once intruders have access to a system on a network, they will generally try to expand their access to other systems by replicating their successful behavior for gaining the initial

[418] A magic cookie is a mechanism by which a server and the client share a secret. The server will allow access only to clients that know the secret (Pipkin, 49).
[419] Pipkin, 49.
[420] Pipkin, 30

unauthorized access. Their first priority is to gather information about the system to which they currently have access, its subnets, and any other systems managed by the same administrator, without alerting system users of their presence if possible. They will try to determine how the system is administered, what accounts have privileges, how much and what type of logging is enabled, and the security measures used.[421]

Once the intruder has gathered what he thinks is enough data, he will then use that data to exploit the network through a variety of means. If the targeted system is connected to a data-sharing network, the intruder has a plethora of programs offering direct access services, most of which use simple text-based protocols that can be subverted even if the intruder has only terminal access. Or, the intruder will use the accessed system's Internet address or host name to communicate with another system. A host's name can be converted to an Internet address generally through a host lookup table, the network interface system (NIS), or the domain name system (DNS). The **nslookup** command can be used to find out which conversion method the other system is using. Any of these methods can easily be comprised.[422]

A potential intruder may also gain access to a user's system through system software start up and shutdown, routers, and the user's login/logout routine if the files controlling those functions are not configured correctly and constantly monitored for tampering. Subversion of any of these functions by a potential intruder subverts the entire system and allows the intruder to execute any privileges the user has.[423]

[421] Pipkin, 25 and 93.
[422] Pipkin, 94.
[423] Pipkin, 55-56.

With twisted-pair and wireless networking, it is possible to monitor the network with available network protocol decoders in turnkey LAN analyzer systems or in software. Many vendors include a network sniffer as part of the diagnostic software that comes with the system. A potential intruder can use much of the administrator's diagnostic information to help him gain unauthorized access to a system.

Recently a hacker group released a utility, Back Orifice that could give anyone on a TCP/IP network complete access to another personal computer using the Windows operating system. Internet Security Systems (ISS) of Atlanta found that Back Orifice provides "an easy method for intruders to install a back door on a compromised machine" and then execute its programmed functions. The utility gives users access to another computer's file system, network information, registry, and processes while also sniffing network traffic and saving all keyboard keystrokes to include passwords.[424]

Network monitoring allows an intruder to watch all the packets that cross the network where they can filter out passwords, any data that is passed across the network, and analyze network traffic to determine the relationship between systems.[425] For example, an unauthorized user could at one time (and probably still can) execute the following actions:

- Request all the information contained in the Domain Name Services (DNS) database through DNS zone transfers;

[424] Andy Patrizio, "Security Firm Exposes Back Orifice Functions," TechWeb News, August 10, 1998, http://www.techweb.com/wire/story/TWB19980807S0012, 1-3.
[425] Pipkin, 48 and 97-104.

- Gain unauthorized access to, request, or put files on a system with TFTP (Trivial File Transfer Protocol)[426] since TFTP requires no authentication (user name or password) to send or receive files from anyone who requests them;
- Gain unauthorized access and information from the NFS (Network File System) because of inappropriate configuration and software problems with the NFS system;
- Eavesdrop and capture keystrokes from the X Windows windowing system;[427]
- Access passwords or access other systems from the FTP (File Transfer Protocol) if it is misconfigured (and overlooked by the administrator) by looking in the user's **/etc/ftpsers** and **~/.netrc** files. Unauthorized users will many times attempt to gain unauthorized access to a system through the FTP since most systems do not log incorrect passwords that are entered via FTP. A potential intruder may even be able to gain unauthorized remote access through the Berkeley Trusted Systems' commands from the FTP directory tree if the protocol is not configured correctly. The FTP will also provide data about the computer system hardware, operating system revision, or version of the program that is operating the system.[428]
- Use the **finger**[429] or **user@system** syntax commands to determine a user's real and login name, office location, phone number, home directory, default shell, **.plan** and **.project** files, information from the GECOS field in the password file, and the

[426] Trivial File Transfer Protocol is generally restricted to send only those files that are in the home directory tree of the user named "tftp." It is also generally used to bootup network devices such as network terminal servers, network-based printers, and X-terminals (Pipkin, 102).

[427] Pipkin, 97-104.

[428] Pipkin, 24 and 97-104.

[429] Finger is an Internet service used to gather information about a person associated with given user identification information (Shafer, 227).

"The finger service allows us to see who's logged on a certain computer" (Peter Bartoli in Siedsma).

terminal's status (idle time if logged in or the last login time if not currently logged in).

- Use the remote **rwho** command to determine who is logged on, the machine name, user name, to which line the user is connected, and the amount of idle time on all systems running the remote daemon **rwhod** using the same connection;[430]
- Use the remote **rusers** command, if the system is using Sun operating software, to generate a list of users on every machine on the subnet;
- Use the SMPT (Simple Mail Transfer Protocol) to verify if a user's login name exists on a system. The **vrfy** command will also give the unauthorized user the person's real name from the GEOCS field of the password file, and the address that the mail is forwarded to, if the mail is forwarded, the aliases defined on the system to include the decode alias which allows the intruder to overwrite any file that is writable by the owner of the alias, or the root or postmaster address and where their home system is. Having the decode alias allows the intruder to put **.rhosts** files in users' home directories, or replace the alias database. The SMPT and NNTP (Network News Transport System) will also provide an intruder data about the computer system hardware, operating system revision, sendmail version, or version of the program operating on the system through the sendmail daemon;[431]

[430] A daemon is a background process capable of initializing other processes with little or no input from the user. Daemons typically provide services (such as printing or server advertising), administrative functions, or access to the host file system in the UNIX environment (Shafer, 136).

[431] Pipkin, 24, 33, and 97-104.

"Sendmail" is a very complex program that has a long history of security problems. The complexity of the sendmail software and the evolutionary development of the program have left it with numerous holes that are continuously being found and patched (Pipkin, 33-34).

- Look for **telnet**, **rlogin**, and **ftp** packets that will contain the user name and associated password since they are passed across the network in clear text; and[432]
- Look for instances of time-based scheduling (CRON) of jobs to substitute their own process and gain the privileges of jobs.[433]

Another convenient technique for a potential intruder to gain additional privileges once on a system is to exploit file permission vulnerabilities. An intruder can exploit the vulnerabilities of the permissions of both the targeted file and its parent directory and the variations in the implementation of special permission bits and access control lists. Some of the more common permission problems that have and more than likely will be again exploited by a knowledgeable intruder are:

- The built-in shell command **unmask** which is used to set file creation permissions.
- Inappropriate permissions on directories that compromise not only the data in that directory, but also all the data in all the subdirectories below it.[434]
- Inappropriate permissions on the home directory[435] that would allow an intruder to write into the home directory where he can alter program startup scripts and configuration files that will allow him to masquerade as the user or gain the user's privileges.

[432] Pipkin, 48.

In the standard UNIX environment, user data can be encrypted, but the login names and passwords that are part of the control environment cannot (Pipkin, 49).

[433] A potential intruder can use permission problems with the CRON jobs directory or with any of the processes started from CRON (Pipkin, 52).

[434] The higher in the directory tree, the more data comprised.

[435] The home directory is the directory assigned when a user logs in, maintains the startup and configuration files for any programs run during that session, and is the location generally used for any work in process during the session (Pipkin, 56).

- Inappropriate device file permissions that allow a potential intruder to gain access to the data on a device and, subsequently, possible control of the entire system.
- Inappropriate permissions in symbolic link files can give an intruder access to the same file in different directories.[436]

Then, to compound the already bad situation even more, trends toward downsizing from proprietary mainframes to open distributed systems, the demand for the information on office PCs to be shared through servers, and the reduction of staff to contain costs have left many network systems with inexperienced managers managing a greater number of systems with unfamiliar operating environments. The combination of ease of access and an interconnected system with overworked and inexperienced system managers makes the potential intruder's task even easier.[437]

3.4.3. End Game.

Once the unauthorized user gains access to the targeted machine or system, there is little that can be done to stop them before they accomplishes their goals. No matter what their ultimate goals, though, they will be gathering data; utilizing the accessed system's resources; or keeping valid users from accessing those resources.[438]

The intruder may want access just for the strategic location of the system on the network to use as a listening post to monitor activities and all data flowing through the accessed system, for network snooping, or for further connection laundering.[439] Or, the intruder may also want to deny services to valid users by altering access permissions,

[436] Pipkin, 56-58.
[437] Pipkin, xi-xii.
[438] Pipkin, 107.
[439] Pipkin, 107.

altering network configurations, overloading services, or sending invalid data to a server.[440] In the worse case, the intruder may want to direct the accessed system to perform some terrorist or criminal function.

Regardless of the intruder's objective, he generally will want to keep his presence and activity as clandestine as possible so he can stay undetected and use the system at his discretion. If the intruder's objective is to acquire some specific data from a system, it is likely he will try to capture it and flee the system as quickly as possible. The intruder will also strive to leave as little evidence as possible, erase as much evidence of their presence as possible, and make the evidence remaining as confusing as possible. The longer it takes for a system manager to discover their presence, the longer the intruder has to accomplish his goal and better protect his anonymity.[441]

Intruders will use a variety of techniques to mask their connection to the targeted system, including:

- Stealth connections to avoid login recording by the targeted system's accounting log files;
- Masquerading – pretending to be an authorized user of the system;
- **utmp** log modification – changing certain parameters in the **utmp** file to remove evidence of their presence;
- IP spoofing – convincing another computer that an intruder is on a system other than the one on which they actually are;[442] and

[440] Pipkin, 108-109.
[441] Pipkin, 75.
[442] Pipkin, 75-78.

- Executing a child process to replace the parent process in the process table, naming his unauthorized programs the same as legitimate programs on the targeted system, and/or installing a modified version of the process status command that will not report the processes being run on the intruder's purloined account.[443]

However, even using all of the techniques at their disposal it would impossible for an intruder to spend much time on a system without leaving some evidence. Consequently, a savvy intruder will attempt to modify, falsify, or eradicate as much of the evidence as he can by:

- Doctoring Logs – editing simple text log files with a text editor to remove evidence of their presence and activity or deleting log files even though such an action will alert the targeted system's administrator that someone is tampering with their system.
- Crashing the system – deleting everything to remove all evidence of an intrusion,[444] or
- Using erasure programs such as Evidence-Eliminator to erase all evidence of their presence on a system.[445]

[443] Pipkin, 78-79.

[444] Pipkin, 79-80.

[445] Evidence-Eliminator erases any files an intruder created and their histories from a system. The company's website offers software that "will defeat Forensic Analysis equipment. Speed up your PC and Internet Browser, reclaim lost Hard Disk space and professionally clean your PC! Make it safer to use the Internet. Did you know... that your computer is spying on you? Did you know for example that every click you make on Windows 98 Start Menu is logged and stored permanently on a hidden encrypted database within your own computer? Deleting "internet cache and history", will not protect you... your PC is keeping frightening records of both your online and off-line activity. Any of the Web Pages, Pictures, Movies, Videos, Sounds, E-mail and Everything Else you or anyone else have ever viewed could easily be recovered - even many years later! How would you feel if somebody snooped this information out of your computer and made it public? Do your children or their friends use your computers? What have they downloaded and tried to delete? Act now! And stop these files coming "back from the dead" to haunt you! You deserve a far more rewarding and safer Internet experience! Start to enjoy the benefits of a truly clean

3.5. Conclusions.

After reading the discussion of the information infrastructure system's vulnerabilities, one is overwhelmed with the scope and magnitude of its security deficiencies. As postulated in Chapter 1. Introduction and confirmed by the preceding discussion, software and the system properties of "openness" (an open network architecture), interconnectivity, and complexity are all identifiable vulnerabilities contributing to the vulnerability of the integrated system. No single vulnerability, though, is exclusively responsible for the system's overall total vulnerability. With the exception of the open architecture, each is serious in and of itself. However, similar to increasing the efficiency and power of the total system by integrating the benefits of these four properties, each property's vulnerability is multiplied by its combination with the others to increase the gravity of the risk to the total system. Just as a system integrates the properties of each part of the system to maximize its positive potential for the system as a whole, a system as integrates the negative aspects (i.e., the vulnerabilities) of the parts to become vulnerabilities for the system as a whole. The consequence is that security of each subsystem (and the system as a whole) then is dependent upon the security of all other subsystems that comprise the total system.

But, contrary to the implied degree of causal equality of the hypothesis, the research suggests the different vulnerabilities' effects are of different orders of magnitude of risk for the system as a whole. The evidence further indicates that software is the prime, or first order, vulnerability and is overwhelmingly the result of defects in the software. And, with

and faster "Like New" PC! Download today with no risk, guaranteed" (Evidence Eliminator Homepage, Robin Hood Software Ltd., November 21, 2001, www.evidence-eliminator.com).

the degree of integration of software and hardware functions in today's information infrastructure system[446] software defects are more than likely culpable for hardware vulnerabilities.

Without defects in software, neither an intruder's exploitation nor software dysfunction effects (other than those associated with failure of the system's physical structures which was outside the defined scope of this research) would be possible. The other properties (open architecture, interconnectivity, and complexity) serve to facilitate systemic exploitation and to increase the gravity of the exploitation effect. Therefore, from a systems perspective the primary role software defects have in total system risk raise their seriousness to a higher order than the other properties' vulnerabilities. Unfortunately, given the state of software design and development dramatic results in eliminating defects from complex software systems are not anticipated in the short-, and probably the mid-, term.

Interconnectivity facilitates exploitation by only allowing a party or a vulnerability exploitation effect to move from one subsystem to other subsystems within the total information infrastructure system relatively easily. Without software's vulnerabilities such movement would only result in a party being able to get to a targeted subsystem or the effects of an exploited vulnerability to remain in its initially affected subsystem. Software's vulnerabilities then allow the party to access the targeted part of the subsystem [data systems or strategic components (routers or servers)] or to produce the exploitation effects. Such properties indicate that interconnectivity is a necessary, but not a sufficient, condition of the

[446] As the discussion has indicated, software designers and developers are constantly seeking ways to replace hardware functions with software.

total system's vulnerability and is considered a second order vulnerability since it only facilitates, but does not cause, an exploitation.

Complexity, the last property hypothesized as a vulnerability, has to be discussed from two perspectives: functionally and structurally. Both are relevant to my initial hypothesis – that complexity and its increase exacerbate the risk to the system. As demonstrated by the preceding discussion, complexity underlies the problem of software defects and further threatens the system by increasing the likelihood that defects will not be eliminated. Further, increasing complexity removes existing slack from an already constrained mechanistic system making the interdependence of the parts even more highly constrained and limited, i.e., tightly coupled. The end result is that software will continue to include defect vulnerabilities and that exploited vulnerability effects will be more likely to cascade through the system with even less opportunity for humans to intervene to understand, delay, or stop them.

Structural complexity is evident from the conceptual scheme for organization (See Chapter 2. Information Infrastructure System) and from maps of the system. Any organizational scheme without boundaries is bound to be complex and a distributed network; the LII, NII, and GII; LAN, MAN, AND GAN; or some combination of the two schemes are surely abstruse. Structural complexity is even more evident from maps of the system (or, parts of the system since a map of the entire system does not exist because of its scope and complexity). This systemic complexity imbues the system with an inherent vulnerability of unpredictable, sometime chaotic aggregate behavior just by being a large complex system. Yuhai Tu has demonstrated that the Internet (a large complex system) exhibits just such behavior at times.[447] Such functional complexity can lead to "accidents" caused by unanticipated interactions of tightly coupled components that seemingly defy attempts to understand, delay, or stop (Perrow's "normal accidents").

Surprisingly, the research uncovered an aspect of the structural complexity not anticipated: types of network organizational structures. Unfortunately, the type of network the information infrastructure system is organized as (scale-free) leaves it most susceptible to a deliberately targeted attack while, at the same time, best protecting it from random degradation such as that produced by the inherent aggregate behavior of large complex systems. With a scale-free network, an increase in highly connected or vital nodes does not necessarily increase the vulnerability of the network; the fact that there are highly connected or vital nodes is in itself a risk. Degradation of these highly connected or vital nodes relatively quickly cause a scale-free network to malfunction.

Although the scale-free network architecture is a sufficient risk to the availability information assurance objective, it is not a necessary condition. The availability of the network can be denied without directly attacking the highly connected nodes. As is shown in Appendix B. Denial of Service, denial of the information infrastructure system's resources to the system's users can be accomplished by overwhelming individual users, LANs, or MANs.

Complexity, therefore, is not necessary, but may be sufficient to threaten the system. There are enough other causes of software defects (poor design and implementation, poor program management, inadequate testing, market pressures, etc.) to preclude complexity as a necessary condition for software's vulnerability. Likewise, the scale-free network

[447] Tu.

structure is not completely at fault for all network vulnerabilities. An exponential structural network is also vulnerable to a deliberately targeted attack, just less so than a scale-free one, and is even more vulnerable to degradation from random causes than a scale-free one.

Both functional and structural complexity may be sufficient to cause a failure of the system though. Enough functional complexity could prevent a software program from ever being designed, developed, or executable. Albert, Jeong, and Barabasi demonstrated that the degradation of enough of a scale-free network could theoretically substantially diminish its functionality. Therefore, both functional and structural complexity may in and of themselves be sufficient enough to cause a failure of the information infrastructure system.

The open nature of the architecture ("openness") is a third order vulnerability of the system. It allows essentially anyone with the necessary means (which are not terribly expensive, difficult to locate, nor technically difficult to use) access to the information infrastructure system: in effect, universal access to the system. But, the system could also be accessed by an unauthorized user or an authorized user with malicious intent even if access to the information infrastructure system were closed. It would just be more difficult. Further, the open architecture has no effect on vulnerability exploitation effects; the condition does not facilitate nor hinder the movement of the exploited vulnerability's effects throughout the rest of the system. This condition merely facilitates, but does not preclude, a party intent upon maliciousness access to the system. Therefore this condition is neither necessary nor sufficient to cause a vulnerability exploitation and properly should probably not be considered a vulnerability, but only a condition that facilitates the worst-case intruder exploitation. However, when cast in the context of security the open architecture could be consider a vulnerability, albeit it a minor one not of terribly serious consequence, since a closed system would pose only a slight impediment to a determined potential intruder.

CONDITION	NECESSARY	SUFFICIENT	VULNERABILITY ORDER OF MAGNITUDE
Software	Yes	No	1st
Interconnectivity	Yes	No	2nd
Complexity	No	Yes	2nd
Network Organizational Architecture	No	Yes	2nd
Open Architecture	No	No	3rd

Figure 3.4. Comparison of Systemic Vulnerabilities

Given the information infrastructure system's prominent role in the fabric of every facet of the nation's life, the sheer number, scope, intractableness, mix, and ubiquity of the just discussed vulnerabilities cannot leave anyone confident or optimistic about the national security of the nation. Understanding of the system's vulnerabilities' orders of magnitude not only illuminates the degree of seriousness of the different vulnerabilities, but also could possibly suggest a strategy for reducing the risk due to those vulnerabilities. How has the federal government responded to this grave national security problem? The next chapter tries to answer that question by analyzing the national policy response to the information infrastructure system's national security risk

CHAPTER 4

POLICY DIS-ORGANIZATION: AN ORGANIZATIONAL ANALYSIS OF U.S. GOVERNMENT INFORMATION INFRASTRUCTURE SYSTEM SECURITY POLICY

> "The government lacks a comprehensive policy and plan to meet the threat.... Funding, missions, (and) technological expertise ... are scattered among dozens of often competing or secretive federal agencies."[448]

Contrary to the above quote, given the salience of information infrastructure system security to U.S. economic well-being and national security one would expect to find a well-reasoned comprehensive security policy to protect the system. Vulnerabilities of the information infrastructure system as a risk to U.S national security have been included in every annual national security strategy since 1992. As noted in Chapter 1. Introduction, President Clinton finally identified that vulnerabilities of the information infrastructure system posed **significant** risks to the national security of the nation in the National Security Strategy in 1995. The 2000 national security strategy, A National Security Strategy For a New Century, included protection of U.S. critical infrastructures, to include the information infrastructure, as in our **vital interest** and, therefore, important to the survival, safety, and vitality of our nation. The strategy goes on to state "we will do what we must to defend these interests, including, when necessary and appropriate, using our military might unilaterally and decisively."[449]

As indicated by the previous chapters, the issue of information infrastructure system security is extremely complex. The inherent complexities of the system that have been discussed in previous chapters include:

[448] "Panel Warns U.S. on Terror," Pittsburgh Post-Gazette, July 15, 1999, A-1.

[449] United States White House, A National Strategy For a New Century, Washington, D.C., December 1999.

- the technical nature of the system's components and the rate of that technology's advancement;
- the information infrastructure system's design (open architecture and connectivity);
- the information infrastructure system's relationship with the other critical infrastructure systems (interconnectivity);
- the nature of the data transmitted over the system (private, public, classified, and/or unclassified) and how to protect it, if at all (information assurance security objectives[450]); and
- the different types of threats to the system (hacker, terrorist, criminal, or nation) and the ambiguity of determining from where that threat originates, whether it be domestic or foreign (uncertainty).

In this chapter two additional complexities will be introduced, discussed, and analyzed. Both are critical variables for information infrastructure system national security policy:

- the stake holders involved: primarily private ownership of most of the system's assets with normal market pressures and government agencies advocating security policy that most likely will adversely impact those firms' ability to react to market pressures; and
- risk avoidance versus risk management security philosophies; intrinsic in any discussion of security because risk avoidance is ingrained in the culture of the

[450] Previously defined in Chapter 1. Introduction.

traditional national security and law enforcement agencies conflicting with the more contemporary commercial concept of risk management.

My initial intent was to use the information assurance objectives of confidentiality, availability, integrity, authentication, and non-repudiation as the framework to analyze U.S. information infrastructure system security policy and the policymaking process to determine how effective the policy implemented the objectives. However, much to my surprise I found that **NO** comprehensive policy existed to analyze,[451] at least not in the public domain.

How can the United States not have an information infrastructure system security policy, especially since the National Research Council, the National Communications System, and the President's National Security Telecommunications Advisory Committee all alerted the nation to the vulnerabilities of the system as early as 1989.[452] Even the

[451] The National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue not withstanding. This document, by its very title, intentionally or unintentionally, sets the same low expectations as a new computer program version 1.0 release: that faults will be discovered during implementation and it will not be the final version. President Clinton admits as much in his introductory letter when he says "the plan for cyber defense will evolve and be updated as we deepen our knowledge of our vulnerabilities and the emerging threats." Richard Clark, National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, also admits the plan "does not lay out in great detail what will be done to secure and defend **private sector networks** (emphasis added by author), but suggests a common framework for action." Unfortunately for security of the information infrastructure system, private sector networks make up the overwhelming majority of the system. The plan is more like a roadmap of what the administration would like to do and where it needs to go.

[452] United States Department of Defense, Report of the DSB Task Force on Information Warfare (Defense), Section 2.4, "Threat."

"A serious threat to communications infrastructure is developing. Public communications networks are becoming increasingly vulnerable to widespread damage from natural, accidental, capricious, or hostile agents." John C. MacDonald, head of the 1989 National Research Council study of the telephone system, said, "the entire system interlocks in such a way that failure anywhere potentially could shut down the entire network" (National Academy of Sciences, Growing Vulnerability of the Public Switched Network).

Although the 1989 NRC report was primarily concerned with the public switched network, the same NRC board, the Computer Science and Telecommunications Board, issued a report in 1990 that echoed the same sentiments for the entire information infrastructure system. "We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable to the effects of poor design and insufficient quality control, to accidents, and

National Security Council (NSC) acknowledged in 1990 in National Security Directive 42 that "telecommunications and information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation.... and shall be secured by such means as are necessary to prevent compromise, denial, or exploitation."[453]

The NSD even specified what the U.S. response to such vulnerabilities should be:

> "A comprehensive coordinated approach must be taken to protect the government's national security telecommunications and information systems (national security systems) against current and projected threats. This approach must include mechanisms for formulating policy, overseeing systems security resources programs, and coordinating and executing technical activities."

The NSD further establishes "initial objectives of policies, and organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation." Unfortunately, this specified approach has not been followed during the intervening years and, consequently, at the end of 2000 the United States still has no comprehensive national information infrastructure system security policy.

This chapter will examine why such a policy for, by its own admission, one of the most serious current risks to its national security, still has not been established. The primary thrust of the analysis will be to examine the effects of the security policymaking

perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb" (National Academy of Sciences, Computers at Risk: Safe Computing in the Information Age).

[453] National Security Directive (NSD) 42, National Policy for Security of National Security Telecommunications and Information Systems, The White House, Washington, D.C., July 5, 1990, found in National Academy of Sciences, Cryptography's Role in Securing The Information Society (CRISIS), Committee to Study National Cryptography, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, Washington, D.C.: Academy Press 1996, 620.

organizational structure on security policy development and to infer other conclusions from that analysis.

4.1. The Organizational Structure.

The organizational diagram at Figure 4.1. Post-PDD 29 (>1994) IIS Security Policy Organization depicts the different federal departments, agencies, and advisory panels that currently have a statutory or administratively mandated role in information infrastructure system security policymaking and their relationships.[454] Any organization that has some mandated responsibility for one or more of the five information assurance objectives at the policymaking level is included. Neither the diagram, nor does this analysis, attempt to account for those organizations that have implementation responsibility.

The research and development organizations are included because their mandated responsibilities can be interpreted to provide them with the authority to make security policy as will be shown later in the chapter. Further, their research and development agendas and priorities are essential to any information infrastructure system security policy since many of the system's inherent vulnerabilities are technical in nature. The success of these agencies'

[454] Almost all organizations, to include the cabinet level departments and agencies, are intentionally shown as subordinate to the National Security Advisor. It will be pointed out later in the chapter that the National Security Advisor has been designated statutorily and administratively as the authority that reports to the President on information infrastructure system security policy.

POST-PDD 29 IIS SECURITY POLICY ORGANIZATION

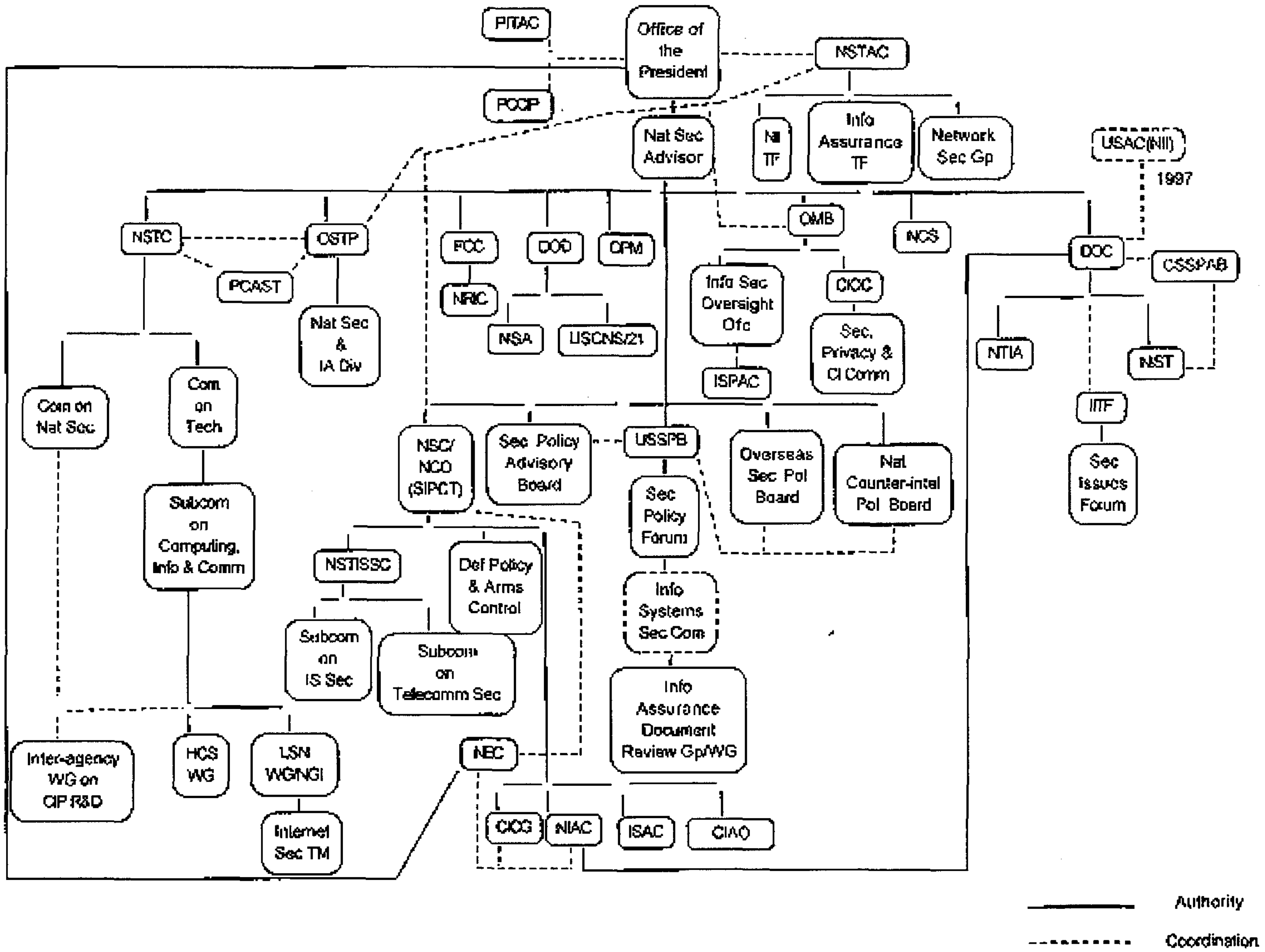


Figure 4.1 - Post-PDD 29 (>1994) IIS Security Policy Organization

R&D efforts, to a degree, determines the success of any policy that is formulated.[455] A more in-depth analysis of the federal R&D efforts is provided in the succeeding chapter, Information Infrastructure System Security and IIS Security R&D Funding.

What is striking at first glance about the picture in Figure 4.1. Post-PDD 29 (>1994) IIS Security Policy Organization is the sheer number of organizations involved. Such a picture, even at a superficial level, does not auger well for efficiency or effectiveness. There are obviously too many players with a primary role to execute successfully any action whether it be planning, development, or implementation.

As early as 1996, the RAND Corp. recommended that a focal point located in the Executive Office of the President be assigned to coordinate U.S. information infrastructure system security policy. The designated office would be responsible for the necessary interagency coordination of the large number of government organizations involved, interactions with Congress, and close coordination with industry.[456] Without some definition of authority and superior-subordinate responsibilities, one would expect

[455] Both the national security strategy for 2000 (United States White House, A National Security Strategy for A New Century, Washington, D.C., December 1999) and Defending America's Cyberspace: The National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue recognize the importance of research and development funding for enhanced security of the information infrastructure system. The national security strategy calls for "increased Federal R&D in information security" (United States White House, A National Security Strategy For a New Century, 18). The national plan for information systems protection devotes an entire program (Program 6: Enhance Research and Development in Support of Programs 1-5) that "establishes research requirements and priorities needed to implement the Plan, ensures their funding, and creates a system to ensure that our information security technology stays abreast with changes in the threat and in overall information systems" (United States White House, Defending America's Cyberspace: The National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue Washington, D.C., 2000).

[456] Molander, Riddile, and Wilson, 7.

I contend that such a finding by RAND was unnecessary since such a responsibility is part of the National Security Advisor's innate duties as granted and defined by the National Security Act of 1947. A more relevant finding by RAND might have been to recommend clarification of the duties of the Assistant to the President for National Security.

Halperin's finding "that all organizations seek influence"[457] to work against coherent, comprehensive action. Unfortunately, Halperin's finding generally does obtain in this case, but not completely in all cases.

Even at the cabinet and independent agency level, the number (13) of departments or agencies is overwhelming. However, a total of 31 organizations have some statutory or administratively mandated responsibility for all or part of information infrastructure system security policy development complicating matters even more. Some have direct statutory or administrative authority (e.g., National Security Advisor) while others have a more derived authority (e.g., OMB). In addition, there are 18 organizations mandated to serve as advisors on the issue to various other organizations (See Appendix D. Organizational Responsibilities and Authorities for the responsibilities and authorities for all organizations included in Figure 4.1. Post-PDD 29 (>1994) IIS Security Policy Organization.

With such an organizational structure, it would be difficult to develop a coherent policy even if the other previously mentioned complexities at the beginning of the chapter could be resolved or somehow excluded from the policymaking process. As the Joint Security Commission II noted in 1999, "This 'everyone is in charge' arrangement means that no one has responsibility for meeting the vital needs for INFOSEC (information security) for national security."[458]

[457] Morton Halperin, Bureaucratic Politics and Foreign Policy, Washington, D.C.: The Brookings Institute, 1973, 26, and Morton H. Halperin, "Why Bureaucrats Play Games," Foreign Policy 2 (Spring 1971), 74.

Allison also defines the same behavior for organizations in Essence of Decision: Explaining the Cuban Missile Crisis, but Halperin also explains the exceptions to this general rule of organizational behavior as will be shown later in the chapter.

[458] United States Joint Security Commission, Report of the Joint Security Commission II, Washington, D.C., August 24, 1999, "Organizing INFOSEC in the Government."

As will be shown later in the discussion, this apparent diffusion of authority ("everyone in charge") did, in fact, contribute to the paucity of coordinated, coherent national policy developed during the 1990s. Without a designated policy decision maker, some policy makers and organizations

- were content to do little in a classic example of the "free-rider" phenomenon,
- bureaucratic competition between contending policy organizations increased to the point of stagnation, and
- no one established burden-sharing responsibilities.

Admittedly, some organizations were more active or accepted a larger role than others.

As with any other organizational chart though, the first blush look is only a small part of the total picture. Upon closer examination, one discovers many other factors that precluded efficient formulation of an effective policy. What is most disturbing about the existing organizational structure is that most routine administrative tasks that could have made a difference were neglected: reconciliation of new and existing statutory and administrative authorities. New legislative and administrative authorities were promulgated without rescinding or adjusting the existing mandates creating increasingly complex, overlapping, and contradictory organizational responsibilities.

By the early 1990s the entire information infrastructure system security organizational structure was already too confusing for any remedy except complete overhaul. The Joint Security Commission reported in 1994 that there is a "profusion of policy formulation authorities, all of whom are addressing essentially the same issues" at the national level.[459] Unfortunately, this did not happen even though Presidential Decision Directive 29, Security Policy Coordination, was an attempt to do just that. The Directive, a direct response to the Commission's earlier finding and recommendation, called for realigning all U.S. national security processes to address better the changed post-Cold War security environment. The Clinton administration, though, continued to issue executive branch mandates with little thought to previous authorities resulting in the current organizational structure depicted in Figure 4.1. Post-PDD 29 (>1994) IIS Security Policy Organization.

In 1999, the reconvened Joint Security Commission II discovered to its amazement that the situation still had not changed much even though the Principles Committee of the National Security Council had been mandated to produce a report for the President "evaluating the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations" within 180 days of publication of PDD 63, Protecting America's Critical Infrastructure (May 22, 1998). As of this date, no such report exists that can be located unless the National Plan for Information Systems Protection, Version 1.0 is intended to satisfy this mandate. This is probably not the case since the document does not appear to successfully fulfill all of the mandate's requirements.

Today, the National Security Telecommunications and Information Systems Security Committee (NSTISSC), Office of Management and Budget (OMB), National

[459] "The current structure of authorities for protecting (information) technology is incoherent and self-defeating.... Attention to the question of authorities ... (is) the minimum starting point necessary to ensure that critical systems will continue to be available to the nation" (United States Joint Security Commission, Report of the Joint Security Commission II, "Conclusion").

Institute of Standards and Technology (NIST), the U.S. Security Policy Board (USSPB), the Critical Infrastructure Protection (CIP) process, and, most recently, the Chief Information Officers' Council (CIOC), along with the previously mentioned NSA, are all developing and publishing information systems security policy that, "although similar, differ sufficiently to create inefficiencies and to cause implementation problems when organizations must coordinate their security protocols and procedures in order to interconnect."[460] Equally startling, several organizations with direct or derived authority appear not to have participated significantly in information infrastructure system national security policymaking.

The Office of Science and Technology Policy (OSTP) could make a convincing case, given its mandate,[461] that it should be the agency responsible for all information infrastructure system policy, including security. Providing added weight to the position that OSTP could, or should, be the agency responsible for IIS security policy, OSTP's National Security and International Affairs Division proclaims on its homepage on the World Wide Web (WWW) that it is responsible for **"science and technology policies in**

[460] United States Joint Security Commission, Redefining Security, Chapter 8, "Information Systems Security."

[461] Its statutory role (42 USC 6614) is to serve as the "source of scientific and technological analysis and judgment for the President with respect to major **policies** (emphasis added), plans, and programs of the Federal government" and "to define coherent approaches for applying science and technology to critical and emerging national and international problems and for promoting coordination of the scientific and technological responsibilities and programs of the Federal departments and agencies in the resolution of such problems (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-101).

In addition, the Director of OSTP is assigned responsibility by Executive Order for directing the exercise of the President's wartime authorities over domestic telecommunications. In emergencies or crises in which the exercise of the President's war power functions is not required or permitted by law, the OSTP Director is also charged with the responsibility to advise and assist the President and Federal departments and agencies with the provision, management, or allocation of telecommunications resources (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-101).

the national security and the commerce-security nexus," (emphasis added) to include critical infrastructure protection and information security,[462] national security/emergency preparedness, emergency telecommunications, the National Communications System, The National Security Telecommunications Advisory Committee, Continuity of Government programs and infrastructure protection programs.[463] However, for whatever reason(s) OSTP seems to have chosen to restrict its role to research and development.

A similar case could be constructed for the National Science and Technology Council (NSTC), a Cabinet level council established by EO 12881 on November 23, 1993 and chaired by the President. The Council is the "principle means for the President to coordinate science, space, and technology policies across the Federal Government."[464] Although primarily a science and technology R&D management organization, the NSTC does provide an interagency strategic management system to foster teamwork and enhance the ability to identify opportunities for interdisciplinary solutions. In addition to other responsibilities, President Clinton directed the NSTC to:

- Coordinate the science and technology policymaking and implementation process across Federal agencies;
- Ensure that science and technology policy decisions are consistent with the President's stated goals; and

[462] United States Office of Science and Technology Policy, National Security and International Affairs Division Web Page, http://www.whitehouse.gov/WH/EOP/OSTP/Security/html/Security.html

[463] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-101.

[464] See any of the President's Supplements to the Budget, FY 1994-2000 and United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-99.

- Ensure that science and technology issues are considered in the development and implementation of Federal policies and programs. [465]

But, similar to OSTP the NSTC has chosen to restrict its information infrastructure systems activities primarily to research and development, albeit information infrastructure system security R&D.

Similarly, the National Communications System (NCS), an independent agency of the Office of the President similar to OSTP and OMB, has elected not to intrude into the policymaking environment even though it seemingly has the authority to do so. President's Reagan's 1983 NSDD 97, National Security Telecommunications Policy, and 1984 Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, expanded the NCS's Committee of Principles' mandate to act as an executive board for "policy, technical, and programmatic NS/EP (national security/emergency preparedness) telecommunications issues." At the same time, the NCS's National Telecommunications Management Structure (NTMS) provides survivable and enduring telecommunications... to support NS/EP telecommunications requirements across the spectrum of emergencies," to include electronic warfare, terrorism, attack, recovery, and reconstitution.[466]

Finally, the Federal Communications Commission (FCC) could legitimately assert a claim to information infrastructure system security policymaking leadership also, although its primary concern is network reliability rather than security of data. The

[465] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-168.

[466] United States White House, Executive Order (EO) 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, Washington, D.C., April 3, 1984.

Commission has the mandate to "regulate, license and monitor the operations of communications services (to include digital and analogue applications and transmission facilities) to insure reliable and competitive nationwide and international communications." FCC mandated functions also include ensuring that communications capabilities are provided for the promotion of life and property and for the **national defense** (emphasis added).[467]

It is my assessment that the above organizations have chosen not to exercise a greater role in the policymaking arena because they did not either have or feel that they had enough power to challenge the traditional national security agencies, even though they have been given explicit authority to do so. Alternatively, most of these organizations traditionally are responsible for highly technical functional areas and probably did not believe they had the expertise or experience to perform the national security policymaking issue adequately or comprehensively.

Morton Halperin, in his observations about the federal bureaucracy, adds validity and granularity to the above analysis. Halperin postulates that all organizations involved in policy decisions "examine any proposal to gauge whether or not it would help their particular organization carry out its missions:" " to maintain the capability to perform their mission... or to gain influence in pursuit of ideological concerns or their other objectives."[468] As will be shown later in the discussion, within the total information infrastructure system security policy environment organizations appeared to exhibit Halperin's finding of examining the policy issue. While the traditional national

[467] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-217.
[468] Halperin, Bureaucratic Politics and Foreign Policy, 26-27.

security/law enforcement and the more commercially oriented agencies appeared to have concluded that the policy issue would certainly increase their organizational stature and influence, there were also at least the four organizations just discussed (OSTP, NSTC, NCS, and FCC) that did not elect to engage in the competition for policy primacy.

Halperin also helps explain these exceptions to his general thesis that organizations will generally seek to expand in size and influence. He postulates that it is erroneous to assume that organization simply seek to grow in size.[469] Disputes over policymaking authority become especially bitter (NSA versus NIST) when the issues involved affect the roles and missions of contending organizations and how the contending organizations perceive changes as affecting the organization's "essence."[470]

In those cases of an issue affecting the essence of the organization, an organization will:

- favor policies and strategies that the dominant group within the organization believes will make the organization as they define it more important;
- struggle hardest for the capabilities that it views as necessary for the essence of the organization;
- resist efforts to take away those functions viewed as part of its essence;
- often be indifferent to functions not seen as part of its essence or necessary to protect its essence; and

[469] Morton H. Halperin with the assistance of Priscilla Clapp and Arnold Kantor "The "X" Factor in Foreign Policy: Highlights of Bureaucratic Politics And Foreign Policy," Brookings Research Report 140, Washington, D.C.: The Brookings Institute, 1975, 3.

[470] Halperin defines the "essence" of an organization as the dominant group's (generally career officials) view of the organization's mission and capabilities (Halperin with Clapp and Kantor, 3 and Halperin,"Why Bureaucrats Play Games," 78).

- sometimes attempt to push a growing function out of its domain entirely.[471]

Items 4 and 5, along with Halperin's later observation that "organizations will seek new functions only if they believe that failure to get responsibility for them would jeopardize their sole responsibility in critical areas,"[472] suggest a rationale for OSTP's, NSTC's, NCS, and FCC's reluctance to aggressively seek a leadership role in information infrastructure security policymaking. OSTP and NSTC clearly see their essence as technical research and development (as will be reinforced in Chapter 5. Information Infrastructure System Security and IIS Security R&D Funding); NCS as technical management; and the FCC as regulatory. It is evident from their behavior that all four organizations were indifferent to the security policymaking function and all, through their inaction, tried to keep the growing function of information infrastructure security policymaking out of their domains entirely.

In the case of OSTP, creation of its National Security and International Affairs Division with its obvious information infrastructure system security role can be explained by a difference between contending groups within the organization over the importance of the information infrastructure security policymaking role to the organization. OSTP's

[471] Halperin, Bureaucratic Politics and Foreign Policy, 49-50; Halperin with Clapp and Kantor, 4; and Halperin, "Why Bureaucrats Play Games," 80.

[472] Halperin, "Why Bureaucrats Play Games," 81.

This organizational attitude could also help explain the rancorous dispute between NSA and NIST during the 1990s over responsibility for national security policymaking in information infrastructure security. NSA might have viewed policymaking in this arena as critical to their mission of computer and information systems security and the organization's role in national security policymaking. NIST, at the same time, would probably have viewed information infrastructure systems security policymaking in the more traditional view of trying to gain size and influence by adding a more high profile mission to its portfolio.

subsequent exhibited behavior demonstrates which group's view of OSTP's essence, or essential role and mission, prevailed.

Complicating the analysis even more though, Halperin further postulates that within the national security policy arena organizations fervently believe "that they should and do take stands which advance the national security of the United States." Determining what the national security interests of the nation are is the problem. Many organizations in the process will initially accept the interests of the organization as national security interests, i.e., that the health of the organization is vital to the nation's security.[473] One could argue that the traditional security and law enforcement agencies adopted this attitude and, consequently, were reluctant to reduce their roles in information infrastructure security policymaking even in the face of sustained distrust and resistance from the owners of the system for this reason.

Further, organizations with "missions' (such as NSA) will strive to maintain or to improve their autonomy. This quest for autonomy leads organizations to resist policies or directives that require them to work closely with another organization.[474] It is generally

[473] Halperin, "Why Bureaucrats Play Games," 73.

"Career officials in organizations with national security missions believe that protecting these interests is vital to the security of the United States. They, therefore, take stands on issues that advance these issues and maneuver to protect these interests against other organizations and senior officials, including the President, by designing programs, missions, and policies to reduce incompatibility with organizational interests" (Halperin, "Why Bureaucrats Play Games," 88-89).

Halperin also draws a distinction between "expensive capabilities" and those with "low-cost capabilities." Organizations with "expensive capabilities" will be particularly concerned about budget decisions and budgeting implications of policy decisions while organizations with "low-cost capabilities" will be relatively unconcerned about the budget implications but highly concerned over the immediate implications of specific policy decisions. However, this particular distinction does not seem to add much to the difference between whether an organization exerts a leadership role or the intensity of effort by those organizations that do contend for a leadership role in the case of information infrastructure system security policy (Halperin, Bureaucratic Politics and Foreign Policy, 26-27 and Halperin, "Why Bureaucrats Play Games," 86).

[474] Halperin, "Why Bureaucrats Play Games," 77 and 80 and Halperin, Bureaucratic Politics and Foreign

accepted that NSA, prior to and during this period, was the premier computer/information technology and technical security organization within the U.S. government and, as such, was accorded great autonomy. Such reasoning can be useful in further explaining the rancor of the dispute between NSA and NIST, particularly with the National Security Agency's primary role in safeguarding the nation during the Cold War. As a result, NSA was not inclined to willingly cooperate with or surrender any of its perceived functions to NIST.

As revealing as this picture of the organizational environmental is, even more revealing is the manner in which it evolved. The remainder of this chapter traces the evolution of the current policymaking organizational structure, suggests explanations for its continued existence, and the effects the structure had on information infrastructure system security policymaking.

4.2. Pre-1994 Organization

To most strikingly show the evolution to today's structure, I have chosen 1994, the publication date of Presidential Decision Directive (PDD)/NSC 29, Security Policy Coordination, as an arbitrary division between past and present structure. PDD 29 was formulated specifically to "coordinate, formulate, evaluate and oversee" United States' security policy. The PDD's prescriptive scope included the entire spectrum of national security; information infrastructure systems security policy was only a part of the total, but surely representative of the need to change or clarify the entire post-Cold War national security policymaking structure and process.

Policy, 226-27.

Prior to PDD 29, the information systems security policymaking structure was as portrayed by Figure 4.2. Pre-PDD 29 (<1994) IIS Security Policy Organization (Actual). The most obvious difference between the pre-PDD 29 and post-PDD 29 organizational structures (shown by comparing Figures 4.1. Post-PDD 29 (>1994) IIS Security Policy Organization and 4.2. Pre-PDD 29 (<1994) IIS Security Policy Organization (Actual) is the fewer number of organizations involved in policymaking prior to 1994 even though the PDD was intended to streamline the process. Even so, the pre-1994 number of agencies and their conflicting mandates (See Appendix D. Organizational Responsibilities and Authorities) still dictated ineffectiveness substantiated by a lack of information infrastructure system security policy prior to 1994.

However, a more compelling reason for change was not the number and conflicting responsibilities, but a lack of leadership. Even though Figure 4.2. Pre-PDD 29 (<1994) IIS Security Policy Organization (Actual) depicts the actual organizational structure, Figure 4.3. Pre-PDD 29 (>1994) IIS Security Policy Organization (Perceived) depicts what seems to have been the perceived organizational structure prior to PDD 29.

The U.S. Security Policy Board commented at its first review of information systems security in 1996 that there are "well- intentioned, but fragmented groups, committees, panels, and boards, each trying to deal with some particular aspect or subset of Information Systems Security and closely-related Defensive Information Warfare."[475]

These comments were not so much about the numbers of organizations involved in information infrastructure system security policymaking as the lack of clear, decisive

[475] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-180.

leadership to direct those organizations in the policymaking process. No federal agency appears to have exerted leadership for information security policymaking and taken the initiative to forge a comprehensive information security policy. Consequently, there was both confusion and paralysis in the formal information infrastructure systems security policymaking process.

It is especially disturbing that the Assistant to the President for National Security Affairs, reaffirmed as the "focal point" for information assurance (after a March 1995 NSTAC request for a national central official),[476] seemingly was not willing or able to either produce a security policy or simplify the organizational environment. The National Security Act of 1947, as amended, specifies that it is the duty of the National Security Advisor "to consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security and to make recommendations to the president in connection therewith."[477]

In addition, the National Security Council Staff that is subordinate to the National Security Advisor, in conjunction with the National Economic Council, advises and assists the President by integrating all domestic, foreign, military, intelligence, and economic policies as it affects United States national security. The NSC is the "highest Executive Branch authority that provides review of, guidance for, and direction to the President of

[476] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organization for Assurance, A-91-92.

[477] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-177.

PRE - PDD 29 IIS SECURITY POLICY ORGANIZATION (ACTUAL)

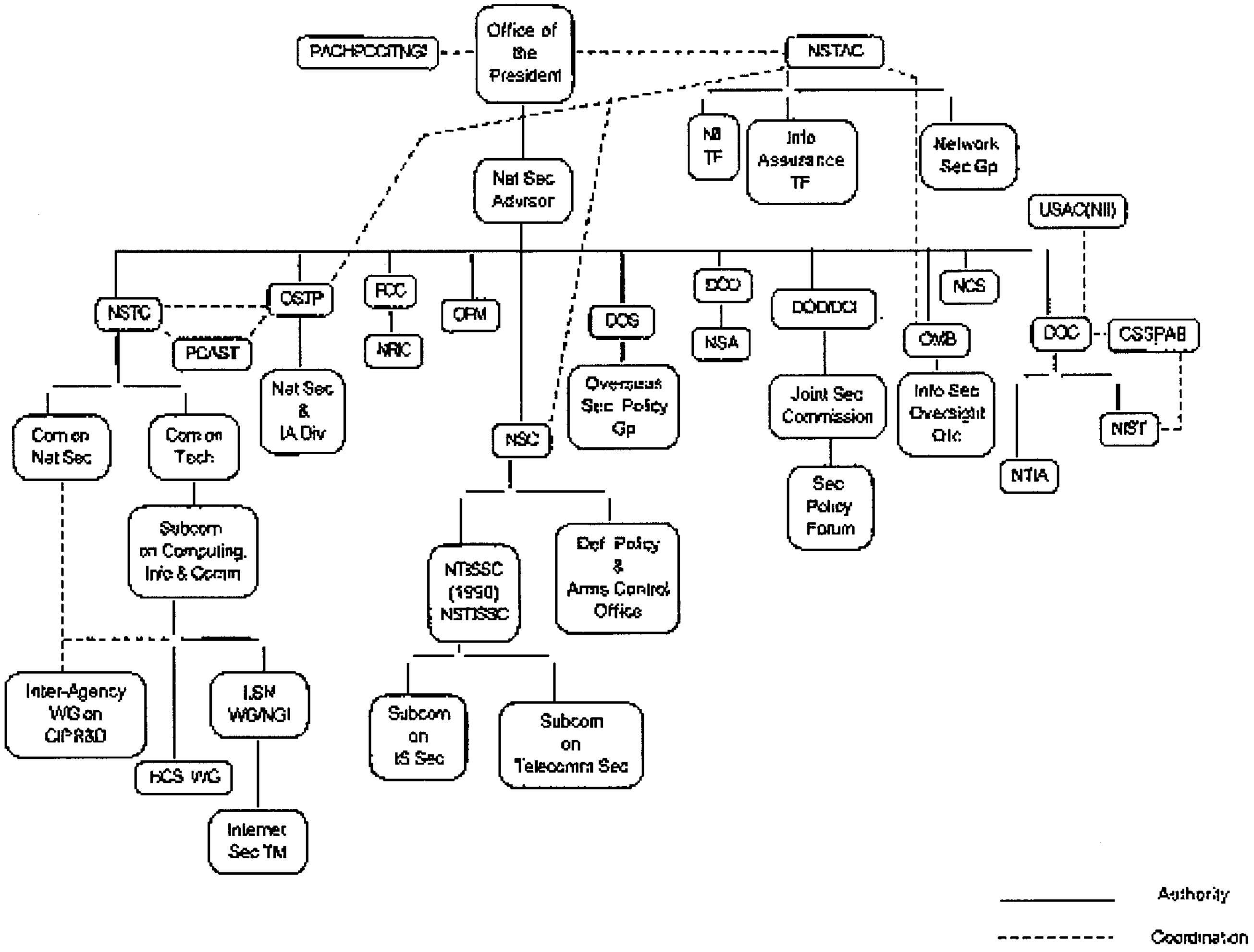


Figure 4.2 - Pre-PDD 29 (<1994) IIS Security Policy Organization (Actual)

all national intelligence, counterintelligence, and special activities, and attendant policies and programs.[478]

With respect to information infrastructure system security, the National Security Advisor had been assigned specific responsibility by Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, on April 3, 1984.[479] In addition to establishing the National Communications System, the Executive Order assigned the National Security Council the responsibility to

> "provide policy direction for the exercise of the war power functions of the President under the National Communications Act of 1934... Advise and assist the President in coordinating the development of policy, plans, programs, and standards within the Federal government for the use of the Nation's telecommunications resources... during those crises or emergencies in which the exercise of the President's war power function is not required or permitted by law; and provide policy direction for the exercise of the President's non-wartime emergency telecommunications functions...; coordinate the development of policy, ... for the mobilization and use of the Nation's commercial, government, and privately owned telecommunications resources, in order to meet national security and emergency preparedness requirements; and provide policy oversight and direction of the activities of the NCS...for the execution of the responsibilities assigned to the Federal departments and agencies."[480]

Further, National Security Decision Directive (NSDD) 145, National Policy on Telecommunications and Automated Information Systems Security,[481] in September 17,

[478] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organization for Assurance, A-91-92 and United States White House, Executive Order (EO) 12333, United States Intelligence Activities, Washington, D.C., December 4, 1981.

[479] Several authorizing documents existed before EO 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions but they are either still classified or not available. The Carter administration produced Presidential Directive (PD) 24, Telecommunications Protection Policy, in 1977, and PD 53, National Security Telecommunications Policy, in 1979, neither of which is available. The Reagan administration also produced NSDD 97, National Security Telecommunications Policy, in 1983 that was concerned with the survivability of the telecommunications systems during war and emergencies and NSDD 84, Safeguarding National Security Information, in 1982 that was more concerned with classification of information and the handling of classified information.

[480] United States White House, Executive Order (EO) 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions.

[481] A memorandum (obtained by the Electronic Privacy Information Center) from Clinton Brooks, Special Assistant to the Director, NSA, provides empirical evidence that NSA purposefully formulated the NSSD to gain bureaucratic "responsibility for the security of all U.S. information systems,... removing (the

National Bureau of Standards, now NIST) from this" (Clinton Brooks, NSSD 145 and the Computer Security Act of 1987, Memorandum obtained by Electronic Privacy Information Center under the Freedom of Information Act, http://www.epic.org/crypto/csa/brooks.gif).

PRE - PDD 29 IIS SECURITY POLICY ORGANIZATION (PERCEIVED)

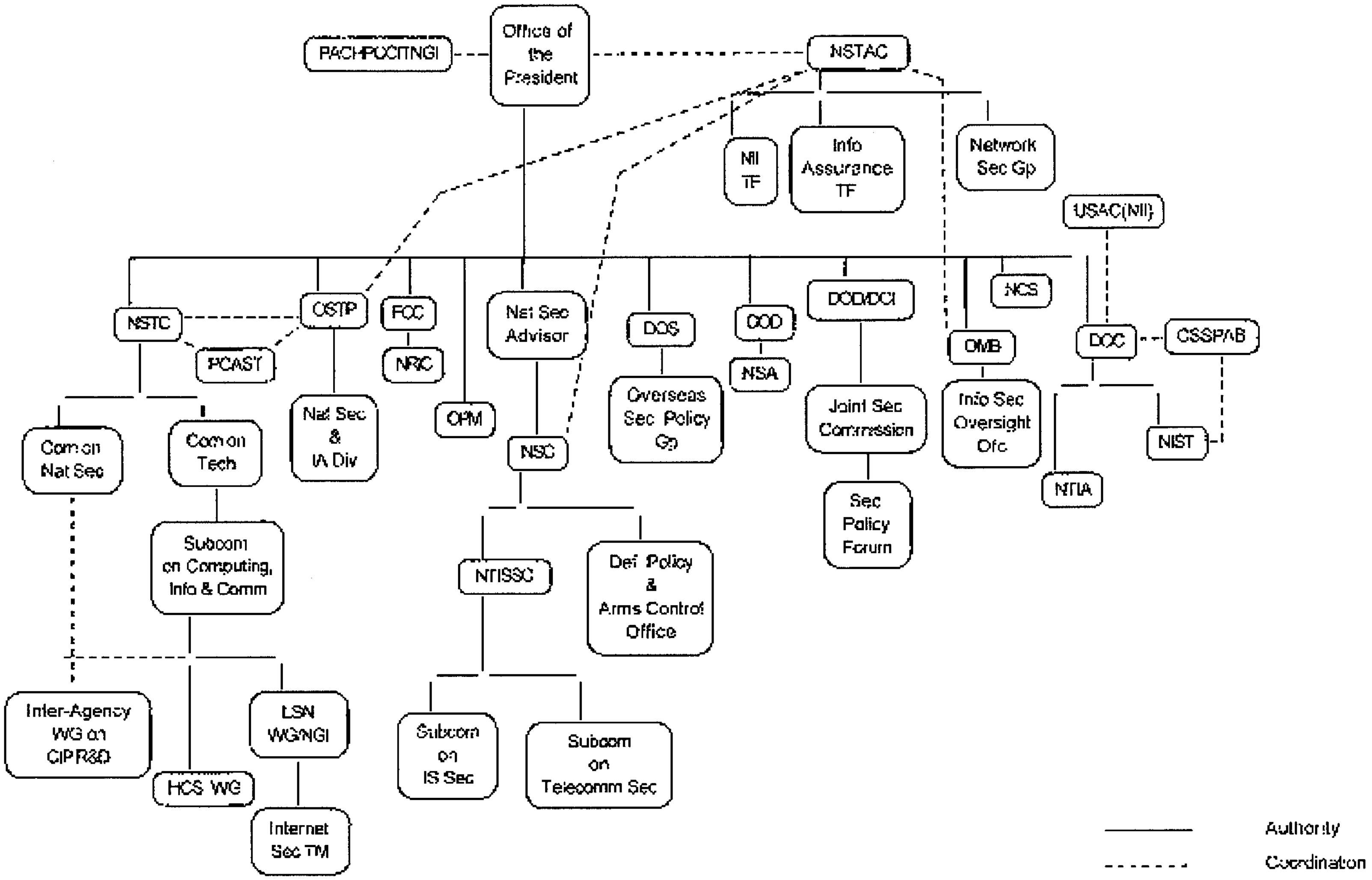


Figure 4.3 - Pre-PDD 29 (<1994) IIS Security Policy Organization (Perceived)

1984, recognized that "traditional distinctions between telecommunications and automated information systems have begun to disappear" and "established initial objectives of policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation;... establishes a mechanism for policy development and dissemination;...."

The NSDD created the National Telecommunications and Information Systems Security Committee (NTISSC), as the **national** authority for information systems security under the oversight of the Systems Security Steering Group chaired by the National Security Advisor. Its authority covered both government classified and sensitive but unclassified and private sector systems.[482] The Secretary of Defense was designated to serve as the Executive Agent of the Government for Telecommunications and Automated Information Systems Security.[483]

Congress, though, objected to the defense and intelligence communities having the degree of authority specified in NSDD 145 over such a large public resource and subsequently passed the Computer Security Act of 1987 (P.L. 100-235) restricting the defense and intelligence agencies' and the NTISSC's roles. Unfortunately, the Computer Security Act of 1987 not only was the first legislation to bind computer and telecommunications resources under a single definition, but it also was probably the

[482] NSDD 145 was quickly followed by a second directive issued by National Security Advisor John Poindexter that extended NSA authority over non-government computer systems (Electronic Privacy Information Center, Computer Security Act of 1987, January 1, 2003, http://www.epic.org/crypto.csa).

[483] United States White House, National Security Decision Directive (NSDD) 145, National Policy on Telecommunications and Automated Information Systems Security, Washington, D.C., September 17, 1984, 17 and United States Joint Security Commission, Report of the Joint Security Commission II, "Organizing INFOSEC in the Government."

genesis of the policymaking morass by creating multiple organizations and divided responsibilities and authorities for information systems security.

The entire episode clearly demonstrates and foreshadowed further bureaucratic competition between the traditional national security departments and agencies and those more closely aligned with industry. Since the enactment of the Computer Security Act, NSA has sought to undercut NIST's authority, most notably through PDD 29, Security Policy Coordination. The Security Policy Board, created by the PDD, recommended that all computer security functions for the government be merged under NSA control.[484]

The Computer Security Act of 1987 strengthened OMB's role in the information security policy arena. It reinforced the original Brooks Act that had conferred responsibility to OMB for "fiscal and policy oversight" of the powers assigned to GSA, NIST, and OPM. The Paperwork Reduction Act further strengthened OMB's responsibility to include "providing direction and overseeing" and ultimately became, in the Clinger-Cohen Information Technology Management Reform Act, "directing and controlling" those agencies.[485] OMB's powers are particularly relevant to this discussion as will be shown later in the chapter.

In 1990, National Security Directive (NSD) 42, National Policy for Security of National Security Telecommunications and Information Systems, tried to resolve the conflicting mandates of the Computer Security Act of 1987. It explicitly defined the

[484] Electronic Privacy Information Center, Computer Security Act of 1987, January 1, 2003, http://www.epic.org/crypto.csa.
[485] United States Joint Security Commission, Report of the Joint Security Commission II, "Organizing INFOSEC in the Government."

responsibility and established the mechanism for ensuring security of "national security systems."[486]

The NSD directed that the government provide for "reliable and continuing assessment of threats and vulnerabilities, and implementation of appropriate effective countermeasures" among other functions. In addition, the NSD established a NSC Policy Coordinating Committee for National Security Communications and Information Systems to "develop policy recommendations." The National Security Telecommunications and Information Systems Security Committee (NSTISSC) (in effect just a renamed NSDD 145 NTISSC) was also established to "develop such specific operating policies, procedures, guidelines, instructions, standards, objectives, and priorities as necessary to implement the provisions of this Directive."

However, instead of clarifying the scope of the responsibilities mandated by the Computer Security Act of 1987, NSD 42 only contributed to the simmering feud between the traditional national security agencies and those more commercially-attuned, management-oriented agencies: principally NSA (and DoD at least tacitly since NSA is subordinate to DoD) and the Department of Commerce's NIST. By designating NSA as the National Manager for National Security Telecommunications and Information Systems Security with responsibility to "act as the U.S. Government focal point for ... telecommunications systems security, and information systems security for national security systems," NSA was authorized to "review and approve all standards, techniques, systems, and equipment related to the security of national security systems." But, NSA

[486] United States White House, National Security Directive (NSD) 42, National Policy for Security of National Security Telecommunications and Information Systems, found in National Academy of Sciences, Cryptography's Role in Securing The Information Society (CRISIS), 621.

was directed to only "coordinate with the National Institute for Standards and Technology in accordance with the provisions of the Computer Security Act of 1987" [487] implying that it had the authority to make information infrastructure system security decisions.

Further obfuscating the policymaking issue, NSD 42 gave the Secretary of Defense, as the Executive Agent of the Government for National Security Telecommunications and Information Systems Security authority to "approve and provide minimum security standards and doctrine for systems subject to the Directive." Since NSA operates under the authority of the Secretary of Defense, this was interpreted to only strengthen NSA's authority since both national security and unclassified information systems were both subject to the directive.

The NSD did try to limit the scope of the directive by narrowly defining the term "national security systems" to include only those communications and information systems operated by the U.S. Government, its contractors, or agents that contain classified information; or that involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that was an integrated part of a weapon or weapons system, or equipment that is critical to the direct fulfillment of military or intelligence missions. However, when one considers the full range of the information infrastructure system the last phrase of the definition can be applied to most means of data transmission.

[487] United States White House, National Security Directive (NSD) 42, National Policy for Security of National Security Telecommunications and Information Systems, found in National Academy of Sciences, Cryptography's Role in Securing The Information Society (CRISIS), 621.

Given the specific authorizations discussed above, it is difficult to understand why there was such a vacuum in leadership. The National Security Advisor clearly was the government official and the National Security Council the government bureaucracy with explicit authority to provide policy leadership for information infrastructure system national security. The NSC even had two policy mechanisms (the NTISSC and the Policy Coordinating Committee for National Security Communications and Information Systems) designated by executive mandate to assist with the process. Each of the legislative and executive authorities discussed were ineffectual attempts by the National Security Advisor and National Security Council to delegate responsibility information infrastructure system national security policy making to other federal government departments and agencies.

Halperin's earlier discussed organizational behavior might have had some role at this early stage, but if so, probably only in a very weak and general way of the organizations involved trying to increase their size and power. Halperin's finding that national security organizations tend to view the missions and goals of their own organization as commensurate with the nation's security goals and objectives might more aptly apply. The traditional national security organizations would see any national security issue as important to both their explicit and implied mission. In this sense, the perception by the traditional national security agencies that the Congress was trying to diminish their role in information infrastructure system security policymaking might be interpreted as an infringement of their essence. Such a perception would prompt determination by these agencies to battle mightily to retain this policymaking function.

Such an argument could explain DoD's attempt to be designated as the federal organization responsible for information infrastructure system security.

More than likely, other factors had a greater role than Halperin's organizational behavioral traits since information infrastructure systems security was an emerging functional issue area more complex than traditional telecommunications security with decision makers having little substantive knowledge of the issue. A more likely possible explanation for the absence of policy leadership by the NSC at this time might be that a perceived definitional distinction between "telecommunications" and "information systems" (which the Computer Security Act of 1987 included under a single definition for the first time) delayed acknowledgement of responsibility.

The policymaking arena was trying to cope with a new issue area as it was still rapidly evolving and did not grasp the implication of computer and transmission systems integration as a completely new paradigm for data availability and use. NSDD 145 and EO 12472, as early as 1984, recognized the conceptual distinction between the two and tried to draw a distinction between them by limiting the responsibility of the NSC to "telecommunications" only. National Security Directive (NSD) 42 adds validity to this interpretation by acknowledging a blurring of an explicit distinction between the two terms even as early as 1990,[488] but did little to clarify the situation. Presidential Review Directive 27, Advanced Telecommunications and Encryption, further supports the

[488] United States White House, National Security Directive (NSD) 42, National Policy for Security of National Security Telecommunications and Information Systems, found in Cryptography's Role in Securing The Information Society (CRISIS), 620.

difficulty that the issue of definition posed for the government as late as 1993 but resolution of the issue was beyond its scope.[489]

The NSC might also have been reluctant to accept responsibility for such a narrow area of national security believing that its organization's mandate should be the broader one of "national security" while "information system security" was only a part of national security and rightfully belonged within the functional purview of more technical agencies. Further, the NSC might have felt that "information system security" was technically too difficult for them and should be left to an organization with more technical expertise. Each, or all, of the offered explanations are plausible but cannot be put forward with certainty. The recorded history does not offer, and no one seems to recall, an explanation for the National Security Advisor's or the NSC's reluctance to accept responsibility and possible leadership.

Another explanation might be that several organizations were concurrently trying to exert their leadership for policymaking, but were unable to achieve primacy. Given normal bureaucratic behavior, such a scenario is also plausible. There is evidence that NSA and NIST were in competition to achieve primacy in the area of information systems security. Both had been mandated missions that could be interpreted as responsible for national information infrastructure system security policy, at least within their specialized areas of confidentiality. Such a prevailing view by the elite or dominant group in each of these organizations would make this functional area a part of each

[489] "Rapid changes in both the telecommunications and computer industries have blurred the traditional gaps that separated these technologies" (United States White House, Presidential Review Directive (PRD) 27, Advance Telecommunications and Encryption, Washington, D.C., 1993).

organization's essence and, as previously discussed, help explain the rancor of the dispute between the two organizations.

The responsibilities specified in the Computer Security Act of 1987 (P.L. 100-235) stipulate that NSA is responsible for government classified information systems-based data while government unclassified information is the responsibility of NIST. Distinction between the two assigned responsibilities is diminished by the 95+% of government classified and unclassified communications transmitted across public switches (which are not secure) and the quantity of computers in the public domain.[490]

That NSA believed it has overall responsibility for information systems security, one only had to access the homepage on its website. The Introduction to its website proclaimed, "The National Security Agency (NSA) is charged with ... the information systems security, or INFOSEC, mission to provide leadership, products, and services to protect classified and unclassified national security systems against exploitation through interception, unauthorized access, or related technical intelligence."[491]

Even with the division of responsibilities between NSA and NIST in the Computer Security Act of 1987, NSA developed a "concept through which it will respond to issues of personal privacy, business privacy, law enforcement... through a key escrow concept"[492] which NIST no doubt took as encroachment on its area of

[490] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-75.

[491] United States National Security Agency, Homepage, http://www.nsa.gov, January 14, 2000.

NSA, to an extent, is correct in asserting such a claim based on historical mandates and its traditional primacy in "signals" intelligence within the U.S. intelligence community. United States White House, Executive Order (EO) 12333, United States Intelligence Activities, directs NSA to "execute the responsibilities of the Secretary of Defense as executive agent for communications security of the U.S." and to "conduct R&D to meet the needs of the U.S. for signals intelligence and communications security."

[492] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and

responsibility. NIST, for its part, was working on development of the Data Encryption Standard and the Digital Signature Standard that could be reciprocally interpreted by NSA as an encroachment of its responsibility.[493]

However, the dispute between the two organizations would seem to be more than the typical bureaucratic organizational dispute over responsibilities and power. Upon closer scrutiny, at least part of the dispute could be also attributed to the different climates, or cultures, in which each of the organizations is accustomed to working. These different cultures reflect each organization's intrinsic essence: NSA's national security essence and NIST's commercial bias. The conflict between the NSA and NIST also serves as a proxy for the larger conflicting interests of information systems corporate owners allied with those agencies traditionally concerned with promotion of American commerce and efficiency (DoC, NIST, OMB, etc.) and the traditional national security organizations and federal law enforcement agencies (DoD, CIA, NSA, DoS, DoJ, FBI).

Evidence indicates that this to be the case. USA Today reported on March 9, 2000 that "other government agencies are refusing to work with the NIPC (National Information Protection Center), privately pointing to the FBI's longstanding reputation for not sharing (information) well with others." The Department of Defense is the only Cabinet-level agency, other than the Department of Justice, represented at the NIPC. The Secret Service and other Department of Treasury organizations and the Department of Transportation all refused to participate although they are designated to have

Organizational Considerations for Assurance, A-75.

[493] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-109.

representatives at the center. The Department of Energy is also not represented even though it is supposed to play a major role.[494]

NSA is the traditional national security organization with perhaps the greatest secrecy about its functions and methods of operation. More importantly as a traditional national security organization, NSA is focused on obviating threat and vulnerability risks regardless of cost.

NIST, on the other hand, is a subordinate organization within the Department of Commerce whose primary mission is "to promote U.S. economic growth by working with industry to develop and apply technology, measurements, and standards ... to improve product quality, to modernize the manufacturing process, to ensure product reliability, and to facilitate rapid commercialization of products based on new scientific discoveries."[495]

As an organization familiar with industry's pressures and the mission to assist industry's growth, NIST's concept of security would be more akin to the commercial sector's: risk management without overly adversely impacting efficiency, time, and cost in getting a product to market. In fact, there is evidence that NIST's concept of security consists of "identifying some incremental approach which has cost realism. Policy issues for the private sector must be translated into cost."[496] Such a concept is extremely salient to the information technology industry, and some within government, which believe that

[494] M.J. Zuckerman, "Asleep at the Switch? How the Government Failed to Stop the World's Worst Internet Attack," USA Today. March 9, 2000.
[495] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-109.
[496] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-110.

the cost of information systems crime is outweighed by the benefits accrued from computerization and ever-expanding use of the information infrastructure system.[497]

The fact that NIST was also developing an "Information Technology Laboratory with special emphasis on security, was acting as a resource clearing house for computer security matters, published a computer security handbook, and was attempting to establish a computer emergency response capability to aid Federal departments and agencies"[498] did little to convince NSA that NIST was not encroaching on its traditional national security turf. The dispute between the two agencies was so entrenched that a Memorandum of Understanding (MOU) explicitly defining the different responsibilities of each agency under the provisions of the Computer Security Act of 1987 (P.L. 100-235) was executed in March 1989.[499]

The long, continuing dispute over cryptological standards and the freedom to export cryptographic devices[500] likewise can be viewed as a microcosm of the tension between the information systems industry/management and business-oriented agencies alliance and the traditional national security organizations and their law enforcement allies. Ignoring individual privacy for the sake of this discussion, the crux of the cryptography issue is the desire of industry to manufacture extremely advanced

[497] United States Congress, House of Representatives, "Opening Statement of Chairwoman Constancy A. Morella," Computer Security, Hearing, Subcommittee on Technology, Committee on Science, 1st Session, 105th Congress, February 11, 1997.

[498] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-110.

[499] United States National Security Agency/National Institute of Standards and Technology, Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235, 24 March 1989.

[500] United States White House, Presidential Review Directive (PRD) 27, Advanced Telecommunications and Encryption, initiated the formal government review process to examine cryptography issues in 1993.

cryptographic hardware and software for worldwide consumption contrary to the desires of the nation's law enforcement community and traditional national security agencies. Although almost every, if not every, study of the subject has recommended no export controls on such cryptologic devices,[501] the issue still has not been definitely decided.

The government's current position is most elegantly stated in the 2000 national security strategy:

> "the United States Government carefully controls high technology exports by placing appropriate restrictions on the sale of goods and technologies that could be used for military purposes or other wise impair our security. Some of this technology has direct or indirect military applications, or may otherwise be used by states or transnational organizations to threaten our national security."

Encryption is one of those "high technologies" the government deems necessary to control.[502] However, the Clinton administration announced its intention to ease the export restrictions September 16, 1999 along with a draft Cyberspace Electronic Security Act of 1999,[503] but reneged on that announcement several days later.[504]

The latest in the encryption debate occurred January 12, 2000. The Clinton administration announced new regulations proposed by the President's Export Council's Subcommittee on Encryption abandoning nearly all export controls on hardware and software vital to assuring the privacy of Internet users. The new rules were available for

[501] The National Research Council's Committee to Study National Cryptography Policy recommended in their 1996 report, Cryptography's Role In Securing the Information Society, after the most thorough and comprehensive examination ever that export controls should not be imposed. The Defense Science Board in its 1996 Report of the Defense Science Board Task Force Information Warfare - Defense (IW-D) similarly recommended no export controls be imposed. The list could be much longer but these two reports are the most comprehensive on the subject and the most widely respected.

[502] United States White House, A National Security Strategy For a New Century, 23-24.

[503] United States White House, Administration Updates Encryption Export Policy, Fact Sheet, Office of the Press Secretary, Washington, D.C., September 16, 1999.

[504] "U.S. to Relax Restrictions on Encryption Technology," Wall Street Journal, New York, September 16, 1999, B6.

public comment for 120 days after which a final revised regulation was to be published.[505]

In reality, the cabinet-level organizations of Figure 4.2. Pre-PDD 29 (<1994) IIS Security Policy Organization (Actual) each exercised some initiative within their narrow functional areas (as indicated by the Security Policy Board's earlier comments), at times propelled by the subordinate organizations most responsible for the function. The most obvious example is the Department of Defense with its continuing (and by far, most extensive of all the agencies) effort to address the issue of information infrastructure system security, NSA with its emphasis on confidentiality issues, DoS with overseas information security, and NIST with overarching responsibility for unclassified information infrastructure and standards.

At the same time, some of these organizations realized that the issue of information system security was larger than one agency and would require coordination across the spectrum of agencies with a mandate for information system security. However, none of the organizations apparently felt it had the authority, or could not generate enough consensus for its authority, to organize the entire information system security policymaking apparatus for coordination. As a result, ad hoc inter-agency coordination groups, especially at the lower functional levels, materialized without explicit executive branch authorization.

The most prominent, but not the only one, was the Joint Security Commission created by the Secretary of Defense and Director of Central Intelligence specifically to

[505] United States Department of Commerce, Commerce Announces Streamlined Encryption Export Regulations, Fact Sheet, Washington, D.C., January 12, 2000.

review their own security practices and procedures and to develop a new approach to security that "would assure the adequacy of protection within the contours of a security system that is simplified, more uniform, and more cost effective."[506]

The Commission concluded that, although its charter limited the review to the Defense and Intelligence Communities, "the problems of fragmentation and inconsistency in security policy development, implementation, and oversight" were government-wide and "must be resolved in order to make meaningful improvements in the overall effectiveness of U.S. Government security."[507] At the same time, the NSC issued PRD 29, National Security Information, to specifically review EO 12356 and other directives pertaining to protection of national security information with a view toward drafting a new Executive Order for information protection.[508]

The Commission in its final report first and foremost recommended that the nation change from a risk avoidance to a risk management strategy of protection that "considers actual threats, inherent vulnerabilities, and the availability and costs of countermeasures as the underlying basis for making security decisions."[509] The Commission also found that information systems security required increased attention because information systems technology is evolving at a faster rate than information systems security technology. The current "policies were outdated, conflictual, and ineffectual; the strategies for obtaining necessary information systems security technology ineffective; mechanisms for obtaining timely threat information and inherent

[506] United States Joint Security Commission, Redefining Security.

[507] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A175.

[508] United States White House. Presidential Review Directives (PRD) 29, National Security Information, Washington, D.C., April 26, 1993.

[509] United States Joint Security Commission, Redefining Security.

systems vulnerabilities poor; and the general readiness in terms of awareness and training inadequate." [510]

The Commission further recommended that a "systems approach" be adopted to replace the current practice of "placing the responsibility for security (of information technology assets) on each of the security disciplines (physical, electronic, personnel, etc.) that created multiple layers of security with little added value." This separate security discipline responsibility for information infrastructure system security was particularly onerous for industry. The commercial sector was required to comply with a bewildering array of requirements that far exceeded the requirements used by government agencies and organizations to protect the same information.[511]

The Commission's "systems" approach further endorsed a change in the paradigm for managing information security from developing security for each individual application, system, and network to developing security for subscribers with worldwide utility, and from protecting isolated systems to protecting systems that are connected and depend upon an infrastructure neither owned nor controlled by the government,[512] in effect, protecting whole of the information infrastructure system described in Chapter 2. The findings and recommendations of the Commission led directly to Presidential Decision Directive 29 and its attempt to streamline government-wide national security policymaking.

[510] United States Joint Security Commission, Redefining Security.
[511] United States Joint Security Commission, Redefining Security, "Executive Summary."
[512] United States Joint Security Commission, Redefining Security, Chapter 8, "Information Systems Security."

4.3. Post-1994 Organization.

With the publication of Presidential Decision Directive 29, Security Policy Coordination, the Clinton administration intended to correct problems with the entire U.S. national security structure, to include the information infrastructure systems security structure.[513] Such a bold move was necessary for at least three reasons:

- the collapse of the Soviet Union and subsequent change in the global security environment changed the requirements for U.S. national security policymaking;
- as a result, many of the traditional mechanisms for addressing national security were dated; and,
- the existing information infrastructure system security policymaking structure was much too complex and confusing to produce timely, effective policy.

PDD 29 established a Security Policy Board (depicted in Figure 4.1. Post-PDD 29 (>1994) IIS Security Policy Organization under the National Security Advisor) with the authority to

> "consider, coordinate, and recommend for implementation to the President, through the Assistant to the President for National Security Affairs ... policy directives for U.S. security policies, procedures, and practices... and be the principal mechanism for reviewing and proposing to the National Security Council (NSC) legislative initiatives and executive orders pertaining to U.S. security policy, procedures and practices that do not fall under the statutory jurisdiction of the Secretary of State."[514]

The Board has five committees, to include an Information Systems Security Committee, that address different security disciplines. The newly constituted Board would seem to be the ideal structure at the right time to untangle the United States' maligned

[513] United States White House, Presidential Decision Directive/National Security Council (PDD/NSC) 29, Security Policy Coordination, Washington, D.C., September 16, 1994.
[514] United States White House, Presidential Decision Directive/National Security Council (PDD/NSC) 29, Security Policy Coordination.

national security policymaking structure. Unfortunately, the earlier analysis of conflicting, overlapping, and unrescinded authorities still obtains. The federal government never completed the administrative task of defining roles and missions within the new policymaking structure nor of rationalizing the authorities. Even with the Board's mandate to revamp and overhaul the entire national security policymaking environment, the situation is more confusing than ever, as seen by Figure 4.1. Post-PDD 29 (>1994) IIS Security Policy Organization.

However, following the JSC's report there was a growing awareness of the information infrastructure as a system instead of individual components, what the system meant for information security, and criticism of the federal government's information technology security policymaking processes.

- The Defense Science Board's report, Information Warfare – Defense, warned of the risks of information networks to national security and its, Information Architecture for the Battlefield, warned of the risks of information systems vulnerabilities to the U.S. military;
- The President's Commission on Critical Infrastructure Protection (PCCIP) published its report, Critical Foundations: Protecting America's Infrastructures, which further reinforced the dangers of networks and their interconnectedness for all critical infrastructures and affirmed the information infrastructure system's preeminent role in the other infrastructures.
- The Joint Staff published Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance providing a detailed picture of the confused state of information infrastructure systems security.

- The National Research Council's Computer Science and Telecommunications Board published Cryptography's Role in Securing the Information Society, effectively renouncing the administration's existing policy of export restrictions.
- The National Science Technology Council recognized that networks, with all of their attendant problems, are the medium of the future and created their own program component (Large Scale Networking) and a separate information infrastructure security program component (HCS – High Confidence Systems) in the High Performance Computing and Communications R&D Program.
- The Next Generation Internet was created to accelerate introduction of more powerful and versatile networks and networking services.

The National Security Council also published PDD 39, U.S. Policy on Counterterrorism, in which "critical national infrastructures" are identified as probable terrorist targets and directed the Attorney General to review the infrastructure's vulnerability. Unfortunately, the critical infrastructures are not specified nor further discussed other than to assign the Department of Transportation responsibility for coordinating "security measures for rail, highway, mass transit, and pipeline facilities."

The PDD, further, does not assign responsibility for security of the "critical national infrastructures" after the Attorney General conducts the vulnerability assessment other than to direct him/her to "make recommendations to me (the President) and the appropriate Cabinet member or Agency head."[515] One can assume that the PDD 63 effort

[515] United States White House, Presidential Decision Directive (PDD) 39, U.S. Policy on Counterterrorism, Washington, D.C., June 21, 1995.

to assess the critical infrastructure vulnerabilities is the direct result of the PDD 39 tasking to the Attorney General.

Unfortunately, these developments only served to further complicate the policymaking organization and process. The PCCIP's report resulted in Presidential Decision Directive 63, Protecting America's Critical Infrastructure. Instead of seizing the opportunity to improve the organizational structure for all critical infrastructure systems security policymaking (including information), the PDD created a rival mechanism for infrastructure security planning (See Figure 4.5. IIS Security Policy Network for identification of all current IIS security policy processes). A National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism was designated within the National Security Council whose jurisdiction also includes foreign terrorism and threats of mass destruction.

The PDD did establish a structure for cooperating with the private sector through the National Infrastructure Protection Center (NIPC), Information Sharing and Analysis Centers (ISACs), the National Infrastructure Assurance Council (NIAC), the Critical Infrastructure Assurance Office (CIAO), and the Critical Infrastructure Coordination Group (CICG). The NIPC is primarily a reactive law-enforcement organization concerned with "facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts."[516] Since it is primarily an implementation organization, I've chosen not to include it in the policymaking organizational structure shown in Figures 4.1. Post-PDD

[516] United States White House, Presidential Decision Directive (PDD) 63, Protecting America's Critical Infrastructure, Washington, D.C., May 22, 1998.

29 (>1994) IIS Security Policy Organization; 4.4. Post-PDD 29 (>1994) IIS Security Policy Process; or 4.5. IIS Security Policy Network.

The ISACs are planned information sharing organizations between the federal government and different critical infrastructure sectors with appropriate federal agencies designated as the agency responsible for facilitating each sector's participation, e.g., Department of Commerce, information and communications; Department of Treasury, banking and finance; etc. The National Infrastructure Assurance Council (NIAC) is a private/public Presidentially appointed council drawn from major infrastructure providers and state and local government officials and chaired by the National Coordinator "to enhance the partnership of the public and private sectors in protecting our critical infrastructure."[517] The Critical Infrastructure Assurance Office (CIAO) "supports the National Coordinator's work with government agencies and the private sector in developing a national plan, ... and to help coordinate a national education and awareness program, legislative action, and public affairs."[518]

The Critical Infrastructure Coordination Council (CICG) is a federal senior policy level coordinating organization chaired by the National Coordinator composed of representatives of sector liaison and functional coordinators of the lead agencies responsible for arranging private sector participation, other relevant departments and agencies, and the National Economic Council. The CICG is charged to "coordinate the

[517] United States White House, Presidential Decision Directive (PDD) 63, Protecting America's Critical Infrastructure.

Even though authorized by PDD 63, Protecting America's Critical Infrastructure, United States White House, Executive Order (EO) 13130, National Infrastructure Assurance Council, Washington, D.C., July 14, 1999, actually establishes the organization and relationships of the NIAC.

[518] United States White House, Presidential Decision Directive (PDD) 63, Protecting America's Critical Infrastructure.

implementation of PDD 63" through "extant policy structures, such as the Security Policy Board, Security Policy Forum and the National Security and Telecommunications and Information System Security Committee."[519]

Finally, to complicate matters even more, PDD 63 proposes "partnering relationships" (whatever those are) between the Critical Infrastructure Assurance Office (CIAO), the National Security Telecommunications and Information Systems Security Committee (NSTISSC), and the U.S. Security Policy Board. CIAO also "partners" with NIST, OMB, and the Chief Information Officer Council (CIOC) in critical infrastructure matters (of which information infrastructure is one).[520] Instead of clarifying the structure, PDD 63 serves only to obfuscate it further by adding another mechanism for information infrastructure system security policymaking (See Figure 4.4. Post-PDD 29 (>1994) IIS Security Policy Process) for a total of six different distinct processes.

During the same time frame, OMB and, subsequently, DoC and NIST were increasing their roles in information infrastructure system security policymaking through perseverance and focus. OMB's and NIST's authority is statutorily mandated by the Computer Security Act of 1987, and in the case of NIST affirmed by MOU with the NSA. OMB's real authority pervades the Executive Branch because of its management responsibilities and the weight its decisions carry within the Executive Branch.

[519] United States White House, Presidential Decision Directive (PDD) 63, Protecting America's Critical Infrastructure.

[520] United States Joint Security Commission, Report of the Joint Security Commission II, "Organizing INFOSEC in the Government."

I have not tried to include these "partnering relationships" in the Post-PDD 29 organizational diagram. To do so would make the diagrams even more confusing and unintelligible. I have tried to include these relationships in Figure 4.5 - IIS Security Policy Organizational Network, to better show the networked nature of the security policymaking organizational environment.

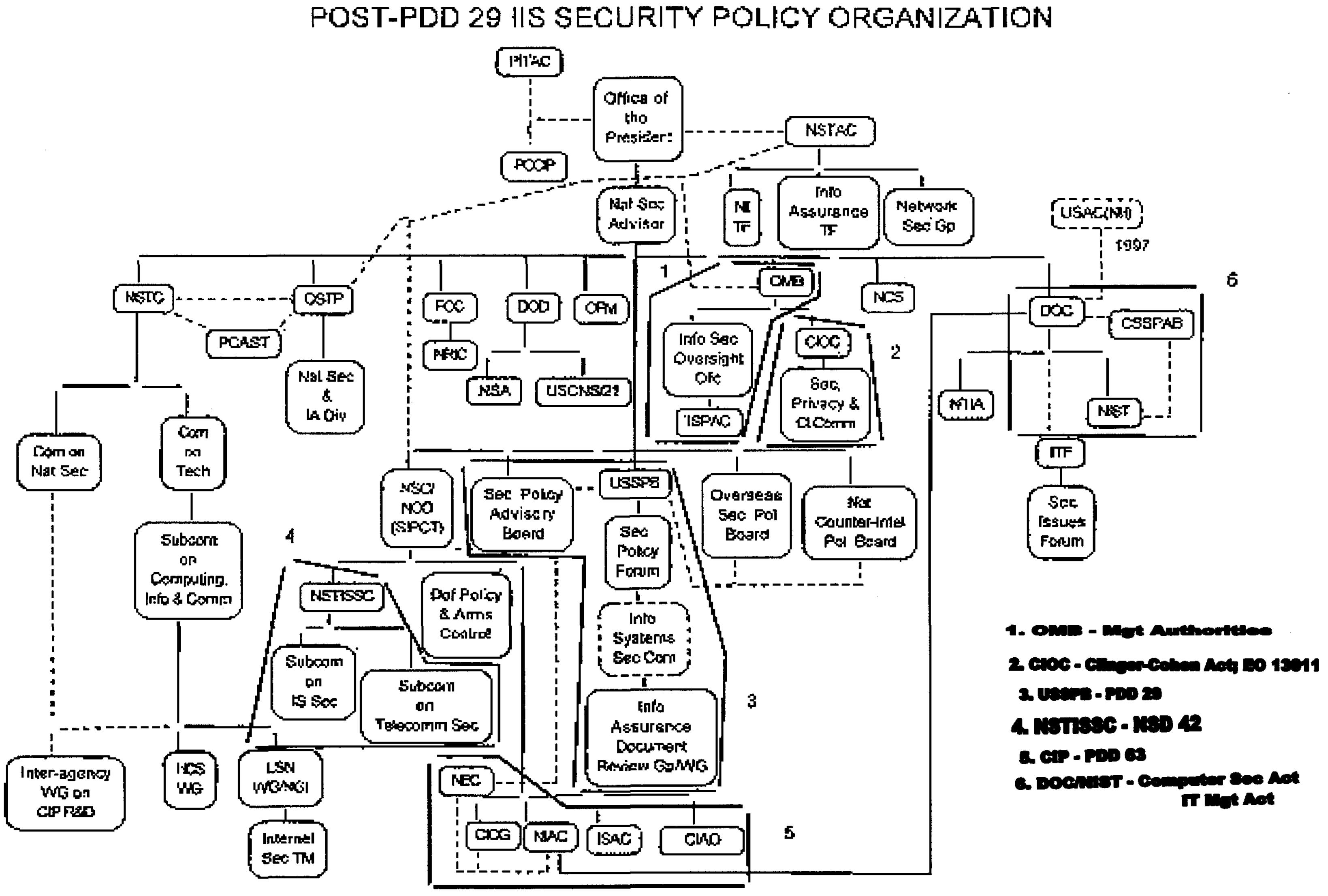


Figure 4.4 - Post-PDD 63 (>1998) IIS Security Policy Process

——— Authority

- - - - - Coordination

The Office of Management and Budget establishes federal policy for the security of federal automated information systems in OMB Circular No. A-130. The circular's goal is to build security into cost-effective management control to complement, but not necessarily impede agency business operations.[521]

However, even with the Computer Security Act's statutory authority OMB must be having difficulty achieving compliance with its directives. Jacob Lew, Director of OMB, felt compelled to publish a memorandum to the heads of all departments and agencies on February 28, 2000 "reminding agencies of the Office of Management and Budget's (OMB) principles for incorporating and funding security as part of agency information technology systems and architectures and of the decision criteria that will be used to evaluate security for information systems investments." Mr. Lew goes on to state that security programs and controls should be consistent with the Computer Security Act, the Paperwork Reduction Act, the Clinger-Cohen Act, OMB Circular A-130, and security guidance issued by NIST for non-national security applications.[522]

Three of the information security policymaking processes identified in Figure 4.4. Post-PDD 29 (>1994) IIS Security Policy Process are subordinate to varying degrees to the Assistant to the President for National Security Affairs[523] making it even more

[521] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-96-97 and Jacob Lew, "Incorporating and Funding Security in Information Systems Investments," Memorandum for the Heads of Departments and Agencies, Office of Management and Budget, Washington, D.C., February 28, 2000.

[522] Lew.

[523]
1. The NSTISSC process established by NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, in 1990;
2. The United States Security Policy Board process established by PDD 29, Security Policy Coordination, in 1994; and
3. The critical infrastructure protection process established by PDD 63, Protecting America's Critical Infrastructure, in 1998.

difficult to understand why there are six processes competing with each other. At the least, these three processes should have been combined, abolished, or somehow integrated to produce a less confusing environment for policy development.

To be somewhat evenhanded, the NSTISSC's mission is much narrower than the other information security policymaking organizations. As previously stated, its mandate is restricted to:

- systems that process classified information or information involving intelligence activities,
- cryptologic activities related to national security, command, and control of military forces, and
- equipment that is an integral part of a weapon or weapons system(s) or is critical to the direct fulfillment of military or intelligence missions.[524]

However, such a mandate could very easily be subsumed under a broader mandate of information infrastructure system security without jeopardizing those specific missions. Such a subsumption would partially simplify the information system security policymaking organizational structure and obviate, to a degree, conflicting responsibilities.

The Chief Information Officer Council (CIOC), authorized by the Clinger-Cohen Act and Executive Order 13011, Federal Information Technology, is an intergovernmental forum that includes the chief information officer (CIO) of every department and agency of the federal government chaired by the Deputy Director for

[524] National Academy of Sciences, Cryptography's Role in Securing The Information Society (CRISIS), 627.

Management of OMB to "improve the design, modernization, use, sharing, and performance of information resources." EO 13011 even mandated the Council "to promote a coordinated, interoperable, **secure** (emphasis added), and shared government-wide infrastructure...."[525]

The CIOC, in conjunction with OMB, has established as a goal government-wide integration of information technology policy development. As part of this vision, the CIOC has published strategic plans for the last three fiscal years.[526]

As if to emphasize both the seriousness of the situation and its willingness to tackle the hard issues, its Security, Privacy, and Critical Infrastructure Committee,[527] as part of the Council's FY2000 Strategic Plan, sees itself as providing leadership, support, and awareness to address the three interrelated areas of security, privacy, and critical infrastructure. It calls for "implementation of security practices within the Federal government that gain public confidence and protect government services, privacy, and

[525] United States Chief Information Officers Council, CIO Council Homepage and United States White House, Executive Order (EO) 13011, Federal Information Technology, Washington, D.C., July 16, 1996.

[526] United States Joint Security Commission, Report of the Joint Security Commission II and United States Chief Information Officers Council, CIO Council Strategic Plan, Washington, D.C., January 1998, http://cio.gov/content/fy1998.htm, ii.

[527] The Security, Privacy, and Critical Infrastructure Committee's Objectives are:

1. Lead the establishment of integrated, government-wide IT guidelines, best practices, tools, training, and proposed policies in areas of privacy, critical infrastructure, and security consistent with OMB Circular No. A-130, Management of Federal Information Resources, Appendices I and III, NIST security guidance, and the Privacy Act. Conspicuous by their absence is any reference to the traditional national security organizations or their role in information infrastructure system security.
2. Support service delivery capabilities of Federal agencies by determining security and privacy approaches that advance appropriate information access, exchange, and protection, and support Electronic Commerce.
3. Promote awareness of security, privacy, and critical infrastructure issues.
4. Establish a leadership role within the CIO community in the implementation of PDD-63, Protecting America's Critical Infrastructure" (United States Chief Information Officers Council, Strategic Plan, Fiscal Year 2000, Washington, D.C., (undated), http://www.cio.gov/content/fy2000.pdf, 6, 26).

sensitive and **national security** (emphasis added by author) information through effective management frameworks."

In addition, the Committee intends to work with OMB and NIST to identify sample or draft policies of security and privacy for use by federal agencies. Such practices, tools, training, and policies will more than likely be more favorably received by the private sector also since they will be "risk-based, cost-effective, and provide sufficient flexibility to accommodate individual agency requirements."[528]

Noticeably absent from this discussion of the CIOC's intentions are the defense, law-enforcement, and traditional national security agencies, most notably NSA. The artificial division created by NSD 42 between "national security" and other security concerns seems to be still in force.

As part of its work, the Chief Information Officers Council has advocated and reviewed plans by all federal agencies for the protection of each agency's respective critical information infrastructure to be implemented no later than May 22, 2003.[529] Its strategic plan envisions coordinating and integrating existing security policymaking groups, assessing and directing ongoing security efforts, and leveraging existing security group resources.[530]

Even though both EO 13011 and the Clinger-Cohen Act have a national security exemption similar to NSD 42's definition of national security systems,[531] the Council

[528] United States Chief Information Officers Council, CIO Council Homepage and United States Chief Information Officers Council, Strategic Plan, Fiscal Year 2000, 1 and 26.
[529] United States Chief Information Officers Council, Strategic Plan, Fiscal Year 2000, 25.
[530] United States Joint Security Commission, Report of the Joint Security Commission II and United States Chief Information Officers Council, Strategic Plan, Fiscal Year 2000, 25.
[531] Limitations (Section 5141) exempt national security systems from the CIOC's efficiency, security, and privacy of federal computer systems responsibilities (Section 5131). National security systems are defined

sees itself as a "focal point for coordinating challenges that cross agency boundaries." To make the point more forcefully, both the Clinger-Cohen Act and the executive order specifically direct the "heads of executive agencies to apply the policies and procedures" established by both mandates "to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in the Act."

The policies and procedures of both mandates authorize the Secretary of Commerce to "promulgate standards, which may be compulsory and binding to the extent that the Secretary determines necessary to improve ... **security** (emphasis added)... and guidelines pertaining to Federal computer systems."[532] If the CIOC and the Secretary of Commerce are able to follow through with their plans, the organizational environment should become somewhat more focused, orderly, and, hopefully, functional.

The Joint Security Commission was reconvened in 1999 to assess progress toward the goals recommended in the original 1994 report and to examine emerging security issues in an environment increasingly dominated by electronic data systems, networks, and communications systems. Unfortunately six years after the initial report and the formation of the Security Policy Board, the Commission found that, as demonstrated by this research, information infrastructure systems national security policy was still "in

by the Act (Section 5142) identically to NSD 42, National Policy for Security of National Security Telecommunications and Information Systems that established the NSTISSC. However, the Act does specific that national security systems do not include "a system used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications) (United States Congress, Clinger-Cohen Act of 1996 (also known as Information Technology Management Reform Act of 1996 (Public Law 104-106, Division E). United States Code. Title 40. Section 1401. 104th Congress, 2nd sess. January 3, 1996).

[532] United States White House, Executive Order (EO) 13011, Federal Information Technology, and United States Congress, Clinger-Cohen Act of 1996.

need of a clear enunciation of principles, goals, and definitions of authorities and responsibilities."

The Commission also found that the Security Policy Board was not only **NOT** addressing the issues associated with the expanded electronic network systems or globalization of business and technology, but that there was no integrated structure in place to address security policies associated with the issues.[533] The Security Policy Board "had been unable to create the intended INFOSEC committee, or an oversight mechanism as PDD 29 mandated."

Since the Board has been "unable to create the intended INFOSEC committee,"[534] it is attempting to provide requirements to assure the confidentiality, availability, integrity, authentication, and non-repudiation of information systems by addressing security and properties of data as it moves through networks, from system to system, through all of its states of transmission, processing, and storage through the Information Assurance Document Review Group/Working Group. As a result, "**information system security policy has remained fragmented at the managerial level, with responsibilities poorly defined and spread over multiple bodies**." (Emphasis added).[535]

Further, the second Commission found that the Policy Board's process was cumbersome and unwieldy, took too long to formulate policy, and resulted in spotty

[533] United States Joint Security Commission, Report of the Joint Security Commission II, "Cross-cutting Issues."

[534] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A175-180; United States Joint Security Commission, Report of the Joint Security Commission II; and United States White House, Presidential Decision Directive/National Security Council (PDD/NSC) 29, Security Policy Coordination.

[535] United States Joint Security Commission, Report of the Joint Security Commission II, "Introduction."

implementation of any approved policies." Contributing to the problem was the existing fragmented specialty threat analysis organization across multiple intelligence producers, disseminators, and users that was oblivious to agency boundaries. Separate centers for counterterrorism, counterintelligence, infrastructure protection, etc. increased the difficulty for the security countermeasures community to obtain timely and accurate threat data.[536] The Commission also found that there was no clearly defined and broadly accepted institutionalized mechanism for the Policy Board to issue national-level policy, even when endorsed and approved by the National Security Advisor.[537]

Further, within the USSPB process, the Security Policy Forum (a subordinate organization to the Board where most of the policymaking should have taken place) did not have the authority to resolve policy disputes and could only strive to achieve policy consensus. Consequently, the Forum had evolved into a "de facto congress of Security Directors," not the Assistant Secretary level of management envisioned by PDD 29. Exclusion of the Assistant Secretaries usually resulted in stalemate within the Forum requiring action by the entire Board further delaying any action. Presumably, the Assistant Secretaries would have not have been quite as parochial as the security directors and would have approached the security issue as a national-level issue instead of a bureaucratic one. Halperin informs us once again that that is not necessarily the case. The Assistant Secretaries belonging to, or being much closer to, the decision making elite would be more reluctant to give away a mission that was considered

[536] United States Joint Security Commission, Report of the Joint Security Commission II, "Understanding the Threat."
[537] United States Joint Security Commission, Report of the Joint Security Commission II, "Overseeing Compliance - A Need Overlooked."

essential to the organization's mission (or essence) or to accept one that was not considered essential. Also, without the Assistant Secretaries' active participation, there also appeared to be a lack of commitment to resourcing the policies approved.[538]

Equally damning, the reconvened Commission concluded that there was no "effective mechanism in place to monitor policy implementation for coherence and consistency or to ensure that policies were applied equitably and in ways consistent with national goals for standard security policies and interagency reciprocity." None of the authorizing documents, PDD-29, EO 12958, EO 12968, PDD-63 and OMB Circular 130, provided for national-level implementation oversight. [539]

4.4. Conclusions.

The most obvious conclusion that can be drawn from the preceding description is that PD 29 did not simplify information infrastructure system policymaking organizational complexity as anticipated. The IIS security policy structure, unbelievably, is now more complex than prior to 1994 (See Figure 4.1. Post-PDD 29 (>1994) IIS Security Policy Organization) and continues to create overwhelming confusion that is exacerbated even more by the PDD 63 mandates, not only within the federal government over who has the authority and/or power to deal with the issue and to what extent, but also within the public at large and the business community.[540]

[538] United States Joint Security Commission, Report of the Joint Security Commission II, "Introduction," "Restricting the Security Policy Board."

[539] United States Joint Security Commission, Report of the Joint Security Commission II, "Overseeing Compliance - A Need Overlooked."

[540] The government's action has created so many entities gathering data on Internet vulnerabilities that it is causing confusion. Imagine living in a community where there are seven different numbers to call for 911 services, says Mark Rasch, Chief Counsel to Global Integrity. Adds Tom Noonan, CEO of Internet Security Systems, "Quite frankly, I'm confused by all these different government groups" (Zuckerman).

How can this organizational complexity and confusion be explained? The empirical data indicate that the root of the complexity and confusion appears to be the different security agendas of the stakeholders involved, principally the federal bureaucracies and the business community. The chart below provides the major stakeholder categories and their primary security agendas.

STAKEHOLDER	**AGENDA**
National Security Agencies	Primarily Risk Avoidance Risk Management (secondary)
Law Enforcement Agencies	Risk Avoidance Prosecution
Management/Business-oriented Agencies	Risk Management
Business Community	Laissez Faire-ism Risk Management
Privacy Groups	Laissez Faire-ism (for confidentiality)

Figure 4.5. Stakeholders' Agendas

Privacy advocacy organizations are also considered a stakeholder category since they are primarily interested in confidentiality (one of the five information security objectives). However, they have been somewhat co-opted on the information security issue (but not their First Amendment protection agenda) by the proposed cryptography policy that guarantees confidentiality of data (and restricts government intrusion) to their satisfaction. As a result, the privacy organizations have reduced their active advocacy significantly in the IIS security policy arena.

Without satisfaction of their privacy agenda, these privacy organizations would have to be considered allied with the information technology industry. Both advocate expanded use of cryptography although the IT industry's overriding interest was more for expanded business opportunities than confidentiality/privacy reasons. Both stakeholders, though, generally oppose any government intrusion into the activities of the information infrastructure system.[541]

When the stakeholders' security agendas are depicted as a comparison of the security philosophies of risk management versus risk avoidance, several observations are readily available (See chart following).

	RISK MANAGEMENT	**RISK AVOIDANCE**
PUBLIC	Information Industry Privacy Organizations	
GOV'T	Management/Business-oriented Agencies (OMB/NIST/DoC)	Law Enforcement Agencies (FBI/DoJ) National Security Agencies (CIA/NSA/DoD)

Figure 4.6. Comparison of Stakeholders' Security Philosophies

What is interesting about such a categorization of the stakeholders by security agenda is the bifurcation of the federal bureaucracy into competing factions of risk management and risk avoidance. The most obvious observation from the above chart is that those government agencies advocating risk avoidance have no public allies. This

[541] Information Technology Association of America (ITAA), "Statement of Principles," ITAA's InfoSec Home Page, Arlington, VA., http://www.itaa.org/infosec/principles.html.

lack of allies is crucial in explaining the confused state of IIS security policymaking and subsequent lack of a comprehensive national IIS security policy.

As previously discussed, within the federal bureaucracy not only is there the normal bureaucratic competition between different agencies trying to increase influence, prestige, and size, but, in the IIS security policy arena, there is also a competition between the traditional national security/law enforcement agencies and those that more traditionally deal with the business sector and unclassified information.

This competition for security policy primacy is an extension of the tension between the business community's and the national security/law enforcement agencies' competing advocacy of risk avoidance versus risk management security philosophies. Admittedly, such a generalization does not hold across the entire spectrum of such agencies, but enough tradition of or advocacy for a specific security philosophy can exist within an institution that it is perceived as an advocate of that philosophy (e.g., many within DoD, a traditional national security agency, advocate a risk management security philosophy, but DoD as an institution is generally viewed as risk avoidant).

This bureaucratic security policy competition transcends the most visible example of NSA and NIST discussed earlier to the traditional national security/law enforcement agencies (CIA, DoD, etc.) and the management/business-oriented agencies (DoC and OMB) in general. Many of the information infrastructure system security responsibilities have been mandated to both DoC and OMB, with narrowly defined exceptions for "national security,"[542] to the chagrin of both the traditional national security and

[542] United States White House, National Security Directive (NSD) 42, National Policy for Security of National Security Telecommunications and Information Systems and retained by the Clinger-Cohen Act.

management/business-oriented agencies. The mandates, along with the support of the business community, allow these management/business-oriented agencies to adequately challenge the traditional national security agencies that consider national security policy their exclusive domain.

Business has been able successfully, so far, to resist pressure from the traditional national security agencies and support the management agencies because the information infrastructure system is almost entirely privately owned and operated (approximately 85%)[543] and the post-Cold War security environment is not as dire, immediate, nor directly threatening the national existence as during the Cold War. The national security agencies have no jurisdiction over the information infrastructure system assets and have not been able, to this point, to make a convincing enough case to force voluntary compliance with more restrictive risk avoidance measures.

The business community does acknowledge the seriousness of the information infrastructure system's vulnerabilities[544] and a need to cooperate with government on information infrastructure system security[545], but maintains "the nation's protection from and response to infrastructure vulnerabilities is not the legal or fiscal responsibility of private industry."[546] The IT industry does have a plan, prepared and advocated by the

[543] Information Technology Association of America (ITAA), "Information Security from the Private Perspective: Obstacles, Opportunities, and Responsibilities," iMP Magazine, September 22, 1999, http://www.cisp.org/imp/september 99/09 99itaa-insight.htm.

[544] "Infosec is likely to become the next Y2K for the IT industry and our customers" (Information Technology Association of America (ITAA), Information Security from the Private Sector Perspective: Obstacles, Opportunities, and Responsibilities).

[545] "Both government and industry have a major stake in protecting the nation's critical infrastructures and their underlying information resources from intentional attack and/or natural disaster" (Information Technology Association of America (ITAA), Information Security from the Private Sector Perspective: Obstacles, Opportunities, and Responsibilities).

[546] Information Technology Association of America (ITAA), "Response to PCCIP Report," ITAA's InfoSec Home Page, Arlington, VA., http://www.itaa.org/es/cne/cippccip.html.

industry's primary trade organization (the Information Technology Association of America (ITAA))[547], designed to "improve U.S. cooperation on issues of information security." Elements of the IT sector's plan include information sharing, awareness, education, training, best practices, research and development, and international coordination.[548]

The IT industry fears any acknowledged responsibility for IIS security will translate into "legal requirements" where it is compelled by the government to provide goods and/or services for national information security.[549] The industry specifically challenges the CCIP Report's twenty recommendations for "new mandatory certifications, regulations and standards to deal with what is perceived as threat to the national information infrastructure."[550]

The IT industry's overriding agenda is to prevent the government from exercising any greater control over its operations than it already does. [551] Its attitude can best be summarized by their claim that the IT products are proprietary: they were developed and

[547] The Information Technology Association of America (ITAA) has been designated the ISAC Sector Coordinator for the Information and Communications sector under PD 63, Protecting America's Critical Infrastructure.

[548] Miller, 5.

[549] Information Technology Association of America (ITAA), Information Security from the Private Sector Perspective: Obstacles, Opportunities, and Responsibilities.

[550] Information Technology Association of America (ITAA), Response to PCCIP Report.

[551] "For many in Silicon Valley, government is irrelevant at best and obstructionist at worst... an institution of tax-seeking bloodsuckers" (Thomas L. Friedman, "Confronting Microsoft's Arrogance," Pittsburgh Post-Gazette, June 11, 2000).

"In aiming to protect the U.S. information infrastructure, extensive and expanded regulation of information technology is unacceptable (Information Technology Association of America (ITAA), Response to PCCIP Report).

Additionally, similar comments expressing the same view have been heard by the author at different conferences by representatives of the information technology industry. The most recent example was during the presentation of Mr. Fred Thompson of UNISYS Corporation at The Matthew B. Ridgway Center for International Security Studies' December, 1999 "The Information Revolution and National Security Conference."

marketed by IT firms, their operation should be left to those that own them and know them best, and any security of those assets should be subject to economic cost-benefits.[552]

The IT industry has thrived in the current unregulated relatively laissez-faire marketplace and does not want government intervention dampening its opportunity to make money or, in its opinion, slowing down the progress of technological innovations. The industry believes that the engine of its success is the rapid pace of new product introduction to the marketplace and fears any governmental intervention will slow that pace and/or restrict business in some other way.[553] However, the issue of information technology security is of enough importance to the industry that the ITAA has published an eighteen-point "Statement of Principles" on information security.[554]

Part of the IT industry's caution about IIS security can be attributed to emphasis. Many of the measures needed to be taken to secure the information infrastructure system are not exclusively data confidentiality protection measures, but are protective measures necessary to protect the availability, integrity, authentication, and non-repudiation of the data.[555] Business is not convinced that all of these issues are, or to what extent they are, pertinent to its continued economic well-being and, therefore, in its self-interest.[556]

The information technology sector also believes that the requirement for security and the security products are in large part determined by the level of risk incurred. The degree of risk provides the commercial incentive to the marketplace to make or not make

[552] Information Technology Association of America (ITAA), Response to PCCIP Report.
[553] Information Technology Association of America (ITAA), Response to PCCIP Report.
[554] Information Technology Association of America (ITAA), Statement of Principle.
[555] Information Technology Association of America (ITAA), Statement of Principles.
[556] Information technology represents over 6 percent of global gross domestic product (GDP), a spending volume of more than $1.8 trillion, over 8 percent of U.S. GDP, and accounted for approximately one third of the U.S.'s real economic growth from 1995 to 1999 (Miller).

such products and services available. When the risk becomes great enough for users, the information technology sector will be enticed by the possibility of profit to provide the needed products and services.[557] At the same time, the industry believes some distinction should be made between the level of risk and threat, i.e., cyber-mischief, cyber-crime, and cyber-war, with the response tailored appropriately.[558]

Further, the business community also has a long-held belief, rightly or wrongly, that the law enforcement agencies are more interested in prosecution, not prevention or correction of vulnerabilities nor mitigation of the consequences of vulnerabilities. The business community has some well-founded skepticism about sharing information with federal agencies. There is a widespread belief within the business community that much of the data it shares with the federal government is not treated with the degree of discretion merited. Business does have legitimate reasons for wanting to protect its proprietary and other private data, but does not seem to be able to generate the degree of concern or respect for the level of protection it would like from the traditional national security and law enforcement agencies.[559]

First and foremost, the business community does not necessarily want all of the data it shares with the government to become public knowledge for a variety of reasons, e.g., proprietary compromise, loss of confidence, publicity of vulnerabilities, etc. Also, it does not want the data it shares to be used as evidence in a legal proceeding, especially against the organization that supplied the data, and, particularly if a legal case could be

[557] Miller, 3-4.

[558] Information Technology Association of America (ITAA), Statement of Principles.

[559] Information Technology Association of America (ITAA), Statement of Principles and Information Technology Association of America (ITAA), Response to PCCIP Report.

constructed only with the shared data. Further, the industry fears that the information it shares, particularly with the government, may lead to increased regulation of the industry or of electronic commerce in general.[560]

Finally, the business community is not completely satisfied that the national security and law enforcement agencies are entirely forthcoming with the information they develop about vulnerabilities, risks, and threats.[561] FBI personnel at NIPC must seek a case-by-case exception of Department of Justice guidelines to inform even the NSC's National Coordinator for Security, Infrastructure Protection and Counter-Terrorism of activities reported to the center.[562] In its view, cooperation is more unidirectional than it should be with the business community providing the bulk of the cooperation.

Regardless of the validity of the business community's concerns, the perception exists and manifests itself in reluctance by the business community to fully share data with the federal government[563] or to cooperate with the traditional national security and law enforcement agencies. A dramatic example of industry's attitude about governmental cooperation is manifested by the two years taken to establish the "partnerships" authorized by PDD 63 between the Department of Commerce and the information technology industry, even though DoC is one of its allies within the federal government.[564]

[560] Miller, 5.
[561] Miller, 7.
[562] Zuckerman.
[563] "Response to PCCIP Report."
[564] The IT industry has moved to establish more cooperation with the government in information sharing. As of January 2001, nineteen of the leading high tech companies announced the formation of a new Information Technology Sharing and Analysis Center (IT-ISAC) open to all U. S. based information technology companies to cooperate on cyber security issues (Miller, 6-7).

In fairness to the federal agencies, federal law, in many cases, mandates that any agency that suspects a violation of the law is required to report that suspicion to the proper authorities. Secondly, the Freedom of Information Act mandates that much of the data received from the business community be made available if requested under the Act. These mandates put an agency in a tremendous moral and legal dilemma: to report what it thinks is a violation of the law and comply with the Freedom of Information Act, or honor agreements, explicit or implicit, about access to the data. Regardless of the reasons, the business community is generally reluctant to cooperate with these traditional national security and law enforcement agencies.

Principally as a result of this contest between the management-oriented agencies (and their IT industry allies) and the more traditional national security/law enforcement agencies, there is no comprehensive plan for security. This competition has resulted in the proliferation of policymaking processes identified in Figure 4.4. Post-PDD 29 (>1994) IIS Security Policy Process exacerbating the structural confusion and consequent policy gridlock. Of the six processes identified, two are national security agency focused and four are management/business-oriented agency focused reflecting the changed post-Cold War security environment of more societal-based and economic threats. All four management/business-oriented agency processes have been established in the post-Cold War environment.

The information infrastructure system security policy area exhibits some of the characteristics of a regime as used in international relations: "a complex of stated and understood principles, norms, rules, processes, and organizations that, in sum, help to govern behavior."[565] Such a complex, in theory, postulates that comprehensive cooperation will evolve through a decentralized process that gradually merges separate rules, activities of organizations, and patterns of compliant behavior and expectations of the participants involved in the specified arena into a unified whole.

In many ways, this is what has happened within information infrastructure systems security issue area to produce what effective security for the IIS that does exist. The earlier Security Policy Board's comment about "well-intentioned, but fragmented groups, committees, panels, and boards, each trying to deal with some particular aspect or subset of Information Systems Security and closely-related Defensive Information Warfare"[566] and the previously discussed lack of policy leadership and government bureaucratic competition suggest a necessity-driven decentralized approach to information infrastructure system security.

A "bottom-up" development typical of most technology-driven changes emerged initially.[567] The community of information infrastructure users and security professionals had a sense of and a general understanding of what needed to be done to provide better protection for the system. In a unique phenomenon not readily apparent in other U.S. policy areas, the implementation and user community voluntarily began, without specific policy, to take the initiative to implement the different objectives of information security management that were most important to its specific organizations and responsibilities.

[565] John T. Rourke, International Politics on the World Stage, Seventh Edition, Guilford, CT.: Dushkin/McGraw-Hill, 1999, 224.
[566] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, A-180.
[567] National Academy of Sciences, The Unpredictable Certainty: Information Infrastructure Through 2000, 199.

Specifically, issues falling within the realm of information infrastructure security were addressed in department or agency policy documents as the need arose. The Department of Defense produced most of these policy documents, but the Department of Commerce, the Department of Justice, the Department of the Treasury, the National Security Telecommunications and Information Systems Security Committee (NSTISSC), OMB, and NIST also published policy about protecting the system.[568] All created information systems security policy that, "although similar, differ(ed) sufficiently to create inefficiencies and to cause implementation problems when organizations must coordinate their security protocols and procedures in order to interconnect."[569]

The most visible and obvious example of operator initiative was formation of the Computer Emergency Response Team located at the Software Engineering Institute of Carnegie-Mellon University, the CIAC (DOE's Computer Incident Advisory Capability), and the Forum for Incident Response and Security Teams (FIRST) as a result of wide-spread, malicious network-based attacks.[570] Another very obvious example of operator/manager initiative that crossed agency boundaries was the Joint Security Commission. As discussed earlier, the Commission was established by the Secretary of Defense and Director of Central Intelligence to review their own agencies' security practices and procedures and to develop a new approach to security.

A final, more auspicious example might be the voluntary partnership forged by the National Security Agency and the National Institute of Standards and Technology to

[568] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-77.

[569] United States Joint Security Commission, Redefining Security, Chapter 8, "Information Systems Security."

[570] United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future.

create the National Information Assurance Partnership in 1997. The agencies used the common need of both government and private consumers and producers for more "confidence and assurance in products ... to secure valuable information" to "combine the extensive information technology security experience of both agencies" to provide "objective measures and test methods for evaluating the quality of Information Technology (IT) security products." Both agencies also retained their core functions:

- NSA to protect the security of the federal government's data and
- NIST to do the same with the civilian and commercial sector while actively promoting (through the reliability of this program) commercialization of techniques and products internationally.[571]

Nothing in the research indicates that these two traditionally bureaucratic competitors were directed by a higher authority to form this partnership. All indications are that the managers of both organizations came to the realization with the heightened information security threats and breaches of the mid to late 1990s that each had expertise in security information and information systems but served different unrelated clients. Each would continue to work in its own area of expertise but would share that expertise with the other. Therefore, each agency's clients would optimally receive the best information technology security.

After examining the IIS security situation and finding that policies were not integrated or rationalized across the spectrum of agencies, the Commission decided it

[571] National Information Assurance Partnership (NIAP), Introducing the National Information Assurance Partnership Webpage, February 9, 2003, http://niap.nist.gov/howabout.html and National Information Assurance Partnership (NIAP), Letter of Partnership, National Security Agency and National Institute of Standards and Technology, August 22, 1997.

needed to expand its mission to include the entire federal government's security effort, not just DoD and the CIA. All of these efforts provided a degree of security for the institutions involved and stimulated policymakers to examine the issue. However, such a process can only go so far toward providing the necessary comprehensive national security or policy.

As observed from earlier descriptions, the policymaking organizational environment as it exists now is extremely complex (See Figure 4.1. Post-PDD 29 (>1994) IIS Security Policy Organization). As a result of a diffusion of authority stemming from collaboration, "partnerships," Presidential advisory organizations, bureaucratic competition, etc., the U.S.'s national information infrastructure system security policy organization appears to be morphing into the very the phenomenon it seeks to control (i.e., a network, See Figure 4.7. IIS Security Policy Network). Figure 4.7. IIS Security Policy Network is a replica of the identical agencies and relationships as Figure 4.1. Post-PDD 29 IIS Security Policy Organization and 4.4. Post-PDD 29 (>1994) IIS Security Policy Process drawn as a network instead of in the traditional vertical/horizontal bureaucratic organizational chart.

Even more interesting, as can be seen from Figure 4.7. IIS Security Policy Network the policy making network resembles a scale-free network, the very type of network the information infrastructure system's structure exhibits. Upon close examination, one can identify end-users (Info Assurance TF, ISPACs, PCCP, etc.) and highly connected nodes (National Security Advisor, CIAO, etc.) characteristic of a scale-free network. If the physical laws of a scale-free network are generalizable to the policy environment, one would expect to see a degradation of function (policymaking) as a result of the vital node not performing its role optimally. Such an effect appears to have happened with the dearth of comprehensive information infrastructure national security policy from 1990 to 2000 adding credibility to the model of the policy environment as a scale-free network.

The National Security Advisor's failure to take a more active direct role (a degradation of that highly connected node's function) hampered the policy making process by not forcing, through his mandated and perceived authority, subordinate policy decision makers (DoD, DoC, USSPB, etc.) to collaborate effectively. The same could be said for the National Security Council. The CIAO's inability to adequately perform its mission of integrating the other critical infrastructures into the information infrastructure national security policy making environment in a timely fashion further supports the concept of a vital node's importance and the degradation of system function correlated to degradation of a vital node.

Several factors in the information infrastructure system national security policy environment contributed to the degradation of these vital nodes leading to the general paralysis of the policy making process:

- the complexity of the issue itself,
- the trans-bureaucratic nature of the issue, and
- the lack of a consensus of any one agency's jurisdiction for the issue.

As can also be seen from Figure 4.7. IIS Security Policy Network even a network depiction of the environment is less than optimum. The policy structure is becoming so complex and confusing that even this type of a depiction of the structure now needs to be shown in three instead of two dimensions to accurately show all relationships.

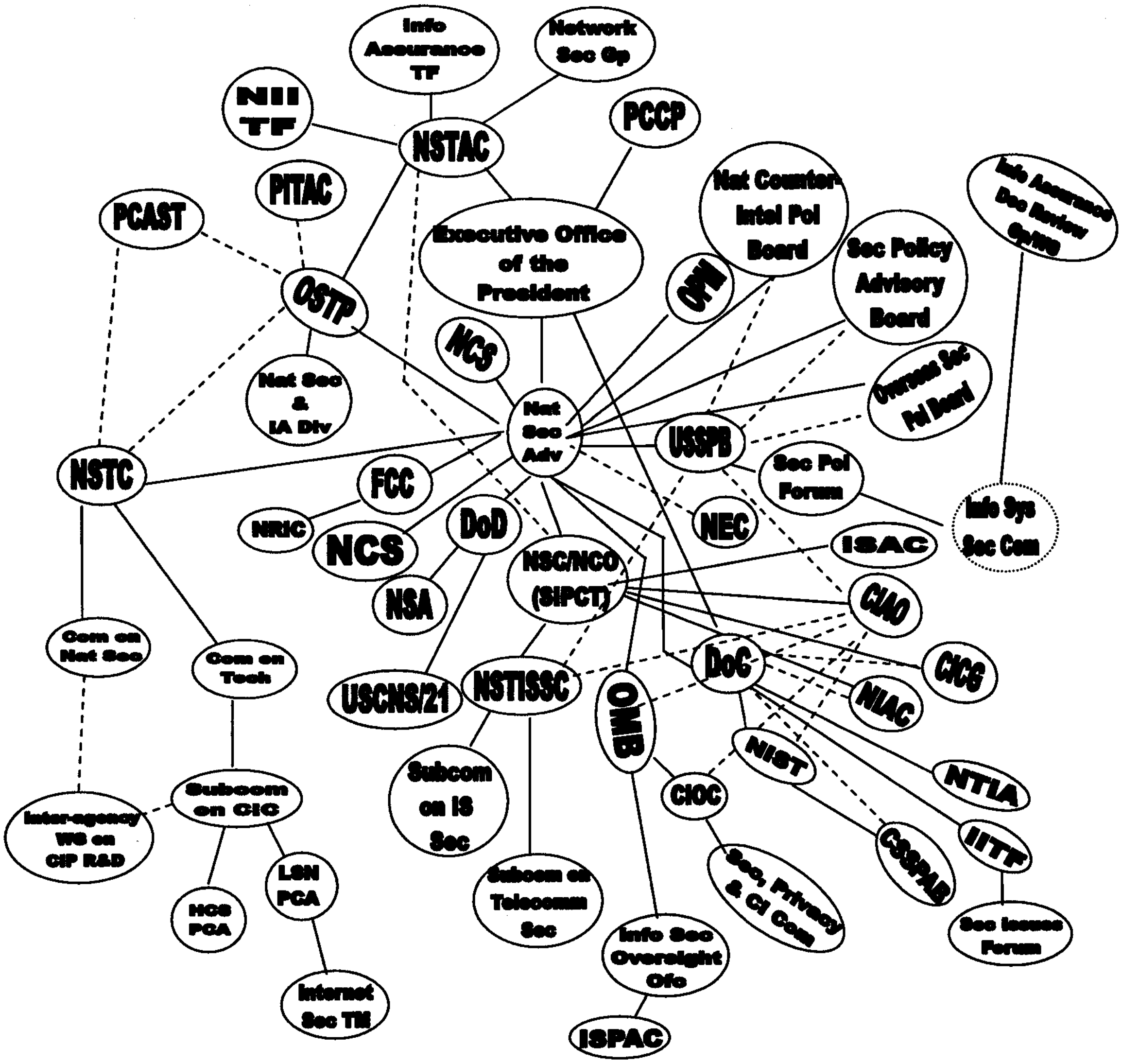
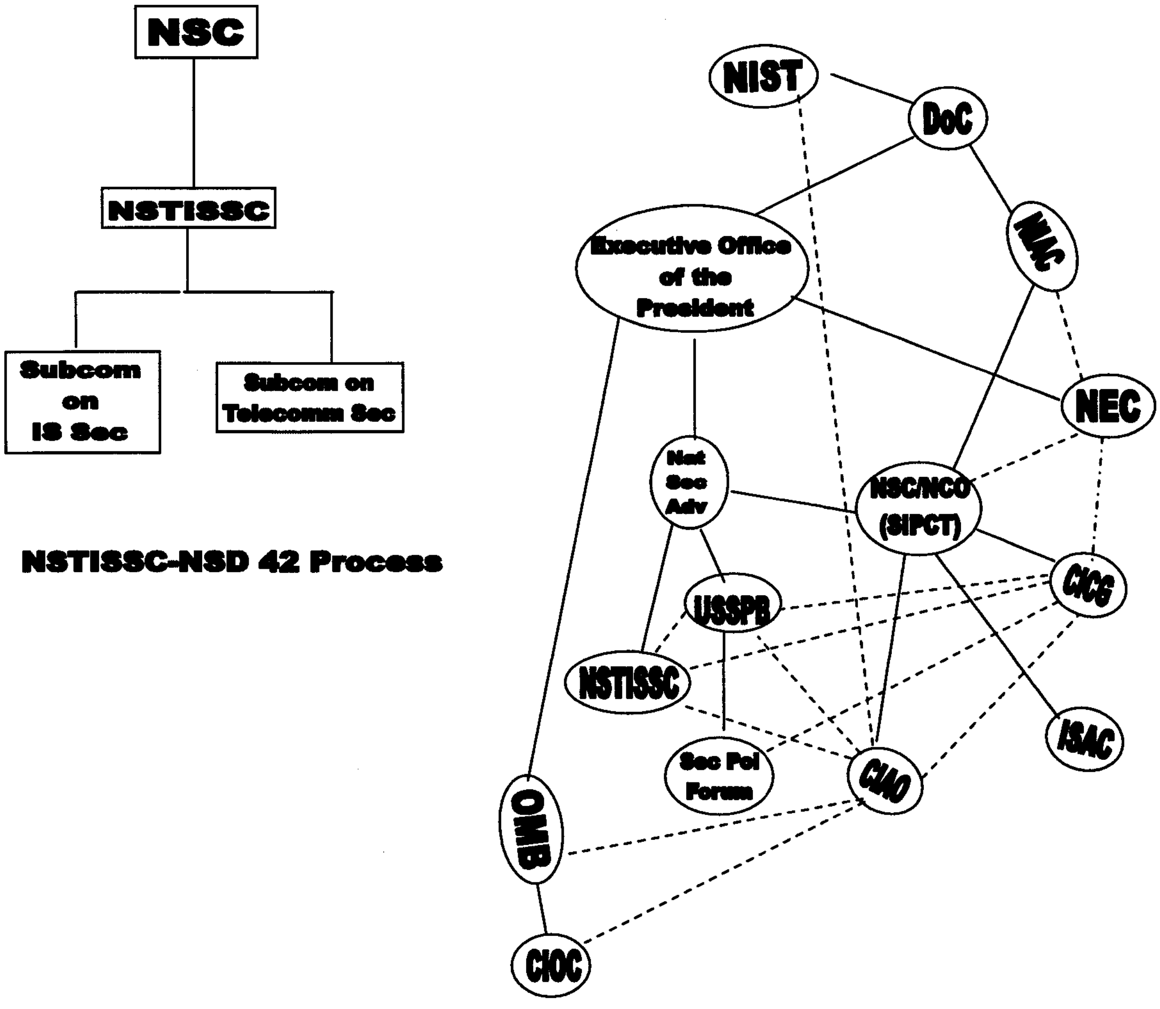


Figure 4.7. ISS Security Policy Organizational Network

Upon closer analysis, one can observe that those later mandated processes (e.g., PDD 63, see Figure 4.8. Comparison of Processes) more closely resemble a network configuration than the earlier ones (see Figure 4.4. Post-PDD 29 (>1994) IIS Security Policy Process or Figure 4.5. IIS Security Policy Network for detailed depiction of all IIS security policy processes and Figure 4.8. Comparison of Processes for comparison). I deliberately chose the NSTISSC process for comparison because it was the first process to be designated exclusively for information infrastructure system security. The PDD 63 CIP process is much more network-like if one depicts the membership of all the different advisory boards, coordinating organizations, etc. Most of the action agencies in the PDD 63 CIP process have multiple federal agency and industry members.

I attribute the difference between the two processes to the uncontested supremacy of the traditional national security/law enforcement during the Cold War era (before 1990) compared to a greater array of national security organizations after the collapse of the USSR. The critical difference is the nature of the threat: solitary directed threat of the Cold War vice the more diffused national security threats of the post-Cold War era.

Just as a network structure makes prediction and control of the information infrastructure system difficult, a network structure for the policymaking process makes prediction, control, and centralized policymaking difficult also. Such a phenomenon does not bode well for a comprehensive national information infrastructure security policy.



NSTISSC-NSD 42 Process

PDD 63 CIP Security Process

Figure 4.8. Comparison of Processes

The sad fact is that much of this policymaking confusion could have been avoided. Once again, Halperin offers an explanation of what might have been. He postulates that "despite the different interests of the participants and the different faces of an issue which they see, officials will frequently agree about what should be done." Such agreement most likely takes place when there is strong Presidential leadership.[572] Unfortunately, throughout his term President Clinton was much more interested in domestic policy than national security matters and did not provide the strong leadership necessary to clarify the policy environment to resolve the organization competition.

[572] Halperin, "Why Bureaucrats Play Games," 74.

CHAPTER 5

INFORMATION INFRASTRUCTURE SYSTEM SECURITY AND IIS SECURITY R&D FUNDING

> "The government lacks a comprehensive policy and plan to meet the threat.... Funding, missions, (and) technological expertise ... are scattered among dozens of often competing or secretive federal agencies."[573]

Unfortunately, the same quote that introduces Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy is as valid for information infrastructure system security research and development organization and funding as for policymaking. As previously stated, research and development is included in this analysis because the R&D agenda and priorities are crucial to correcting the technical vulnerabilities;[574] the success of those efforts, to a degree, determines the success of any security policy that is formulated; and the funding history of both information infrastructure system security and security R&D completes the picture of the government's ambivalence to the information infrastructure system's security.

Ideally, the level of spending by a government on an issue provides evidence of the issue's importance for that government. Unfortunately, the research's findings on funding and research and development augment and reinforce Chapter's 4's policy analysis conclusion that there is little consistent federal focus on the information infrastructure system's security. The research in this chapter will further show that research and development "programs...concentrated on 'respond and react' technologies rather than

[573] "Panel Warns U.S. on Terror," Pittsburgh Post-Gazette, July 15, 1999, A-1.

considering the full range of risk management needs" and that "the funding model used by industry and government was not always conducive to taking the long view of security."[575]

Both the National Security Strategy 2000, A National Security Strategy for A New Century, and Defending America's Cyberspace: The National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue, as well as other IT or IT security documents,[576] recognize the importance of information infrastructure system security

[574] The national plan acknowledges that "many of the tasks required in the first five steps of the plan cannot be performed well or, in some cases, cannot be performed at all, with today's technology (United States White House, Defending America's Cyberspace, 25).

[575] United States National Security Telecommunications Advisory Committee (NSTAC), Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration, ES 1-2.

[576] A Network Security Group, National Security Telecommunications Advisory Committee, National Security Information Exchange (NSIE) Risk Assessment (1996) concluded that government and industry sponsored R&D is insufficient (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizations Considerations for Assurance, A-198).

A symposium sponsored by the President's NSTAC at Purdue University in October 1998 concluded that "eliminating vulnerabilities and deterring future threats will require improvements in security technology" (United States National Security Telecommunications Advisory Committee (NSTAC), Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration, ES-1).

The PITAC report, "Information Technology Research: Investing in Our Future," February 24, 1999, stated that

> "the economic and strategic importance of information technology to our society demanded increasing Federal support for information technology research and development because of **industry's focus on the near term in today's competitive environment** (emphasis added). In need of particular attention is software since the demand has grown far faster than the ability to produce it, particularly software that is far more usable, reliable, and powerful than what is being produced today" (United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium, A Report by the Subcommittee on Computing, Information, and Communications Research and Development, National Science and Technology Council, Supplement to the President's FY 2000 Budget, April 8, 1999).

The Report of the DSB Task Force on Information Warfare (Defense) in 1997 concluded that information R&D should focus on the following areas:

- Robust survivable system architectures;
- Protection against a solitary event/attack leading to a critical function failure;
- Designs to provide for graceful degradation and rapid restoration of critical functions;
- Techniques and tools for modeling, monitoring, and management of large-scale distributed/networked systems;

research and development to the United States' national security. The national plan for information systems protection recommended increased funding of $500M for critical infrastructure protection research. It even devotes an entire program (Program 6: Enhance Research and Development in Support of Programs 1-5) to

> "establish research requirements and priorities needed to implement the Plan, ensure their funding, and create a system to ensure that our information security technology stays abreast of changes in the threat and in overall information systems."[577]

President Clinton further reinforced the importance of information technology research and development on January 21, 2000, with a $605 million increase in information infrastructure system R&D funding over previously requested funding for FY2001. This additional funding was to help "develop information systems that ensure privacy and security of data to allow people to get information they want, when they want it, in forms that are easy to use" through network protection, advanced encryption, and methods to design and test software without sacrificing speed and ease of use.[578]

The national scientific community recognized the importance of research and development as well. The President's National Security Telecommunications Advisory Committee (NSTAC) first identified "six technology areas in which government and industry should pursue commercially applicable security tools" in its 1990 as part of its

- Tools and techniques for automated detection and analysis of localized or coordinated large-scale attacks;
- Tools for synthesizing and projecting the anticipated performance of survivable distributed systems;
- Tools and environments for IW-D oriented operational training; and
- Testbeds and simulation-based mechanisms for evaluating emerging IW-D technology and tactics (United States Department of Defense, Report of the DSB Task Force on Information Warfare (Defense), Section 6.9 – "Focus the R&D").

[577] United States White House, Defending America's Cyberspace.

[578] United States White House, President Clinton Announces Nearly A $3 Billion Increase in Twenty-First Century Research Fund, Office of the Press Secretary, Washington, D.C., January 21, 2000.

threat review of the public switch network.[579] The NSTAC then followed up the initial findings of the 1990 public switch network assessment with a research and development exchange in 1991 to "provide a forum for industry and government officials to discuss those six technology areas and exchange information about ongoing R&D projects."

A second exchange was conducted in September 1996 to "provide industry and government with the opportunity to develop a common understanding of network security problems affecting national security and emergency preparedness (NS/EP) telecommunications."[580] The Intrusion Detection Subgroup of the NSTAC even identified IT security research and development **national policy** (emphasis added by author) and technological development as "requiring attention" in 1997.[581] The NSTAC has consistently continued to emphasize the need for both continued IT security research and development and for a government-industry-academic coordinated approach during the intervening years.

With such public emphasis on information infrastructure system research and development, one might legitimately ask why the national effort has not produced more timely results to correct the vulnerabilities of the system. The Defense Advanced Research Projects Agency's Information Science and Technology (ISAT) 1996 Summer Study on Survivable Distributed Information Systems addressed essentially the same issue:

> "Laboratory successes are not impacting the nationally critical technologies. Strategies for developing the necessary security software, hardware and other security technologies have

[579] See footnote 3, Chapter 1. Introduction for more information on the public switch network assessment and its results.

[580] United States National Security Telecommunications Advisory Committee (NSTAC), Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration, 1-2.

[581] United States National Security Telecommunications Advisory Committee (NSTAC), "Report on the NS/EP Implications of Intrusion Detection Technology Research and Development," Washington, D.C., December 1997.

> not been very effective over the years. Not only has the government not followed through with incentives offered to industry to develop security products, it has failed to control and coordinate its own R&D programs. As a result, some attractive lines of research have been neglected while there have been duplications of effort and products produced that are not readily interoperable with other computer security products. Moreover, security has been focused almost exclusively on providing protection to classified information and systems to the detriment of protecting unclassified information and the infrastructure assets."[582]

Part of the problem lies with the technical intractableness of the issue and other complexities discussed in Chapter 3. Information Infrastructure System Vulnerabilities, Risks, and Threats. But, as the following research shows, much of the answer to the lack of emphasis and the dearth of results for both IT security and IT security R&D funding lies with the same organizational turbulence prevalent in the security policy issue discussed in Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy.

5.1. Information Infrastructure System Security Funding.

Although the primary emphasis of this chapter is information infrastructure system security research and development, the research also examined the federal government's fiscal commitment to securing the existing system as further empirical evidence of resolve to protect this critical infrastructure and to provide for the nation's security. One would have hoped from the earlier statements of official U.S. government policy documents that the level of spending for information infrastructure system security would be relatively high both in actual monetary outlay and as a percentage of appropriated funds. However, as will be demonstrated, the federal government fell woefully short in both categories.

[582] United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizations Considerations for Assurance, 2-99.

In order to provide the greatest objectivity to the evaluation, comparison of information infrastructure system security funding with some standard is desirable. However, as far as I can determine, the only standard for evaluating information infrastructure system security funding is a recommendation by the Joint Security Commission in 1994:

> "five to ten percent of the total cost of developing and operating information systems and networks as an appropriate funding level to ensure the availability, confidentiality, and integrity [the core information assurance objectives (added by author)] of the systems and networks."[583]

I interpret this statement to mean that 5–10 percent of total federally appropriated funding for information infrastructure systems should be spent for system security. Absent any other, this is the standard I will apply to the federal government's outlays for IIS security funding.

Similar to information infrastructure system security policymaking and its organization, just trying to determine the level of federal information infrastructure system security funding, and even more so for security-related R&D funding, is an exercise in frustration. Even the High Performance Computing and Communications Program FY 1995 Implementation Plan officially commented on this difficulty:

> "Since its inception in 1992, the HPCC Program has undergone changes that make it difficult to track actual funding against the originally planned funding profile. New agencies have been added, major new responsibilities have been added, some agencies' activities not originally defined within HPCC have now been moved under this funding category."[584]

Although the above quote is descriptive of only one relatively small R&D program, it is symptomatic of the entire federal IT security and security R&D effort. Few Executive

[583] United States Joint Security Commission, Redefining Security, Chapter 8, "Information Systems Security."

[584] United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 1995 Implementation Plan, April 8, 1994.

Branch departments and agencies have separate budget line items for IT security, and much of the data in the federal budgets are not detailed enough to derive whether the funds, or part of the funds, are intended for security. In many cases, security resources are included as overhead in department or agency accounts. With information infrastructure system security R&D specifically, much of the funding data is in special programs conducted by a single agency or interagency consortia with little detail to determine whether security research and development is included in the program.[585]

There is no attempt to aggregate information system security or security R&D data within the federal budget until 1999. Until then, there generally is no correlation between agency security budgets and execution of national security priorities. Finally, I suspect that much of the federal funding for both information security and information security R&D is either "black," i.e., hidden in the budget under other items, or classified.

All of this means that problems of comparability due to widely varying systems, security data standards, and data reliability among agencies limit the accuracy and completeness of current reporting. Collectively, these budgetary oversights make determining the true costs of information infrastructure system security and security-related R&D extremely problematic.[586]

Because of these above factors, I daresay it would be impossible to determine over the course of the last decade how much money the United States federal government has spent on either information infrastructure system security or information security R&D.

[585] According to Chapter 7, "Investing in Science and Technology," of The President's 7-Year Balanced Budget Plan, departments and agencies are sponsoring 8 different information technology research and development programs. These 8 do not include administration initiated inter-agency programs such as NGI, IT^2, and IITF, but are exclusive programs of NIST, NSTC, DARPA, DoE, NSF, and HPCC.

[586] United States Joint Security Commission, Report of the Joint Security Commission II, "Understanding the Cost."

Hopefully, this situation may be changing in the future. According to the Report of the Joint Security Commission II of August 24, 1999, the Chief Information Officer Council (CIOC) is formulating a budget for information security across the federal government.[587]

The federal budget for Fiscal Year 1999, 2000, and 2001 does contain a priority management objective for information technology, but even this effort to consolidate federal funding for information technology demonstrates difficulty in finding credible, accurate data as the following discussion illustrates. The budget proper provides funding data for IT R&D in the section on "Promoting Research" and total IT funding in the Analytical Perspectives in "Information Technology Investments." OMB's Report on Information Technology Spending for the Federal Government for Fiscal Years 1999, 2000, and 2001[588] appears to be a more detailed explanation of the section in "Analytical Perspectives" but contains no security-related funding as a category. The funding is identified only as expenditures by mission areas within the IT infrastructure/office automation, and the IT architecture/planning objectives. There is no security planning objective. There are several mission areas within the objectives that are security- related (e.g., Mission 027: Security Activities, and Mission 046: Defense Information Assurance Program), but few departments or agencies report funding for either mission area.

As this analysis shows, very little ($523M (or 1.4%) in FY 99, $672.7M (or 1.8%) in FY 00, and $1180.7M (or 3.1%) in FY 01) of the approximately $38 billion spent each year

[587] United States Joint Security Commission, Report of the Joint Security Commission II, "Organizing INFOSEC in the Government."

Such a budget has not been created as of the publication of this analysis. Or, if it has, has not been published in the open press.

[588] United States Office of Management and Budget, "Report on Information Technology Investments (Exhibit 53), FY2001 Budget," Preparation, Submission, and Execution of the Budget. Circular No. A-11.Washington, D.C., 2000.

on information technology is devoted to security; well outside the Joint Security Commission's recommendation of 5-10% of all IT funding. Most of the federal funds are still devoted to maintaining the steady state, acquisition, network architecture planning and implementation, and other efficiency measures, not explicitly for security of the existing or planned networks.

As much as I would like to believe that the network architecture planning was to mediate the intrinsic effects of the scale-free network structure identified as a vulnerability in Chapter 3. Information Infrastructure System Vulnerabilities, Risks, and Threats, I am somewhat skeptical. The research on network structure was not published until 2000 (See Albert, Jeong, and Barabaasi's and Tu's articles in the July 27, 2000 edition of Nature). More than likely, the network architecture planning was to determine how best to expand the network and to make it most efficient, not some security related aspect of network architecture planning, unfortunately.

When compared to only OMB's development/modernization/enhancement budget proposals, security-related funding of 7.5%, 10.4 % and 17.4% in FY 2000, 2001 and 2002, respectively, actually satisfies or exceeds the Commission's recommendation of 5-10%. However, the funding does not fully satisfy the Joint Security Commission's standard since development/modernization/enhancement component is only part of the government's information technology expenditures (See Total (sig/nonsig) in Table 5.1. OMB's IT Funding For FY 99/00/01). What the comparison does show, though, is that

Table 5.1. OMB's IT Funding For FY 99/00/01
(In Millions of Dollars)

	FY1999	FY2000	FY2001
OMB			
(dev/mod/ enhance)	6893.6	6,440.5	6,766.4
(steady state)	7999.1	8.932.2	9,956.9
Total (sig/nonsig)	**37595.0**	**38,106.2**	**39,727.9**
(sec-related)*	523.0	672.7	1,180.7
% of Total IT Funding	1.4	1.8	3.1
% of OMB's dev/ mod/enhance		10.4	17.4

*Security-related funding figures are not a separate category in the report, but are derived from detailed analysis of individual departments'/agencies' plans from the OMB Report (See Table 5.3. U.S. Government Security Related Funding (FY 99/00/01) for each specific department's or agency's funding).

security-related funding is gaining a larger share of funds to improve the system. Still, according to the Commission's standard of commitment, one has to conclude that the U.S. federal government is either not sincere in its pronouncements about the importance of information infrastructure system security or is not devoted to mitigating the problem.

5.2. Information Infrastructure System Security R&D.

Unfortunately, similar to the security policymaking organizational environment of Figures 4.1. Post-PDD 29 IIS Security Policy Organization; 4.2. Pre-PDD 29 IIS Security Policy Organization (Actual); and 4.4. Post-PDD 63 (>1998) IIS Security Policy Process in the previous chapter, the organizational structure of information technology research and development is not much clearer nor more rationalized. OSTP has exercised different degrees of organizational responsibility for information infrastructure system security R&D.[589] Currently, specific offices within the Office of Science and Technology Policy (National Security and International Affairs Division) and lateral organizations (Committee on National Security and Committee on Technology of the National Science and Technology Council) have varying roles for different aspects of the R&D.

[589] United States Office of Science and Technology Policy, Homepage, http://www.whitehouse.gov/OSTP, May 17, 1999.

The Office of Science and Technology Policy (OSTP) was created by the National Science and Technology Policy, Organization and Priorities Act of 1976 as the primary advisor to the President for formulation, articulation, budget development, and coordination of science and technology policy and investment. PDD 63, Protecting America's Critical Infrastructure, further solidifies OSTP as the lead research and development manager by designating it as "responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council (United States White House, Presidential Decision Directive (PDD) 63, Protecting America's Critical Infrastructure).

As can be seen by OSTP's mandates, the organization does have the authority to oversee technology policy, and could have used that authority do supervise information infrastructure system security R&D policy, but has chosen not to do so completely (See Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy for a detailed discussion of OSTP's organizational behavior).

As Appendix D. Organizational Responsibilities and Authorities indicates, identical or similar mandates by other federal organizations pursuing research and development independently (e.g., DoD, NSA, NIST, etc.), and added advisory organizations have created lines of authority, coordination, and communication confusion within the information infrastructure system R&D organizational environment (See Figure 5.1 for OSTP R&D organizational environment).

The National Science and Technology Council (NSTC) was established on November 23, 1993 by Executive Order 12881 as the "principle means to coordinate science, space, and technology policies across the Federal government," (almost a direct replica of OSTP's mandate). Two of its committees are particularly relevant to this discussion: the Committee on National Security and the Committee on Technology. The mission of the Committee on National Security is to "advise and assist the NSTC to increase the overall effectiveness and productivity of Federal efforts in national security research and development."

The Committee on Technology has responsibility for overall technology policy, program and budget guidance, and direction for research and development to the Executive Branch for federal technology R&D.[590] Its Subcommittee on Computing, Information, and Communications R&D along with the National Coordination Office for Computing, Information and Communications will be discussed in more detail later in the chapter.

[590] United States National Science and Technology Council, Council Committees Purposes Webpage, http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/committee/ct_purpose,.html.

Once again, here is an organization with authorization that would allow it to oversee information infrastructure system security, but chooses not to exercise its mandate completely or fully.

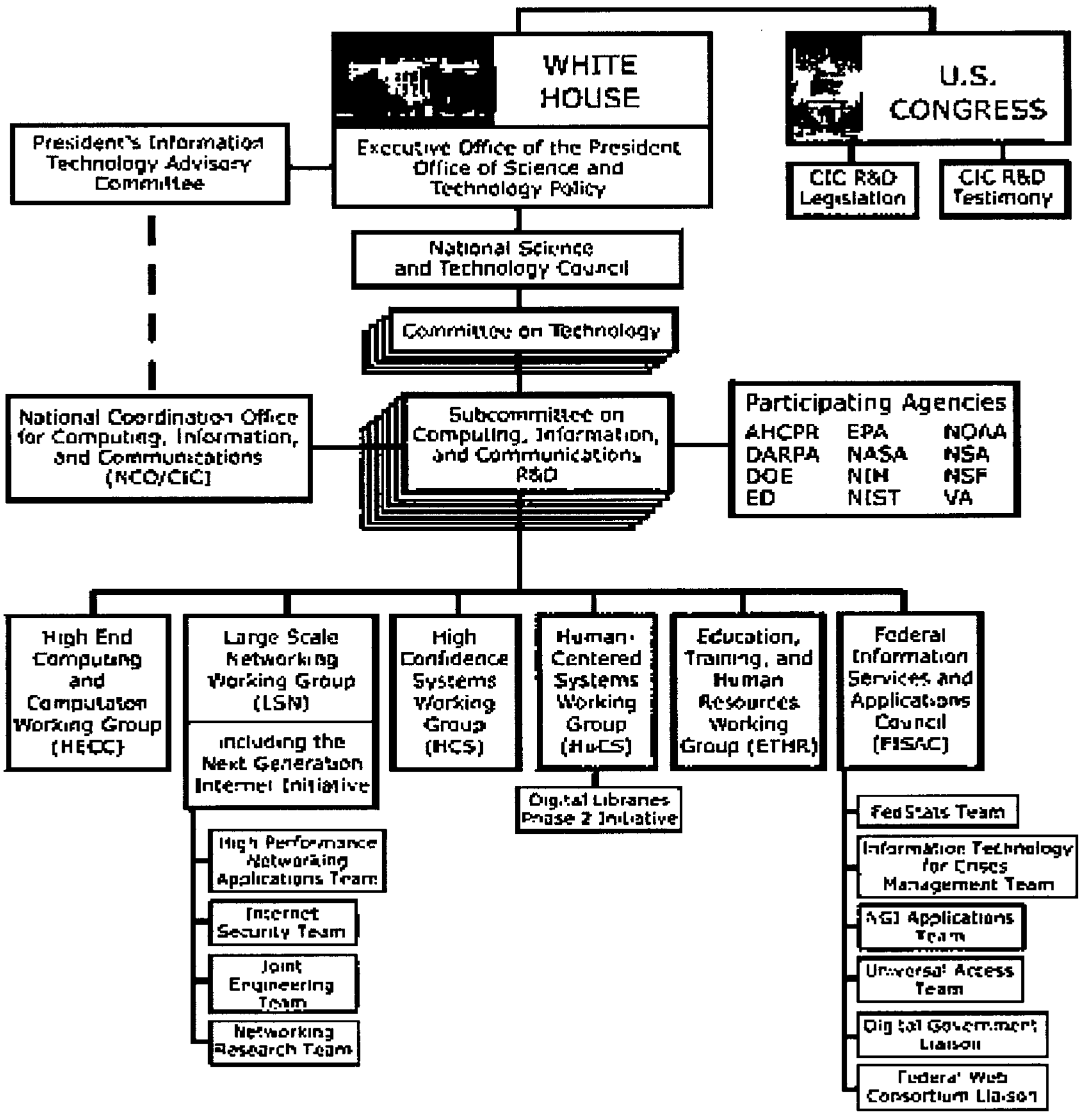

WHITE HOUSE
U.S. CONGRESS
President's Information Technology Advisory Committee
Executive Office of the President Office of Science and Technology Policy
CIC R&D Legislation
CIC R&D Testimony
National Science and Technology Council
Committee on Technology
National Coordination Office for Computing, Information, and Communications (NCO/CIC)
Subcommittee on Computing, Information, and Communications R&D
Participating Agencies
AHCPR EPA NOAA
DARPA NASA NSA
DOE NIH NSF
ED NIST VA
High End Computing and Computation Working Group (HECC)
Large Scale Networking Working Group (LSN)
including the Next Generation Internet Initiative
High Confidence Systems Working Group (HCS)
Human-Centered Systems Working Group (HuCS)
Education, Training, and Human Resources Working Group (ETHR)
Federal Information Services and Applications Council (FISAC)
Digital Libraries Phase 2 Initiative
High Performance Networking Applications Team
Internet Security Team
Joint Engineering Team
Networking Research Team
FedStats Team
Information Technology for Crises Management Team
NGI Applications Team
Universal Access Team
Digital Government Liaison
Federal Web Consortium Liaison

Figure 5.1. OSTP R&D Organization[591]

[591] United States Office of Science and Technology, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.

Both the Committee on National Security and the Committee on Technology jointly manage the Interagency Working Group on Critical Infrastructure Protection (CIP) Research and Development (R&D). The interagency working group coordinates multi-department, multi-agency R&D in CIP technologies to:

- satisfy the needs of the federal government for protecting infrastructures,
- increase the overall effectiveness and productivity of federal efforts in national security research and development by addressing the technical aspects of national policy and planning,[592] and
- accelerate the development and deployment of advanced CIP technologies."[593]

The President's Committee of Advisors on Science and Technology Policy (PCAST) was authorized at the same time as the NSTC by E.O. 12882 of November 23, 1993 and extended by EO's 12974 and 13062 at least through September 30, 1999. The PCAST was established to provide nonfederal IT sector advice to the President and the National Science and Technology Council on the nation's investment in science and technology. It reports to the President through the Assistant to the President for Science and Technology.[594]

The President's Information Technology Advisory Committee (PITAC) was organized on February 17, 1997, by Executive Order 13035 from the President's Advisory Committee on High Performance Computing and Communications, Information Technology, and the Next Generation Internet to "provide the President with an independent

[592] United States National Science and Technology Council, Council Committees Purpose Webpage.
[593] United States National Science and Technology Council, Homepage, http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/NSTC_Home.html, 5/17/99.
[594] United States White House, Executive Order 12882, President's Committee of Advisors on Science and Technology Policy.

assessment of the Federal government's role in HPCC, information technology, and Next Generation Internet R&D."[595] The PITAC reports to the President through the Assistant to the President for Science and Technology so the Director of OSTP has a certain degree of control over both what the PITAC and the PCAST does and what it recommends. More about the PITAC and the its role in information technology R&D and its relationship with the HPCC Program will discussed later and in the conclusions.

The High Performance Computing and Communications Program (HPCC) was authorized with bipartisan Congressional support in 1991 through passage of the High Performance Computing Act as a dynamic R&D program to extend U.S. leadership in high performance computing and communications. The Program coordinated R&D initiatives, at least those that were unclassified, across the entire spectrum of federal departments and agencies and provided the sustained focus needed for developing high performance computing and communications technologies.[596] HPCC was the only federally funded program that attempted to coordinate information infrastructure system R&D and consolidate funding over the decade of the 1990s.

I intend to use the HPCC Program as a model for federal research and development to demonstrate indirectly not only the difficulties with determining and evaluating information infrastructure system and security-related R&D funding, but also to demonstrate how the organizational environment has affected the research and

[595] United States Office of Science and Technology, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium, and United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 1998 Implementation Plan, September 3, 1998, 6.

[596] United States Office of Science and Technology, High Performance Computing and Communications: Advancing the Frontiers of Information Technology, A Report by the Committee on Computing, Information, and Communications, National Science and Technology Council, Supplement to the President's FY 1997 Budget, November 1996.

development. It is also the best model for illustrating the level and focus of spending and the organizational turbulence in federal information infrastructure system security research and development for the following reasons:

- fairly accurate records exist for the initiatives and funding over the years of the Program's existence and
- consolidated budgets and detailed funding descriptions make determining the security R&D funds within the HPCC Program somewhat easier and more reliable with some level of confidence.

The following very detailed description of HPCC activities is included to present as clear a picture as possible to substantiate later generalizations of organizational turbulence, lack of commitment to coordinated security-related information infrastructure system security R&D, and the lengths operators below policy making level went to get security-related information infrastructure system security R&D funded. In my analysis of the HPCC documents, I restricted myself to those programs and projects that specifically targeted security or those which deliberately sought to enhance the five security management objectives: confidentiality, availability, integrity, authentication, and non-repudiation of the system and the data it provides.

5.3. High Performance Computing and Communications Program (HPCC)[597] Funding Data.

A. Fiscal Year 1994.[598] Although begun in 1991, 1994 is the first year for which detailed R&D descriptions and funding data are available. The President proposed a budget of

[597] Except as noted, all of the data about the HPCC Program is extracted from NSTC's annual supplements to the President's budget and NCO's annual implementation plans for the HPCC Program. HPCC's annual funding for security R&D is recapitulated by year at the end of the section for comparison and analysis.

$1.096 billion for FY 1994 to accomplish the HPCC goals; an increase of 36 percent over FY 1993's appropriated $805 million.[599]

Initially, security concerns were glaringly absent. As Peter G. Neumann says in Computer Related Risks, "Very-high performance architectures have in general ignored security problems to achieve performance."[600] High performance computing and networking was just beginning to realize its potential and the emphasis was on viability, efficiency, affordability, and cost-effectiveness.[601] The major thrust of research and development in HPCC was to "accelerate the development of future generations of high performance computers and networks and the use of these resources... to be brought into the commercial marketplace as rapidly as possible ... to strengthen the national competitiveness."[602] High integrity, fault-tolerant, trusted, scalable computing systems were considered to be part of the common foundation for a broad range of information technology-based applications.

The National Science and Technology Committee did acknowledge, however, that there is a "need for increased security and privacy," but that need is considered only

[598] United States Office of Science and Technology Policy, High Performance Computing and Communications: Toward a National Information Infrastructure.

[599] United States Office of Science and Technology Policy, High Performance Computing and Communications: Toward a National Information Infrastructure.

Actual FY 94 appropriated funding for High Performance Computing and Communications R&D was $938 million (United States Office of Science and Technology Policy, High Performance Computing and Communications: Technology for the National Information Infrastructure).

[600] Neumann, Computer Related Risks, 213.

[601] United States Office of Science and Technology Policy, High Performance Computing and Communications: Toward a National Information Infrastructure.

All of the HPCC activities "depend heavily on the development of more cost-effective approaches to writing and maintaining software..." (United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 1995 Implementation Plan).

[602] United States Office of Science and Technology Policy, High Performance Computing and Communications: Toward a National Information Infrastructure.

"desirable but not critical to deployment" by the Committee. However, the Committee did consider both security and privacy as essential for deployment in the long term as a Grand Challenge and as a Key National Challenge Application Area for national security. However, national security concerns at this time were viewed only as "requiring far greater computing capability than is currently available" to be addressed by the accelerated development of scalable computing systems.[603]

Consistent with the announced strategy, security research was planned in only a few component areas' research as a low-order priority. Even when analyzing the individual agency's intentions in the implementation plan, the amount spent or planned to be spent is categorized by program activity and not by individual research project within the program activity. Unfortunately, rarely is a program activity solely related to security; only certain projects within a program activity investigated ways to mitigate or correct a vulnerability and the information is not detailed enough to determine the amount being spent solely for security-related projects

Only NSA's research specifically addressed national security. Confidentiality improvements continued through NSA's on-going cryptographic research. However, availability was ignored and information integrity questions were nascent. Such a restricted perspective in 1994 might be explained by the lack of time the HPCC Program had to develop fully or to coordinate planned R&D with the NCO and the participating departments and agencies. The National Security Agency and the Department of Defense had only joined the High Performance Computing and Communication program within the

[603] United States Office of Science and Technology Policy, High Performance Computing and Communications: Toward a National Information Infrastructure.

past year. However, within this year, DARPA and NSA, along with NIST, were credited with research (which more than likely had already been planned by these organizations) on:

- network security,
- trusted systems technologies,
- privacy enhanced mail,
- authentication, and
- dual-use technologies through gigabit research projects.[604]

Also, although only established in 1991, the initiative was already reorganizing. A new program component area (PCA), Information Infrastructure Technology and Applications (IITA), was added to enable the integration of critical information systems. This new research focus did have as one of its mandates to "integrate developments in mechanisms in enhanced privacy and security into a scalable systems context." Intended research and development by DoE and NSA in this new PCA was envisioned in the areas of:

- secure information resources discovery and retrieval,
- intrusion detection,
- multi-realm cross authentication,
- smart card technologies,
- secure electronic commerce,
- secure distributed engineering and design environments, and
- biometric identification evaluation.

[604] The implementation plan did note that key management issues and choice of either dynamic or static algorithms for digital signature and encryption still needed to be settled.

The implementation plan also recognized within several PCAs the importance of security, particularly relative to the proposed National Information Infrastructure (NII). In the National Research and Education Network (NREN) PCA:

- recognized the importance of developing an infrastructure of network services, such as security and authentication, with standard interfaces (but the emphasis is more on developing standard interfaces for services to preclude duplication of services than on security);
- acknowledged the need for a realistic, scalable, deployable national and international security architecture to manage and control the interconnected NII;
- NSA planned to develop
    - the policy mechanisms and methodologies for a secure operating system based on the Synergy microkernel prototype;
    - associated software and hardware for ensuring network integrity, controlling access and protecting data from unauthorized use; and
    - a high speed network testbed to explore network security issues; and
- DoE planned to make Kerberos-based authentication services available in full production basis across its Esnet and to establish a distributed computing test bed for evaluating security, among other functions.

Within the Advanced Software Technology and Algorithms PCA, proposed FY 95 security R&D intended to:

- improve system reliability through software portability and software libraries by demonstrating a prototype system for access and retrieval of reusable software;[605]
- develop the underlying infrastructure services for authentication, authorization, privacy, and security;
- sponsor research by the National Science Foundation to create a more effective software development paradigm and technology base founded on the principles of composition and solid architecture rather than construction and ad hoc styles;
- sponsor research by NASA on software program debugging tools; and
- continue NIST research and development of programming interfaces for digital signature, authentication, and other security services, and an information technology security accreditation program by creating and publishing specifications for security, reliability and integrity requirements.

Although not participating in the HPCC program, the National Telecommunications and Information Administration (NTIA) of the Department of Commerce was providing funding to develop networking projects.[606]

B. Fiscal Year 1995.[607] FY 1995 continued FY 94's emphasis on technical development, efficiency, cost-effectiveness, and affordability. The NSTC foresaw an urgent need to develop the administration approved NII as quickly as possible for the health and welfare

[605] NASA had sponsored the HPCC Software Exchange Experiment in FY 93 to provide the infrastructure of interconnected software repositories for sharing and reusing software modules (United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 95 Implementation Plan).

[606] United States Office of Science and Technology Policy, High Performance Computing and Communications: Toward a National Information Infrastructure.

[607] United States Office of Science and Technology Policy, High Performance Computing and Communications: Technology for the National Information Infrastructure and United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 1995 Implementation Plan.

and economic competitiveness of the nation into the 21st century. Proposed FY 95 funding for High Performance Computing and Communications research and development was $1,154.7 million, a 23 percent increase over the appropriated $937.9 FY 94 funding.[608]

Network security was acknowledged as "vital to HPCC agencies and to many other users such as the medical and financial communities" as part of the proposed NII. The Computer Emergency Response Team (CERT), DoE's Computer Incident Advisory Capability (CIAC), the Forum for Incident Response and Security Teams (FIRST), and other unauthorized entry response teams that monitor and react to unauthorized activities, potential network intrusions, and potential system vulnerabilities were also finally recognized at the policy making level as essential to security of the network.

These emergency response capabilities had been created by different federal departments or agencies (in cooperation with industry and/or academia in many cases) late in the 1980s and early 1990s as an operative (tactical) response to increasing intruder activity. This emergency response capability creation and legitimization process provides further empirical evidence for the earlier advanced contention that the process of providing information infrastructure system security followed the previously introduced (Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy) international relations regime-building model instead of the normal bureaucratic model's top-down direction. Bottom-up initiation of action slowly created critical masses of like-minded organizations to gain

[608] United States Office of Science and Technology Policy, High Performance Computing and Communications: Technology for the National Information Infrastructure.

acceptance at higher and higher levels of authority until the notion gained greater and greater universal acceptance.

FY 95 security-related research emphasized:

- gigabit encryption systems and use of KERBEROS authentication system, digital signatures, and privacy-enhanced mail to improve confidentiality;[609]
- certifying and accrediting information sent over a network to improve integrity;
- developing firewalls and other authorization mechanisms to better guarantee information integrity and availability by protecting the infrastructure from intrusion attacks;
- developing process shadowing, reliable distributed transaction protocols, and event and data redo logging to keep data consistent and up-to-date in the face of system failures to increase availability and integrity;[610]
- incorporating security in the management of current and future networks by protecting network trunks and individual systems, and
- developing emerging software tools (for example, debuggers and production environment tools to schedule jobs, multitask, implement quotas, and provide on-line documentation) to correct the fundamental software vulnerability of the information infrastructure system while also enhancing availability and integrity.[611]

[609] United States Office of Science and Technology Policy, High Performance Computing and Communications: Technology for the National Information Infrastructure.

[610] United States Office of Science and Technology Policy, High Performance Computing and Communications: Technology for the National Information Infrastructure.

[611] Evolving conventions and standards that enable developers to transport software to different architectures with the same structure were thought to facilitate and to standardize the software development process and improve both availability and integrity (United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future).

C. Fiscal Year 1996.[612] In FY 1996, the NSTC identified "high confidence systems that will provide the availability, reliability, integrity, confidentiality, and privacy needed by the Nation's ubiquitous information infrastructure" as one of six "Strategic Focus Areas for R&D that will benefit the nation's diverse users of information," but does not fund research directly related to the issue. At the same time, the same report stresses that software and services technologies are needed to "facilitate a marketplace" of advanced distributed applications that will operate over the underlying networking infrastructure.[613]

The Council recognized that the challenge would be to provide security solutions that can scale to emerging technologies such as multimedia, ultra-high data rates, mobile computing, and very large-scale distributed information storage and retrieval.[614] The supplement recommends $1,142.7 million, approximately a 10 percent increase over FY 1995 appropriated funding for research and development of HPCC initiatives in FY 1996.

To further develop the NII initiative, the NSTC endorsed the following current programs and proposed research:

- the HORUS project to create an environment for reliable distributed computing with fault tolerance to detect and react to failures and make distributed network software easier to develop;
- the TRAVELER project that searched for ways to provide security for mobile computers;

[612] United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future.

[613] United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future, 29.

[614] United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future, 32-33.

- the Synergy system that will be integrateable, scalable, and suitable for use by commercial carriers, by third-party providers of security services, and by applications for embedded security functions;
- the NSF Supercomputer Centers' use of one-time password and Kerberos authentication system for future extension to the entire Internet;
- addition of cross-realm functionality to Kerberos to support multi-site multi-organizational collaborative research and the SILDS project for billing, payment, accounting and associated privacy mechanisms;
- addition of secure http enhancements to the National Computational Science Alliance (NCSA) Mosaic to create Secure-Mosaic and its incorporation into CommerceNet;
- coordination of ARPA, NSA, and the Defense Information Infrastructure (DII) research programs in digital signatures, e-mail security, secure operating systems, secure distributed applications over a single administrative domain, secure routing protocols, security checking, and survivability and recoverability for collaborative document preparation and enhanced security for the next-generation World Wide Web (WWW) architecture;[615] and
- an effort by NASA to improve the protection of sensitive but unclassified data used in collaborative aeronautics engineering between the Federal government and industry.[616]

[615] United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future, 29-31.

[616] United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future, 32-33.

HPCC agencies were also responding to widespread malicious, network-based attacks by increasing emphasis on security research and prototype deployment. ARPA, DoE, NASA, NIST, and NSA were specifically addressing:

- preventing unauthorized entry into computing systems,
- protecting the network infrastructure from external and internal attack,
- protecting information in repositories and in transit,
- providing data security controls within applications,
- privacy protection for medical and other sensitive applications,
- secure electronic commerce,
- secure internetworking for distributed simulations,
- secure collaborative work, and
- security in emergencies, crises, hazards, or emergency response.[617]

D. Fiscal Year 1997.[618] In FY 97, the NSTC once again continued the thrust of technical efficiency through technological development with support of:

- an Information-Wide-Area-Year (I-WAY) project to demonstrate local and national high performance networking,
- reduction of costs in graphics rendering,
- improvements in low latency rates for local area distributed computing applications,
- formal theoretical methods for verifying complex chip design,

[617] United States Office of Science and Technology Policy, High Performance Computing and Communications: Foundation for America's Information Future.

[618] United States Office of Science and Technology Policy, High Performance Computing and Communications: Advancing the Frontiers of Information Technology.

- formation of an Applications Council to speed the early application of Computing, Information, and Communications (CIC) technologies throughout the Federal government.

Even after endorsing high confidence systems as a strategic focus area the previous year, there are no purely information infrastructure system security-related expected milestones for FY 1997. The FY97 supplement requests $1,038 million in research and development funding, a decrease in the $1,043 million authorized by Congress in FY 96.

As part of reorganization, the HPCC program's efforts were reorganized from the six Strategic Focus Areas of FY1996 into five new Program Component Areas (PCAs) to reflect high priority investment areas by the Federal agencies that participated in the coordinated R&D programs:

- High End Computing and Computation (HECC);
- Large Scale Networking (LSN);
- High Confidence Systems (HCS);
- Human Centered Systems (HuCS); and
- Education, Training, and Human Resources (ETHR).

The new PCAs were intended to focus research and development more on the Grand Challenges and National Challenges, to include national security and national defense where the goal was to improve civil and defense infrastructure (transportation, energy, and communications systems) and to protect critical information systems against attack and during emergencies.[619]

[619] United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 97 Implementation Plan.

communications systems) and to protect critical information systems against attack and during emergencies.[619]

Security of the technology and its applications gained some prominence with this reorganization; both security-related research (High Confidence Systems) and networks (Large Scale Networking) became PCAs. The LSN PCA's goal was to assure U.S. leadership in communications in high performance network components through technical development, engineering, and management, but omits research of network security vulnerabilities although network management and authentication were planned research and development focus areas.

HCS strove to develop technologies that provided users with high levels of security, protection of privacy and data, reliability, and restorability of information services. HCS research was envisioned to integrate fields of research and create standard metrics for properties such as safety, security, performance, and reliability. The limits of composability were also to be explored to determine if there are collections of high confidence properties (e.g., security and performance) that could not be derived from compositional principles. Fields of high confidence systems research included fault tolerance, real time operation, security, and functional correctness. HSC PCA requested funding for FY 97 was $30.04 million; less that 3 percent of the $1,043.02 million requested for all HPCC PCA programs.

The HCS PCA R&D focused on:

- the information infrastructure system's reliability, resiliency, and survivability for only national defense secure systems through

[619] United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 97 Implementation Plan.

•• management of networks under load, failure, or intrusion[620] through DARPA's Network Security Activity's collaboration with the Defensive Information Warfare program and NSA's Secure Operating System Development Program and Synergy research program;[621]

•• emergency response;

•• firewalls;[622]

•• secure enclaves;

•• formal methodology;

•• high speed cryptography for information security in virtual laboratories through NSA's High Speed Data Protection Electronics Program; and

•• infrastructure protocols for secure and reliable networks;

- security and privacy of sensitive unclassified data (patient records, electronic commerce, and emergency management) through:

•• personal identification,

[620] Researchers were developing new specification-based intrusion detection techniques to detect even types of attacks that have never been seen before and a communications thumbprinting scheme to trace attackers' activities widely over a network (United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 97 Implementation Plan).

[621] NSA was developing an "open architecture" along with secure distributed system prototypes based upon security policy-flexible, operating system micorkernels that would integrate the INFOSEC research work in computer misuse and anomaly detection (audit/intrusion detection); real-time, multimedia availability; network security management; high-speed networking; and secure database management systems (United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 97 Implementation Plan).

[622] Firewall research was being combined with a Domain and Type Enforcement security mechanism that could flexibly restrict which clients can use what applications and services over a network to increase the system's integrity. A public key certificate infrastructure based on an open architecture and security policy flexible operating system microkernels were being developed for cryptographic authentication and authorization. For more immediate improvement of confidentiality and integrity, the Kerberos authentication system was extended to allow use of public-key cryptography and digital signatures (United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 97 Implementation Plan).

- •• access control,
- •• authentication,
- •• encryption and other privacy assurance techniques,
- •• public key infrastructures,
- •• trusted agents for secure distributed computing, and
- •• telemedicine testbed networks;

- remote operation of scientific instruments and surgical procedures;
- restorability;
- testing and evaluation.
- interoperability standards; and
- reliability and security for mobile computing environments.[623]

The HECC PCA security-related research included:

- better theoretical verification of complex chip design, fault-detection, and recovery;
- resource allocation across multiple administrative domains;
- multi-level security for better data availability and integrity; and
- long-term research in system software technologies, advanced simulation techniques, and fast, efficient algorithms for simulation and modeling to improve the reliability of software design and development.

Within the LSN PCA:

[623] United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY97 Implementation Plan.

- long-term research in advanced network components and technologies for engineering and management of large-scale networks was thought to optimize not only the efficiency of these networks, but also improve security.
- DARPA, to increase survivability, was developing multi-cast communications protocols for distributed systems that would continue to provide reliable service even when a compromised processor behaved maliciously.
- DARPA's Scalable Systems and Software Program supported the development of computing and advance software technologies needed to enable the development, introduction, and use of effective, reliable, and secure scalable and distributed high performance computing technologies. And,
- education about security, safety, functional correctness, performance in real time, and fault tolerance was to be organized and disseminated.

Although not programmed as HCS funds,[624] DoE continued and sponsored quite a few new programs in other PCAs designed to improve the confidentiality, availability, and integrity of existing and anticipated networks:

- Continued from FY96
  - •• security architecture that provides transparent and easily administered security services (now within the new HuCS PCA);
  - •• an initial design for a heterogeneous secure software system; and
  - •• a set of ER-DP security workshops with the goal of identifying common security R&D challenges within the LSN PCA;

[624] DoE had not programmed any funds for FY 97 for the High Confidence Systems PCA (United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY97 Implementation Plan).

- Proposed in FY 97 to:

  •• provide the adaptive secure high-speed communications library for evaluation and use and to prototype the Secure Software distribution system;

  •• develop a strategy, protocols, and tools that address congestion caused by WWW traffic (e.g., reliable multicast);

  •• secure information retrieval and search mechanisms and interoperable authentication realms during Gigabit research and development;

  •• develop information surety and security technologies and mechanisms integration in a distributed and multi-communications services base architecture during National Challenge research and development, and

  •• develop security procedures for voice and data transmission based on sending the data encapsulated in a chaotic signal and decoding the signal using techniques for controlling chaos.

NIST, through the development of standards, supported enhanced security for computers and communications systems, specifically through R&D in application programming interfaces for digital signature, authentication, and other security services and for reliable information exchange among applications. The healthcare agencies all sponsored some research for secure storage and transfer of patients' records.

E. Fiscal Year 1998.[625] In FY 1998, computing, information, and communications (CIC) security (especially of networks) gained some balance with technology development and

[625] United States Office of Science and Technology Policy, High Performance Computing and Communications: Technologies for the 21st Century, Committee on Computing, Information, and Communications, National Science and Technology Council, Supplement to the President's FY 1998 Budget,

deployment. Although there is even recognition of the critical role of IT and IT security in the nation's long-term security, the primary emphasis was still on research to solve efficiency bottlenecks and bring the next technological advance to rapid deployment and integration.[626]

The NSTC, in its annual report focused exclusively on the promise of digital technology to transform every sector of the economy by "harnessing information technology" and dismissed, or at least discounted, system security.[627] Of the 15 research areas identified in the report as priorities for the FY 1998 budget preparation, none were directly related to information or other critical infrastructure security.[628] Even in addressing its goal to "enhance national security and global stability," the Council in its annual report spoke only to the collaboration and coordination needed to solve the problems for global stability. The NSTC's Committee on National Security focused its attention on R&D initiatives concerning nonproliferation and technology transfers![629]

The budget request for FY 98 research and development was $1,103.7 million, an increase of about 9 percent over the $1,008.5 million appropriated in FY 97. However, the HCS funding request for FY 98 was only $33.2 million, still only about 3 percent of total requested funding for research and development.

November 1997 and United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 1998 Implementation Plan.

[626] "CIC R&D programs help Federal departments and agencies to fulfill their evolving missions, assure the long-term **national security**, better understand and manage our physical environment, improve health care, help improve the teaching of our children, provide tools for lifelong training and distance learning to our workforce, and sustain critical U.S. economic competitiveness" (United States Office of Science and Technology Policy, High Performance Computing and Communications: Technologies for the 21st Century, 1).

[627] United States White House, National Science and Technology Council Annual Report, 1997, National Science and Technology Council, Washington, D.C., April 1998.

[628] United States White House, National Science and Technology Council Annual Report, 1997.

[629] United States White House, National Science and Technology Council Annual Report, 1997.

The dominant thrust within the Large Scale Networking PCA continued to be on the "efficient development and execution of scalable distributed applications" and increasing the capacity, networking services, and media of the future network.[630] The PCA adopted the Next Generation Internet initiative as its dominant focus where all security, reliability, and privacy issues were to be investigated.[631] The NGI initiative was to invest R&D funds for new networking technologies that demonstrated new applications in distance education, telemedicine, national security, and collaboratories.[632]

The High End Computing and Computation (HECC) PCA as part of its focus on advances in hardware and software for high end (teraflops- and petaflops-scale) complex computing and algorithms for modeling and simulation was investigating new backplane networks supporting security.[633] Within the High Confidence Systems PCA (the primary program component area concerned with security), research and development focused on technologies to achieve high levels of security, protection, availability, and restorability of information services to resist component failure and malicious manipulation and to respond to damage or perceived threat by adaptation or reconfiguration. FY 98 HCS PCA research, specifically, was to develop:

[630] Much emphasis is on reducing congestion (and even greater anticipated congestion) caused by Web traffic on the Internet through reliable multicast protocols and tools (United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 1998 Implementation Plan, 20).

[631] Initial information infrastructure systems' security emphasis is on transaction security. DARPA was prototyping flexible, efficient, and secure protocols in its Active Networks program (United States Office of Science and Technology Policy, High Performance Computing and Communications: Technologies for the 21st Century and United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 98 Implementation Plan).

[632] United States White House, National Science and Technology Council Annual Report, 1997.

[633] United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 1998 Implementation Plan, 14.

- protocols and mechanisms that allowed intrusion detection systems to detect, trace, and share information (GRIDS Intrusion Detection system);
- high assurance configurable security architectures through quality-of-service protocols (Quorum);
- privacy protection methods; and
- tools for assessing the vulnerability of the source code of any system element, including the computing system, the network, and the network information's content, procedures, or protocols used to create, store, transmit, route, reconfigure, receive, aggregate, or display data.

Interestingly, five (DoE, ED, NOAA, EPA, AHCPR) of the twelve participating agencies had no funds in their FY 1998 budgets dedicated to HCS research, although some security research and development is supported through other program component areas (e.g., LSN and HECC). Of course, NSA continued its research in cryptography to assure confidentiality. Other NSA information systems security research was now coordinated with DARPA's research in cutting edge technologies:

- a suite of information security services to implement security technology with minimal disruption to existing systems;
- standards for secure interoperability of non-homogeneous computer and telecommunications systems;
- robust secure network management techniques to provide flexible authentication services through access control mechanisms that could be layered over existing operating systems;

- secure transaction and technologies for increasing systems' reliability and recoverability under conditions of load failure;
- Secure Access Wrapper (SAW) to access commercial off-the-shelf (COTS) and legacy databases in very large-scale information systems;
- Task-Based Authorization (TBA) for access control to distributed computing; and
- determining and countering optical network vulnerabilities through attack-resistant network control and management algorithms for a Secure All-Optical Network.

The National Library of Medicine and the Veterans Administration were engaged in research in technologies for accurately and confidentially storing and transmitting patients' records. Finally, the National Institute of Standards and Technology was developing:

- standards for reliable information exchange,
- standards and test methods for cryptographic modules,
- test methods for security products and systems,
- infrastructure for public key based security, and
- common architectures that promote use of strong authentication technologies.

F. Fiscal Year 1999.[634] In FY 99, the emphasis once again continued to be on efficiency through rapid development and deployment of information technology. The supplement to the budget requests $860.9 million for CIC research and development, without any request

[634] United States Office of Science and Technology Policy, High Performance Computing and Communications: Networked Computing for the 21st Century, Committee on Computing, Information, and Communications, National Science and Technology Council, Supplement to the President's FY 1999 Budget, August 1998.

for funding of programs previously found within the High Confidence Systems Program Component Area that was abolished.

The NSTC Committee on National Security did "investigate infrastructure protection research" while continuing its work on nonproliferation and technology transfer. As part of that investigation:

- a series of organizational meetings were conducted,
- a comprehensive review of infrastructural vulnerabilities was completed,
- R&D efforts effective in reducing vulnerability(ies) were identified,
- gaps in R&D and shortfalls in funding were identified,
- a comprehensive draft R&D plan was developed, and
- R&D priorities were established.[635]

Also, as a result of the Committee on National Security's organizational review, the Federal Information Services and Applications Council (succeeding the former Applications Council) was created to foster faster migration of technology from the information technologies R&D community to government agencies and information services communities. Further, the management organization for research and development was reorganized in December 1997, and the High Confidence Systems Program Component Area (the previously designated security-related PCA) was no longer reported through the NSTC or the HPCC program.[636]

[635] United States White House, National Science and Technology Council Annual Report, 1998, National Science and Technology Council, Washington, D.C., March 1999.

[636] United States Office of Science and Technology Policy, High Performance Computing and Communications: Networked Computing for the 21st Century.

Some security-related research and development was being conducted by the two PCAs still managed by the NSTC: High End Computing and Computation (HECC) and Large Scale Networking (LSN). Within HECC, research continued on debugging and performance tools:

- One project in FY 98 had developed methods and implementations to allow highly secure execution of code downloaded from untrusted sources through theorem-proving software at the receiving site that verified the downloaded code's desirable safety characteristics. If either the code or the proof had been tampered with or otherwise corrupted, the proof would fail. And,
- DARPA funded research through its Information Survivability program that focused on developing an architecture for low-power configurable computational elements and real-time adaptive control and resource management that could be used to guarantee minimum essential continued operation of critical system functions in the face of concerted information warfare attacks by providing distributed computing between secure enclaves with strong barriers to detect, isolate, and repel malicious and suspicious activity.[637]

During the previous year:

- the Committee on Technology had overseen the publication of the Next Generation Internet (NGI) Plan and a demonstration of technologies and applications being

[637] Boeing Corp. has developed and successfully demonstrated the Intruder Detection and Isolation Protocol that uses cooperative exchange of information between network components to isolate and cut off an attack. An automated tool for analysis of vulnerabilities in source code had been developed and tested. Through the use of a code called a kernel hypervisor, the Web can be browsed so that only the files specifically permitted by the user will be affected by any actions initiated by the browser or its children (United States Office of Science and Technology Policy, High Performance Computing and Communications: Networked Computing for the 21st Century).

developed under the NGI initiative (Netamorphosis). Goal 1 of the NGI states that "research, development, and experimentation... should add functionality and improve performance in reliability, security and robustness" (along with other attributes);

•A Networking Research Team was to

•• coordinate the networking research of the LSN agencies, to include research in privacy and security[638] and

•• add, as suggested by the FY 2000 Interagency Research and Development Priorities (Jones-Lew Memorandum), a critical infrastructure protection area of special emphasis to promote and coordinate research to reduce vulnerabilities and to develop technologies that will detect, contain, and mitigate attacks against or other failures in these infrastructures;[639] and

• NASA funded and managed research in advanced network technologies that were richer in features, higher in performance, and deliverable at a reasonable cost.[640]

Also, in FY 98, NIST had:

• completed a reference system for the IP Security (IPSEC) protocol;

• completed a WEB-based Interoperability Tester (WIT) for IPSEC that allowed vendors to test against the same reference without downloading and installing the reference system;

[638] United States Office of Science and Technology Policy, High Performance Computing and Communications: Networked Computing for the 21st Century.

[639] United States White House, National Science and Technology Council Annual Report, 1998.

[640] United States Office of Science and Technology Policy, High Performance Computing and Communications: Networked Computing.

- developed and issued a Minimum Interoperability Specification for Public Key Infrastructure Components to ensure that PKI components from multiple vendors would interoperate across entire networks and the Internet;
- conducted collaborations in internet security with the Government Information Technology Services (GITS) Innovation Fund in the use of advanced network security mechanisms such as Kerberos, security smart cards, secure messaging, and PKI components;
- begun identifying, evaluating, and establishing the advanced encryption standard, intended to replace the existing Data Encryption Standard (DES) as the standard algorithm for symmetric key encryption and the encryption capability of the 21st century;
- established the Federal Computer Incident Response Capability (FedCIRC) to monitor threats to, receive notification of, analyze vulnerabilities of, and support response to incidents on the information infrastructure system;
- focused on improving the needed high degree of confidence in software used in mission-critical functions, managing high value assets, or embedded systems; and
- fostered the development of formal laboratories to test and certify security products against published formal specifications.

NSA continued mathematical cryptographic research to produce more secure and efficient algorithms for privacy protection and authentication, as well as developing better techniques for integrating security services into commercial products and services. It also continued to research:

- optical encryption technology (fabricating etched mirrors on semiconductor laser surfaces),
- high speed/low power electronics (for greater efficiency in encryption),
- improved biometric authentication techniques,
- new visualization and risk assessment tools [a prototype tool to analyze the characteristics of decision tables (Tablewise)], and
- security enhancements for the next generation operating systems and for object technology (the Internet Security Association and Key Management Protocol).

Of those activities previously reported within the HCS PCA, research and development continued on assurance technologies, information security, information survivability, protecting the privacy of medical records, and secure programming languages.[641]

- The National Science Foundation was sponsoring research on the security of mobile code systems such as Java which had led to the extended stack inspection model; and
- the Federal Aviation Administration was sponsoring research to rigorously define architecture constraints to protect safety-critical processes from non-safety-critical components and approaches for structural test coverage analysis.[642]

G. Fiscal Year 2000.[643] The FY 2000 Supplement to the President's Budget proposed $366 million in funding priorities to implement the Information Technology for the Twenty-first

[641] United States Office of Science and Technology Policy, High Performance Computing and Communications: Networked Computing for the 21st Century.

[642] United States Office of Science and Technology Policy, High Performance Computing and Communications: Networked Computing for the 21st Century.

Century Initiative (IT^2) which had concluded that the Federal government had been underinvesting in long term information technology research relative to its importance to the nation. The Committee proposed $1,462 million in research funding for FY 2000, an 11 percent increase over the $1,314 million appropriated in FY 1999.[644]

The budget recommended funding for security within several program component areas. In the High End Computing and Computation PCA, the NSTC proposed to support research and development in software and system architecture that could solve some of the inherent information infrastructure system vulnerabilities and theoretical foundations of cryptography and computational complexity. Specifically, the report supported research in distributed and network environmental issues, including software security and parallel computing complexity through modular parallel sparse matrix solvers and software tools for unstructured mesh computations on distributed-memory computers.[645]

Within LSN:

- a proposed Internet Security Team (IST) was to facilitate testing and experimentation with emerging advanced security technologies and serve as a focal point for application and engineering requirements for security systems;
- the Department of Energy was to conduct research and development on:
  - •• security for high speed services to applications,
  - •• routing and congestion control,
  - •• differentiated services to applications,

[643] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.
[644] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.
[645] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.

•• manageable security infrastructure and architecture,

•• integration of services across autonomous systems and networks,

•• network performance measurement and management,[646]

•• networking technologies to add functionality and improve performance in Internet security, and

•• network robustness and reliability through revolutionary applications in enabling technologies such as distributed computing and privacy and security;[647] and

• the NSF's Internet Technologies program was to focus not only on the fundamental science and technology needed to facilitate the efficient, high speed transfer of information through networks and distributed systems, but also on network security, design, and architecture to make them more reliable and robust.[648]

Within the HCS PCA (restored after being deleted from the budget in FY99), research and development was to "develop technologies for achieving predictably high levels of computing and communications system availability, reliability, safety, security, and

[646] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.

[647] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.

The 1998 NGI Research Act provided the impetus for most of the proposed research as well as:

• NASA testing of Quality of Service technologies that provide preferential treatment to select applications to replace dedicated circuits supporting critical network applications such as mission control when networks are congested;

• NIST to extended the Internet Engineering Task Force Internet Protocol Security protocols which provide a platform for research into Internet security systems integration; and

• The National Library of Medicine to demonstrate the use of the NGI for transfer of massive amounts of data accurately, securely, and almost instantaneously (United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium).

[648] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.

survivability" from internal and external threats and natural disasters.[649] To intensify the effort to provide assurance, reliability, and security, the HCS agencies through an HCS Working Group were developing an HCS national research agenda to provide a scientific supporting theoretical basis; tools and techniques; and engineering and experimentation for critical information technologies to address challenges such as increased reliance on software and on a commodity technology base, increased scale and complexity, stress due to system performance demands, demands for interconnectivity, rush to market, and threat.[650]

Through the Information Security (INFOSEC) Research Council's coordination of NSA's, DARPA's, DoE's, NIST's and DoD's service laboratories' research, the following projects were to be supported by the NSTC and the HPCC program:

- NSA's:
  - active network defense,
  - secure network management,
  - network security engineering for globally distributed systems and services coupled with dynamic and pervasive information sharing, collaboration, cryptography, and secure communications technology; and
  - a DoD Minimum Essential Information Infrastructure (MEII) as recommended by the Defense Science Board in 1996.[651]

[649] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.
[650] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.
[651] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.

- DARPA's
  - intrusion detection systems to detect intrusions, assess damage and suggest the appropriate response while allowing crisis-mode operation of critical infrastructure components and
  - modular security services of integrated secure and fault-tolerant operating systems, firewalls, and system management tools;[652]
- NSF's computing-communications research;
- NIST's and NSA's National Information Assurance Partnership;
- NIH's research in protecting patient's records; and[653]
- NASA, NSF and NIST's:
  - high performance networking environments,
  - fault-tolerant and redundant hardware structures,
  - high confidence systems,
  - secure Internet programming using Java and several derivatives,
  - programs to enhance consumer confidence in the quality of commercial security products,
  - access control and software development and analysis tools,
  - testing technologies, and
  - standards.

[652] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.

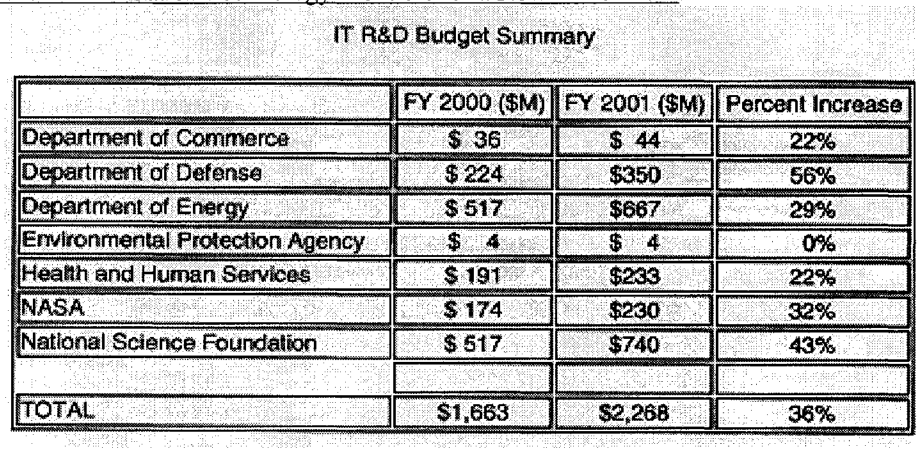
[653] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.

Even within the Human Center Systems (HuCS) Program Component Area, research was to be conducted through the Digital Libraries Initiative, Phase Two, to extend the security and privacy of multimedia databases through a security mediator for the Web and to make government more accessible to the public without comprising privacy and security – both the individual's and the Government's.[654]

5.4. Recapitulation of HPCC Program Funding.

Discrepancies in funding figures in the annual HPCC Supplements to the President's Budget and the separate annual HPCC Implementation Plans further supports the argument of confusion and lack of direction in early attempts to address information infrastructure systems security, coordinated R&D, and the difficulty in locating data. Even as late as 2000, trying to locate accurate funding data is tedious and the result tenuous at best. Three documents exist that provide the IT R&D requests: the FY2000 Budget; a supplement from the Office of the White House to the President's Press Conference on January 21, 2000;[655] and an IT R&D Handout for FY2001 Budget Rollout

[654] United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium.



IT R&D Budget Summary

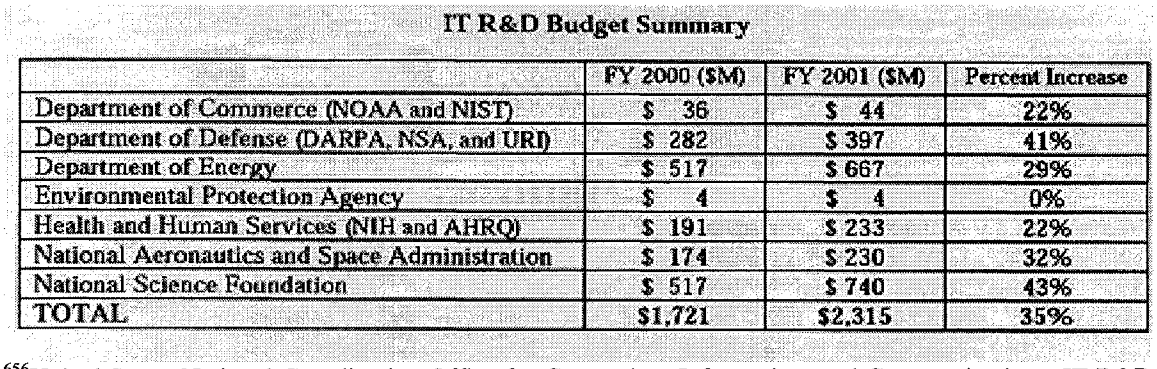
	FY 2000 ($M)	FY 2001 ($M)	Percent Increase
Department of Commerce	$ 36	$ 44	22%
Department of Defense	$ 224	$350	56%
Department of Energy	$ 517	$667	29%
Environmental Protection Agency	$ 4	$ 4	0%
Health and Human Services	$ 191	$233	22%
NASA	$ 174	$230	32%
National Science Foundation	$ 517	$740	43%
TOTAL	$1,663	$2,268	36%

[655] United States White House, "President Clinton Announces Nearly A $3 Billion Increase in Twenty-First

by the National Coordination Office on February 7, 2000.[656] The figures in Table 5.2. Recapitulation of Funding for High Performance Computing and Communications (HPCC), FY 1993 – FY 2000 are the largest sum from either source in order to show the best-case situation.

Although not specifically about security-related research, the Joint Security Commission's statement does provide a benchmark by which to measure the performance of the federal government for information infrastructure system security. If one extrapolates the Commission's statement and its philosophy from IT security funding in general to IT security-related R&D, then five to ten percent of all federal information technology research and development funds should be devoted to information system security R&D. As can be easily seen from the chart, at no time (with the exception of FY2000) did HPCC security-related R&D funding approach the Joint Security Commission's standard of 5-10 percent when the data on security-related R&D could be

Century Research Fund.



IT R&D Budget Summary

	FY 2000 ($M)	FY 2001 ($M)	Percent Increase
Department of Commerce (NOAA and NIST)	$ 36	$ 44	22%
Department of Defense (DARPA, NSA, and URI)	$ 282	$ 397	41%
Department of Energy	$ 517	$ 667	29%
Environmental Protection Agency	$ 4	$ 4	0%
Health and Human Services (NIH and AHRQ)	$ 191	$ 233	22%
National Aeronautics and Space Administration	$ 174	$ 230	32%
National Science Foundation	$ 517	$ 740	43%
TOTAL	$1,721	$2,315	35%

[656] United States National Coordination Office for Computing, Information, and Communications, IT R&D Handout for FY2001 Budget Rollout by the National Coordination Office, Washington, D.C., February 7, 2000.

Table 5.2. Recapitulation of Funding For High Performance Computing and Communications (HPCC), FY 1993 - FY 2000

(Figures in Millions Dollars)

	REQUESTED	APPROPRIATED	SECURITY RELATED	SEC-REL % OF APPR
FY 91		489.4		
FY 92		655 (655)		
FY 93		805 (795)		
FY 94	1,096	937.9* (938)		
FY 95	1,154.7	1,038 (1,129)		
FY 96	1,142.7	1,043.02 (1043)	30.04	2.9 (2.9)
FY 97	1,038.48	1,008.5 (1009)	30	2.9 (2.9)
FY 98	1,103.7	1,069.5 (1074)	33.18 (26.31)	3.1 (3.1)
FY 99	860**	828 (795)		
FY 00	919	(911)	103.5 (requested)	11.2
TOTALS	**7,314.58**	**7,874.32**	**196.72**	

*includes funding from additional agencies that joined the HPCC program's R&D.

** HCS, HuCS, & ETHR funding not included due to re-organization of NSTC.

Note: Data in parentheses are contained in a historical recapitulation of the HPCC's funding in the HPCC FY 1999-2000 Implementation Plan.

Extracted from the program's budget. One can only hope that the federal government is finally providing IT security-related R&D funding that its publicly expressed level of seriousness from FY1991 would merit and that the FY2000 funding is the beginning of a trend instead of an isolated incident.

In the best-case scenario that FY 2000 is indeed a watershed event that marks a turnaround in funding, technical solutions to the information infrastructure system's vulnerabilities are much more likely to be discovered and developed. However, even at the FY2000 elevated level of spending, funding for security-related R& D does not approach the level of funding spent for the Strategic Defense Initiative (a.k.a. "Star Wars"), another equally technologically dubious national security project. SDI had spent almost $27.6 Billion through FY1996 (in FY96 dollars) since first proposed in 1983. SDI was expected to cost between $100 Billion and $1 Trillion when completed, if the technology could ever be developed.[657] The $7.874 Billion spent on information technology R&D (and the $196.72 Million on security-related R&D) through FY 2000 by the HPCC Program only makes the government's true feelings about the information infrastructure system's national security risk clearer.

Admittedly, information technology's $7.84 Billion is only for R&D and covers only one R&D program (HPCC) within the federal government, but it can provide a convincing comparative analogue for the level of funding. Even when compared to the IT R&D funding in the "President's Supplement" and the "IT Handout" instead of just the HPCC Program, one can more clearly see the discrepancy between IT security and SDI.

[657] Stephen I. Schwartz, U.S. Nuclear Weapons Cost Study Project, Education Foundation for Nuclear Science, Bulletin of the Atomic Scientists, July 5, 2000, http://www.thebulletin.org/issues/1995/nd95/nd95.schwartz.html.

Further most of SDI's costs are research and development also and some of its costs are more than likely "hidden" in other parts of the budget (similar to IT R&D) so the comparison is not entirely skewed.

5.5. Conclusions.

Even a cursory examination of the research gives one the impression that there was plenty of information technology security-related research and development being conducted over the past decade. Given the seemingly expansive number of initiatives, one has to wonder why the Joint Security Commission I and II, the ISAT, and others decry the funding and the results of IT security-related R&D. The reasons seem to be organizational turbulence and inefficiency, inconsistency of focus and effort, and the lack of a commitment by the federal government to information infrastructure system security.

As can be easily seen from the history of HPCC program security-related R&D, the federal information infrastructure system security research and development organization over the decade resembles the information infrastructure system security policymaking organizational environment. Both are disorganized, short of accomplished goals, and do not show much evidence of a federal priority.

Organizationally, federal information infrastructure system security R&D over the past decade has not been well coordinated. Even though OSTP has the legislative mandate for coordinating scientific and technological approaches to national and international problems, there is little evidence the Director exercised that responsibility with respect to information infrastructure system security R&D.

The evidence does seem to suggest that only in the HPCC Program did the Director fulfill his mandate but that might be more a function of the organization of the program with the Presidentially appointed PITAC and NSTC advisory boards providing the impetus instead of OSTP.[658] And, the HPCC was probably just a small part of the federal information infrastructure system R&D effort. Much more information infrastructure system R&D that the Director should have been coordinating was more than likely being conducted by other agencies (DoD, DARPA, NSA, NIST, DoE, etc.) within the federal government.

Within the HPCC Program, one can observe a pattern of the organizational, funding, and priority turbulence that more than likely was less than what existed within the rest of the federal government since the HPCC was at least a centrally coordinated program. Even within the HPCC Program, organization for efficiency is suspect at best. The organizational figures of Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy demonstrates the difficulty of diagramming the relationships involved. Although nominally in charge, the Director of OSTP shares supervisory responsibility with at least three other organizations: The President's Information Technology Advisory Committee (PITAC), the National Science and Technology Council (NSTC), and the National Coordination Office for Computing, Information, and Communications (NCO/CIC) (not to be confused with the National Coordinator for Security, Information Protection, and Counter-Terrorism (NCSIPC-T) of the National Security Council). With both the PITAC and NSTC serving as presidential advisory organizations as well as either subordinate to or coordinating with the OSTP Director, the lines of communications and delineation of authority is bound to be somewhat less than clear or optimal.

[658] Both the PITAC and NSTC published studies detailing the vulnerabilities and the risks those vulnerabilities posed.

As can be seen from Figure 5.2. Number of Agencies Participating in HPCC Program, even the number of organizations participating in the Program is turbulent with organizations both joining and leaving over the life of the program:

FY 1991 – 8

FY 1992 – 8

FY 1993 – 10

FY 1994 – 10 (DARPA and NSA joined)

FY 1995 – 12 (VA and AHCPR joined)

FY 1996 – 12

FY 1997 – 12

FY 1998 – 12

FY 1999 – 10

FY 2000 – 10 (VA and Department of Education no longer included)

Figure 5.2. Number of Agencies Participating in HPCC Program[659]

With multiple organizations advocating their own research and development agendas, for the same reasons of competition discussed in Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy, a well-coordinated R&D effort is unlikely, even in the HPCC

[659] United States National Coordination Office for Computing, Information, and Communications, High Performance Computing and Communications: FY 1999 – FY 2000 Implementation Plan, Interagency Working Group on Information Technology Research and Development, Office of Science and Technology Policy, Washington, D.C., April 2000.

Program. This is even more unlikely when participants with their differing agendas enter and leave the program.

To obfuscate matters further, the HPCC Program has been reorganized internally at least five times since 1994. With particular respect to information infrastructure system security, a program component area focusing on security (High Confidence Systems) was created, abolished, and then re-instated all within five years, FY 1996-2000. In addition to the organizational consequences of such moves, this action speaks volumes about the federal government's attitude towards information infrastructure system security. The ability to sustain focus on particular directions of security-related research becomes especially more difficult since there was no program component area over the life of the Program to focus any effort that did exist.

As the research shows, there is scant consolidated federal information infrastructure system security or security-related R&D funding data available to analyze and from which to draw conclusions until 1999. The data available do indicate that in neither information technology security nor security-related R&D did the government meet the Joint Security Commission's standard of 5-10 percent funding for security within the past decade. However, what federal government funded research and development there is does tend to be focused on defense and national security research and not development.

The research could have benefited from a comparison of federal versus private sector security-related spending. Unfortunately, even scantier information than that available for the federal government's security-related spending exists for the private sector for much the same reasons: funding was not segregated according to function, record keeping was imperfect, and no attempt has been made to aggregate what data there is.[660] It is safe to say, though, that the level of security-related spending in the private sector, for

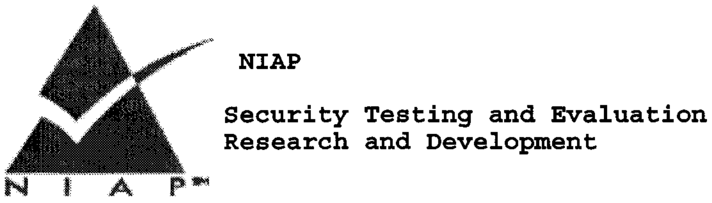
[660] I have tried to find data concerning the private sector's security-related spending. I have queried the industry's primary trade organization, the Information Technology Association of America (ITAA) with little result as evidenced by the following e-mail reply:

> "Mac, a good place to start -- to find the information that you are looking for -- might be the Institute for Information Infrastructure Protection, a consortium between industry and the academic community. They are located at Dartmouth University.
>
> Shannon L. Kellogg
> Vice President
> Information Security Policy and Programs ITAA
> http://www.itaa.org/infosec
> +1-703-284-5357"

I next queried the Dartmouth Institute for Information Infrastructure Protection (an industry–academe collaboration) with the same results (see e-mail response following)

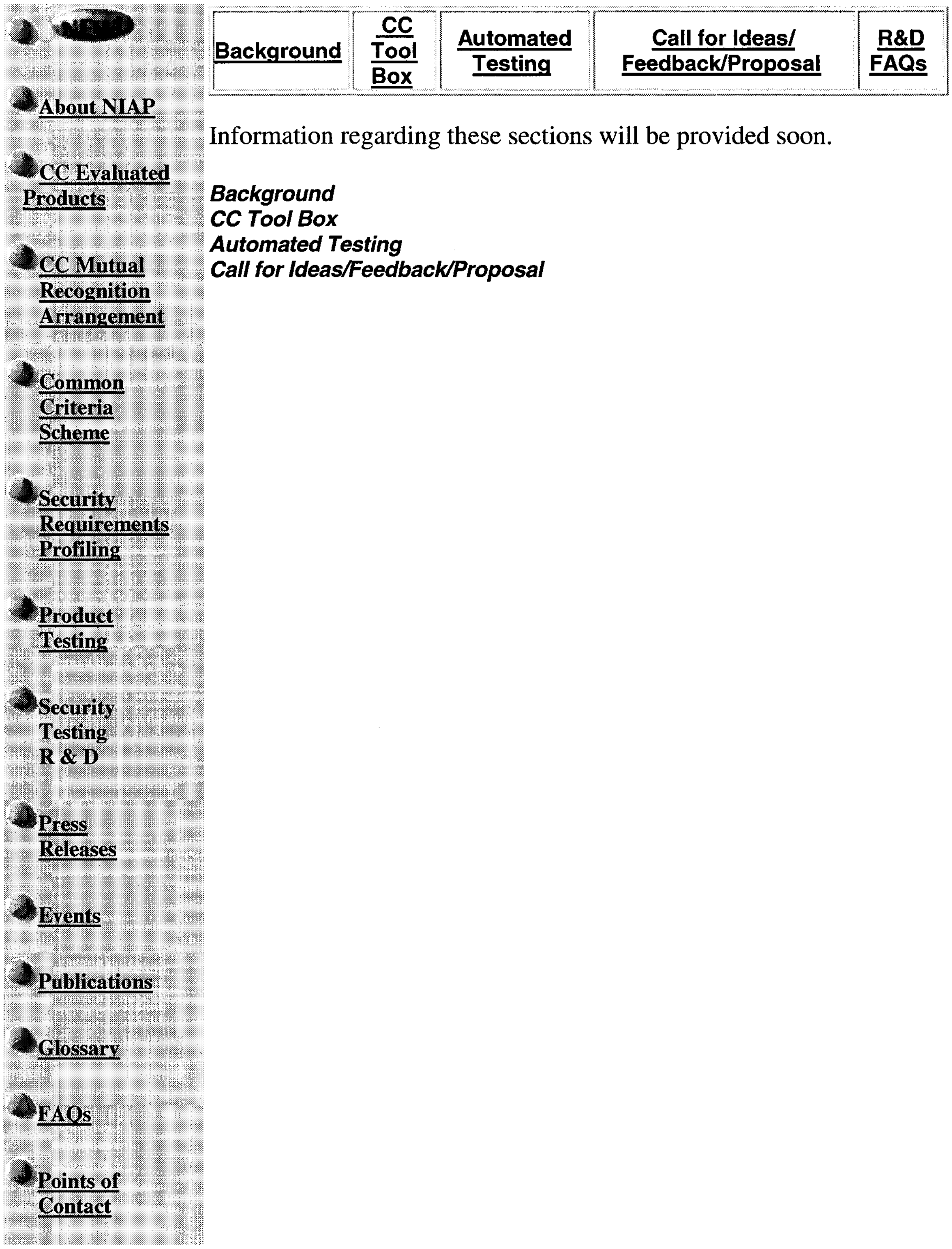
> "Mac:
>
> I am sorry for my delay in responding. T I3P does not have the data that you are looking for; we are a relatively new institution, and our interactions with industry to date have been largely focused on identifying the cyber security needs of critical infrastructure providers. We have surveyed existing government and academic R&D programs in cyber security, but are just beginning work on identifying relevant R&D in private industry.
>
> I am sorry not to be of more assistance. Good luck with your project, and I would certainly be interested in learning more about your findings.
>
> Best regards,
> Tracey Cote
> Institute for Information Infrastructure Protection"

I have also searched the Department of Commerce and NIST websites looking for data on private sector funding with no results. The National Information Assurance Partnership (a joint NIST/NSA activity) looks promising for the future but has nothing yet as seen from the this page from their Security Testing and Evaluation Research and Development webpage:



NIAP

Security Testing and Evaluation
Research and Development



Information regarding these sections will be provided soon.

Background
CC Tool Box
Automated Testing
Call for Ideas/Feedback/Proposal

I have sent a request to the NIAP asking if they have data of the IT industry's investment in security R&D over the decade of the 1990s but have yet to receive a response from them.

both security of existing system and security-related R&D, more than likely was less than, but surely not more, than the federal level of spending.

Further, corporations are just not interested in spending all the money necessary for security. What money that is spent for industry's market-driven research and development is most frequently spent on development at the expense of research to maximize investment since development will get a product to market much quicker than basic research will.[661] And, finally, I suspect separating federal from private sector spending would be hopeless. Federal funds are more than likely commingled with the private sector's to the point that they are inseparable, especially during most of the decade of the 1990s. HPCC (and DARPA) funds allocated for security R&D eventually ended up in the private sector. The federal agencies served only as a conduit for the funds to private firms or academic institutions that actually conducted the research and development. That is how the Internet was created; ARPA funded BBN to do the research and develop the network. So, even if one could locate funding data for private sector information technology security research and development, the probability of determining whether it was federal or private sector dollars would be hopelessly improbable.

Even within the HPCC Program, no detailed budget data are available for the program's initial two years (FY92-93); only the amounts appropriated by Congress to support the program. Then, because of the structure of the HPCC budgets in both the Supplements to the President's Budget and the Implementation Plans for FY94 and 95, no security-related funding information is available. R&D funding totals are available, but no

[661] Miller, 9 and ABCNews, "Computers: World Wide Warfare."

attempt is made to define security-related R&D funding within either the program components areas' or the participating agencies' individual budgets.

By examining the consolidated budget data in the table, Recapitulation of Funding for High Performance Computing and Communications (HPCC), FY 1993 – FY 2000, one can see that in those years where detailed budget information is available (FY96-98) the percentage of funds for security-related R&D is 3% or less of all information technology R&D in HPCC. Unfortunately, this sum is clearly less than the 5-10% recommended by the Joint Security Commission in its 1996 study as needed to provide security for the system. If one extrapolates from this admittedly small R&D effort to the rest of the federal government, then government-wide federal funding for information infrastructure system security-related R&D is sadly deficient when compared to the only standard available for security R&D investment.

Over the past decade, information technology, and the HPCC Program specifically, appear to have conformed to the model of an emerging technology: safety and security concerns are initially secondary to developing the technology's potential and efficiency. There is even anecdotal evidence that not enough funding is being applied to the R&D efficiency effort.[662] Outside of HPCC, there is little unclassified empirical evidence that the model is still not valid: the budget still has no consolidated data for IT security or security-related R&D, program descriptions do not necessarily identify projects as security or security-related, and there is still no national information technology security policy.

[662] Mr. Fred Tompkins, UNISYS Corp., related to me in a conversation in January, 2000, that the IT industry has traditionally worked on a five year application time for basic research, but the application time now is down to three years and is constantly diminishing.

Security R&D responsibility within the HPCC Program devolved from other functional area responsibilities (NREN, ATA, HECC, etc. PCAs) as the program expanded and security became a greater concern. Expressions of concern about, funding for, and organizational responsibility for the emerging information system's security, with the exception of confidentiality, are initially minimal but gradually become more visible as the technology matures and becomes more ingrained into the national economy and society. Information confidentiality was already an established security concern of earlier, more traditional means of communications and retained a predominant role in the emerging technology of HPCC security-related R&D from the beginning.

The High Confidence Systems PCA, specifically, supports the emerging technology model, at least within the HPCC Program. Its creation after six years of the Program's existence suggests that the IT community had begun to realize the criticality of security to operation of the system. Deactivation after only three years (FY97-99), and then re-establishment in a year (FY2000) suggests that the security versus efficiency issue was still being debated by the information technology R&D community with different camps being more persuasive at different times. Re-establishment of the program further suggests that the NSTC has once again determined that security is important enough to the system's operation to merit an exclusive focused effort.

The above statements are not meant to imply that many of the funded projects and the research and development foci did not lead to advances in information infrastructure

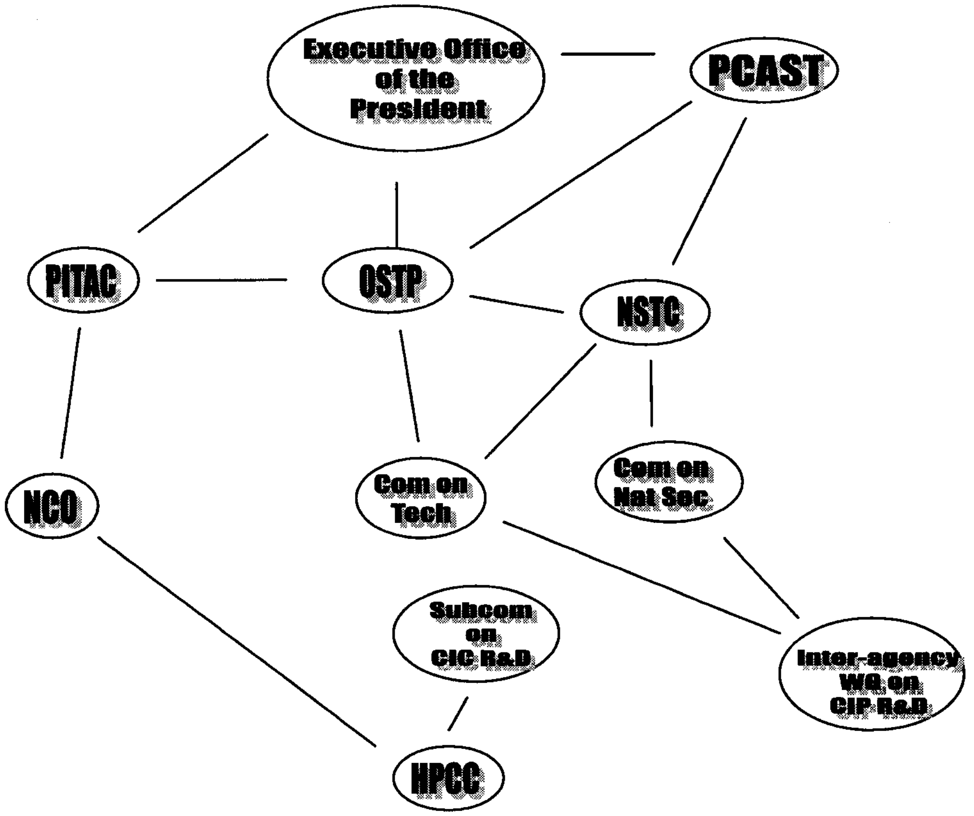


Figure 5.3. HPCC R&D Network Organization

system security; just that they were not conceived or conducted exclusively to investigate or correct system vulnerabilities.[663] Security-related projects were secondary to furthering the technology's efficiency and give the impression that they were "after-thoughts" of the major thrust of a project. I take admission of these security-related research efforts within projects primarily designed to increase efficiency as evidence that

[663] There is some evidence that the Network Reliability and Interoperability Council within the Federal Communications Commission did focus research and development on telecommunications security (particularly availability) after a series of phone outages in the late 1980s and early 1990s (See Appendix D. Organizational Responsibilities and Authorities for examples of NRIC's emphasis on telecommunications security).

operators and other lower-level managers who had to contend with the security compromises persisted in including security R&D whenever and however they could. Over the life of the HPCC program, one observes numerous instances where some aspect of one or more of the security management objectives is injected into HECC, LSN, or other program components areas.

The picture of security R&D, particularly the HPCC Program, presented here further supports the notion that the information infrastructure system security in general has mimicked the Internet as a complex, interactive, open-ended network. As can be observed from both the diagram (Figure 5.1. OSTP R&D Organization) and the discussion, the IT R&D organization does not fit the traditional bureaucratic hierarchy. With the number of different organizations involved and their collaboratory and coordinating instead of superior/subordinate relationships, the organizational structure is much more akin to a network (See Figure 5.2. HPCC R&D Network Organization). Also, the bottom-up recognition of security vulnerabilities and research to correct/mitigate those vulnerabilities completes the picture of an Internet-based growth model and simultaneously provides further empirical evidence of the international relations regime-building model introduced in Chapter 4. Policy Dis-Oganization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy.[664]

The research results are not intended to discount some truly difficult technical obstacles to IT security research and development. The lack of metrics to indicate a system's security status, assess risks, and measure performance as well as the lack of large-

[664] Security and security-related R&D were neither a deliberate centrally coordinated activity nor a result of targeted allocation, but more the result of departments/agencies individually placing emphasis on the issue and pressing for action.

scale testbeds to test products in realistic environments are significant issues that were not addressed either early or adequately.[665] Even given these difficult issues, the evidence seems to suggest DARPA's 1996 ISAT Summer Study's conclusions that the government failed to control and coordinate its own information infrastructure system R&D programs were, and seemingly are, still valid.

Consequently, fewer technologically security-related successes, with the possible exception of confidentiality advances, than might have been expected were developed and made available to the information infrastructure system. The implications are that the system still has many of the same technical vulnerabilities it always had or even more with new technologies bringing in their own vulnerabilities. In much the same manner as policymaking disorganization, without better coordination and much higher funding devoted to security-related R&D statements by government decision makers of the importance of security to the IIS belie their true beliefs.

[665] United States National Security Telecommunications Advisory Committee (NSTAC), Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration, ES-1.

Metrics are crucial to measure the effectiveness of security programs. Metrics are the means by which:

- risks are assessed, new security tools and products evaluated, professional accreditation and standards developed, and security's value in organizations quantified;
- a business case can be developed and used to communicate with senior managers in all types of organizations;
- increased investment in security can be rationalized;
- an organization's level of success and performance can be validated; and
- the true nature of the threat can be identified (United States National Security Telecommunications Advisory Committee (NSTAC), Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration, 5 and 10).

The lack of large-scale testbeds limits the ability of organizations to develop scalable information security solutions. As networks and systems grow more complex, conducting tests and experiments becomes increasingly more difficult and expensive (United States National Security Telecommunications Advisory Committee (NSTAC), Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration, 7-8).

Some optimism for research and development might derive from the aforementioned National Information Assurance Partnership (NIA) of the National Security Agency and the National Institute of Standards and Technology. Not only is the (NIAP) interested in developing credible testing based on objective criteria, but it also intends "foster research and development in security tests, methods, and metrics." NIAP intends to accomplish this part of their mission through sponsored partnerships with industry and internal R&D efforts.[666]

[666] National Information Assurance Partnership (NIAP), Introducing the National Information Assurance Partnership Webpage, February 9, 2003, http://niap.nist.gov/howabout.html.

TABLE 5.3. U.S. GOVERNMENT SECURITY-RELATED FUNDING (FY 99/00/01)

(in millions of dollars)

Agency	Project	FY99	FY00	FY01
AF	MEE comm network	19.1	55.4	87.7
	Reliability & Maintainability IS	11.4	11.6	12.1
	Public Key Infrastructure	0.0	14.5	24.9
	IS Security	107.6	119.3	111.4
Army	IS Security	113.3	134.5	106.8
DoD	Security Activities	9.9	19.8	33.7
	IS Security	105	137.1	173.5
	PKI	0.0	0.0	1.0
	Info Sec/Assurance Activities	4.5	12.6	12.2
	DoD/IG Info Assurance	0.3	12.6	12.2
	Defense Info Assurance Program Mgt Office	4.2	2.2	2.2
	Info Assurance-Info Protection Sec Architecture	0.0	2.2	3.1
DoC	Network Reliability	0.0	0.0	1.0
DoE	Kaiser-Hill Cyber Security	0.0	1.0	0.0
DoI	Classified Network	0.0	0.0	8.0

TABLE 5.3 (cont'd)

Agency	Project	FY99	FY00	FY01
	IT Security Risk Assessment	0.0	1.0	0.0
DoJ	Encrypted Voice Radio Program	23.0	39.0	35.0
	Public Key Infrastructure	1.0	1.0	6.0
DoL	CIP	3.3	2.2	13.2
DoT	Sustaining Backup Emergency Comm	2.0	5.0	12.0
	Info Security - NAS Info Coord	2.0	10.0	5.0
	IS Security	4.0	17.0	46.0
EPA	Confidential Business Info Tracking Sys	2.0	2.0	2.0
HHS	CDC Security	1.3	0.7	0.7
	Secure E-mail/ Sybase Server	0.0	0.3	0.0
	HCFA Internal Systems Security	2.7	3.0	3.3
	Medicare Contractor System Security	0.0	4.0	10.0
NASA	IT Security	28.0	46.0	44.0
Navy	IS/Assurance Activities	79.4	118.7	112.7
Total Security-Related funding		**523.0**	**672.7**	**1180.7**

CHAPTER 6

CONCLUSIONS

This research was undertaken to answer the question, is the information infrastructure system a risk to the national security of the United States, and, if so, what has the federal government done to address that risk? Implicit in that question are several other questions:

1. What exactly is the information infrastructure system?

2. Why would an information infrastructure system ever be a risk to any nation's national security?

3. Why would the information infrastructure system be a risk to the United States' national security?

4. How could an information system be a risk to a nation's national security?

5. What has the United States' federal government done through policy or direct or indirect action to obviate or reduce the risk of the system to the national security?

6. How effective have the federal government's actions been in reducing the system's risk to the nation's security?

These questions served as the structure to conduct the research and are addressed specifically by:

- Chapter 1. Introduction to answer Questions 2 and 3;
- Chapter 2. Information Infrastructure System, Question 1;
- Chapter3. Information Infrastructure System Vulnerabilities, Risks, and Threats, Question 4; and

- Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy and Chapter 5. Information Infrastructure System Security and IIS Security R&D Funding, Questions 5 and 6.

Since the research to address these questions was both extensive and complex, this chapter will synthesize the conclusions of each of those individual chapters to answer the hypothesis:

> the United States' national security can be imperiled by the information infrastructure system's inherent structural vulnerabilities of:
>
> - an open system architecture,
> - Interconnectedness within itself and with other critical infrastructures, and
> - Integration of software programs and software with hardware by disrupting the system, exploiting data, and/or producing causal uncertainty of observed effects in the system.

6.1. Why Would An Information Infrastructure System Ever Be A Risk To Any Nation's, To Include The United States', National Security?

Chapter 1 answers questions 2 and 3 of the above questions by establishing the conceptual foundations of a nation's national security and how those concerns translate into current risks for the United States. Absent the need to defend United States' core (i.e., territory and people) from direct attack by another nation, the nation's national security is now concerned more with:

• maintaining its institutions and the fundamental values of human dignity, personal freedom, individual rights, and the pursuit of happiness, peace, and prosperity;

• ensuring a healthy and growing U.S. economy; and

• promoting open, democratic and representative political systems and an open international economic and trade system.[667]

The institutions and processes that provide for the well-being of the people and their pursuit of happiness, peace, and prosperity; the U.S. economy; an open international economic and trade system; and our own open, democratic and representative political system are now dependent upon the critical services organized as infrastructure systems.[668] The President's Commission on Critical Infrastructure Protection identified eight infrastructure systems[669] as critical to the United States' defense, way of life, governance, economy, and public good. These eight infrastructures are all so vital that their incapacitation or destruction would have a debilitating impact on the national security.

[667] United States White House, National Security Strategy of the United States, January 1993, 3.

[668] United States National Security Telecommunications Advisory Committee (NSTAC), Issue Review: A Review of NSTAC Issues Addressed Prior to NSTAC XIX, iii and Sterns, "The Promise of the National Information Infrastructure" in National Academy of Sciences, Revolution in the U.S. Information Infrastructure, 25.

[669] • Telecommunications (Also called Information and Communications): A critical infrastructure characterized by computing and telecommunications equipment, software, processes, and people that support:

•• the processing, storage, and transmission of data and information,

•• the processes and people that convert data into information and information into knowledge, and

•• the data and information themselves (United States White House, Critical Foundations: Protecting America's Infrastructures, "Glossary").

• Electric power systems,
• Gas and oil storage and transportation,
• Banking and finance,
• Transportation,
• Water supply systems,
• Emergency services, and
• Continuity of government services (United States White House, Critical Foundations: Protecting America's Infrastructures).

Protecting each of these infrastructures is especially critical not only because of their individual role in the life of the nation, but also because they are interconnected; each is dependent upon the others for optimum functionality and long-term sustention.[670] For example, the information infrastructure system is dependent upon the power system to provide not only the power but also the necessary operational environment while the other six infrastructures contribute indirectly to the long-term sustention of the information infrastructure's components and the people who operate it. At the same time, each of the other infrastructures is dependent upon the telecommunications infrastructure to manage their functions and to provide optimum performance.

A major disruption of any of these critical infrastructures could lead to major losses and affect national security, the economy, and the public good. The PCCIP defines electric power systems as the single most important critical infrastructure system since all of the other critical infrastructures are dependent upon it for power to function.[671] However, since the electric power system, as well as the other critical infrastructures, are dependent upon the information infrastructure to manage their functions[672] one can legitimately make the case that the information infrastructure system is potentially the single most damaging risk[673] jeopardizing the United States' national security in the post-Cold War era.

[670] United States White House, Critical Foundations: Protecting America's Infrastructures, "The Case for Action."

[671] United States White House, Critical Foundations: Protecting America's Infrastructures, "Glossary" and "The Case of Action"; The RAND Corporation, "Strategic Warfare Rising," 1-2; and Molander, Riddile, and Wilson, "Strategic Information Warfare: A New Face of War," 3-4.

U.S. power projection plans might be deterred or disrupted by threats or attacks against infrastructures vital to overseas deployment (Slabodkin, 2).

[672] All critical infrastructures are now connected to networks and to each other through the telecommunications critical infrastructure (United States White House, Critical Foundations: Protecting America's Infrastructures).

[673] United States White House, Critical Foundations: Protecting America's Infrastructures, "The Case for Action."

The service provided by this critical infrastructure is much subtler than just the provision of data; it is becoming deeply embedded as an essential element of organizations and institutions and undergirds the functioning of all sectors of a developed nation's life.[674] It has become the bedrock upon which the United States' society and institutions are built and upon which they are dependent. Few would disagree that the electric power and information infrastructures together are vital to the previously mentioned U.S. national security criteria.

6.2. What Exactly Is The Information Infrastructure System?

As defined in Chapter 2. Information Infrastructure System, an information infrastructure system is a combination of all public and private computing and transmission functions in a gigantic global network of networks of which the U.S. system is only a part.[675] Interconnectivity of different computing systems is the basis of the information infrastructure system's utility; it allows data to be shared autonomously (without additional separate discrete activities) between computing systems. The Internet is but one part of the total infrastructure but serves as a superlative analogue for the total system since it was the genesis of and most accurately approximates the total evolved system structurally.

The research also established that the information infrastructure is indeed a system, a very complex system. As a system, each individual part is critically important to the functionality of the whole. With the exception of an end user, if one part's function is degraded or halted, the entire system's functionality is degraded or halted. An end user's degradation or stoppage will obviously obviate the functionality of the system for that end

[674] United States White House, Critical Foundations: Protecting America's Infrastructures.

[675] United States White House, Critical Foundations: Protecting America's Infrastructures, "Critical Foundations" and "Appendix A: Information and Communications."

user and any intended recipient(s) or transmitter(s) of the data, but not necessarily affect the functionality of the rest of the system.

6.3. How Could An Information System Be A Risk To A Nation's National Security?

Interconnectivity, though, is not risk free. Firstly, interconnectivity permits anyone with malicious intent the same ease of access to other subsystems or users as legitimate users. Secondly, interconnectivity also permits a user, generally one with malicious or, at least, mischievous intent, the means to enhance his anonymity (thus reducing the risk of being caught) by allowing initiation of an activity through other users' or system components if desired.[676]

Thirdly, because the resulting interconnected combination is a system it possesses system characteristics. The most important system characteristic for the information system is the ability of different functions to operate as one function without any additional input (autonomously). Data moves ("cascades") from one part of the system to other parts as input for (one would assume beneficial or, at least, planned) functions. This same characteristic also permits data that can produce planned malicious and unplanned, unanticipated activity and/or their effects to "cascade." Therefore, deleterious (as well as beneficial) effects (or, at least the data that produces them) are able to migrate unimpeded from the subsystem where they occur to other connected subsystems.

Unfortunately for the United States' national security, the system has evolved to maximize efficiency with little regard for the security of the data transmitted or of the system itself. The ARPA effort to design the initial long distance connections between

[676] Although more a function of an intruder's software knowledge and expertise than interconnectivity, an intruder can further enhance his anonymity by disguising malicious or mischievous activity with a time delay or to resemble an accident instead of an attack.

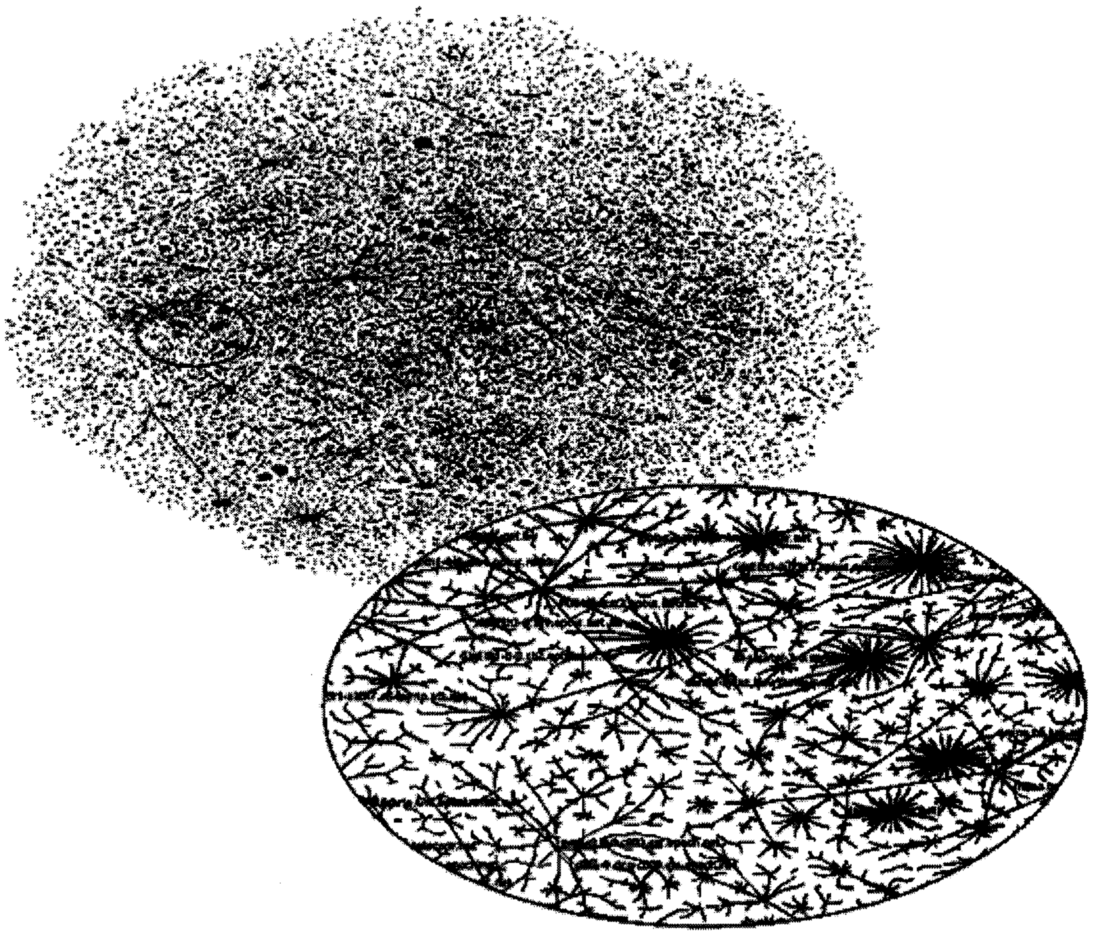


Figure 6.1. The Internet: 2001[677]

computers really had no criteria other than connectivity. The technical task of connecting computers to share data was much too difficult in itself for the designers to worry about other criteria. No one involved in the initial project could envision the system they designed becoming the critical component of modern life that it has become.

In a classic free market model, the evolution of the initial system by private commercial firms has emphasized efficiency instead of security to maximize profits. As a result, the structure that has evolved resembles a scale-free network with its inherent

[677] The Internet: 2001, Peacock Maps, Inc., http://209.9.224.243/peacockmaps.

vulnerability of few nodes serving as a connection between a majority of networks (See Figure 6.1. The Internet: 2001 for an approximate picture of both the extent of the infrastructure today and the critical node vulnerability). As can clearly be seen in the enlarged insert, some nodes are much more highly connected than others. As described in Chapter 3. Information Infrastructure System Vulnerabilities, Risks, and Threats, degradation of these most highly connected nodes rapidly leads to degradation of the system's performance and eventually failure of all connections for that node since the highly connected node is the solitary link to the rest of the system for those nodes leading into to it.

Although not postulated as a vulnerability in the original hypothesis, the structure of information infrastructure system's architecture was discovered to be a sufficient but not necessary condition of risk to imperil the United States' national security during the research. Degradation or compromise of the system's highly connected nodes compromises only the availability information assurance objective and not necessarily the other four,[678] but without the data available the other four become moot. Also, without the data available the originally intended function cannot be performed.

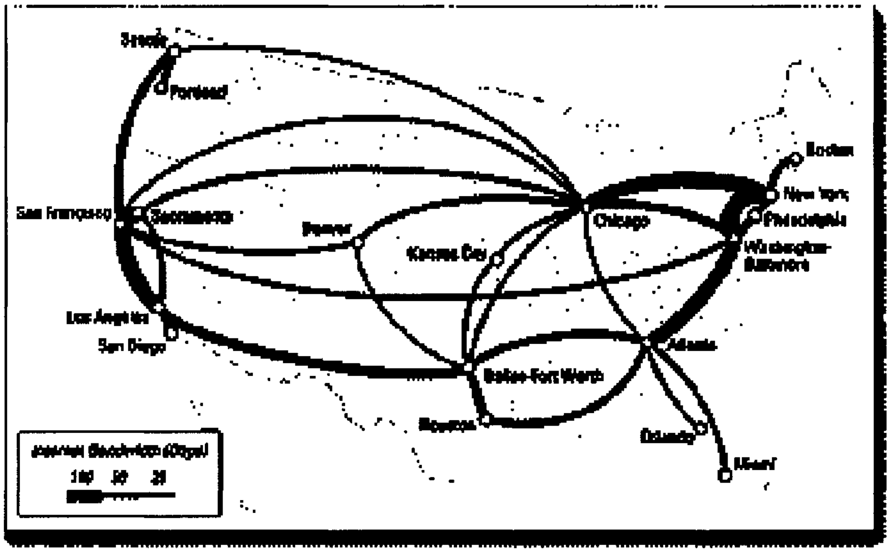
Compromise of the availability objective (at least for a single user, multiple users, one or more LANs or MANs) can be accomplished by overwhelming system components of

[678] The information assurance objectives are:

- confidentiality - assurance that information is not disclosed to unauthorized persons, processes, or devices;
- availability - timely, reliable access to data and information services for authorized users;
- integrity - quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information;
- authentication - security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. and
- nonrepudiation - assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

a discrete portion of the network rather than the entire network; exactly what distributed denial of service attackers do. It is not much of a stretch to imagine what a coordinated distributed denial of service attack by a terrorist or criminal organization or hostile nation could do too much of the existing information infrastructure system. With the United States' dependence upon the system, such massive denial of service over time could be disastrous even without continuous denial of availability. Repeated incidents of service denial could erode public confidence in the ability of the system to perform its functions.

What is especially troubling from a national security risk perspective is cybergeography, an entirely new discipline that has evolved along with the computer and network technology. Through the techniques of this new discipline, the location of every



© 2002 TeleGeography, Inc.
[679]

Figure 6.2. Major U.S. Routers

[679] Major U.S. Routers, TeleGeography, Inc., Washington, DC, info@telegeography.com.

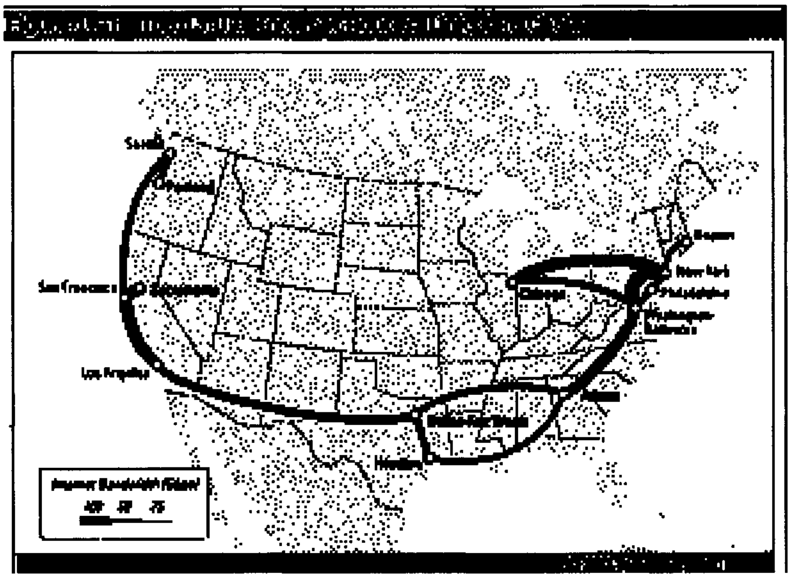
point on the infrastructure can be determined, to include the locations of the backbone's routers over which the majority of, if not all, data traffic is transmitted are known. (See Figure 6.2. Major U.S. Routers). When overlaid with the top 15 U.S. Internet routes (Figure 6.3. Top 15 U.S. Internet Routes), the targets most at risk should become clearly evident.

Unfortunately for security, not only can the virtual location of each point be determined as indicated in Figure 6.2, but that point's location can also be pinpointed by coordinates or geographical address.[680] Knowledge of a router's exact location obviously makes it not only vulnerable to the technical exploitation on which the research focused, but also to physical destruction.

A second condition of the evolved network architecture is its "openness," i.e., the ability of anyone with the means to gain access with no restrictions. Although more a policy decision than a structural condition, this characteristic of the information infrastructure system allows a potential security threat relatively easy access to its target. However, it is not considered a critical vulnerability since a determined potential threat could overcome restrictions on access to the information infrastructure system. A determined potential malicious user theoretically could access the system given even the most stringent access restrictions through other technical vulnerabilities or by exploiting human vulnerabilities. One only need look to intruders' ability to gain access to other users' personal data and data files once they have accessed the system as evidence of the ease with which potential security threats can gain access to restricted data. Therefore, though postulated as a causal variable (i.e., both a necessary and sufficient condition) of the information infrastructure

[680] A. Lakhina, J.W. Byers, M. Corvella, and I. Matta. On the Geographic Location of Internet Resources. Technical Report 2002-15. Computer Science Department, Boston University. Boston, MA., May 2002. http://www.cs.bu.edu/techreports/pdf/2002-015-internet-geography.pdf.

system's risk to the national security of the United States, the open nature of the architecture of today's system is neither but serves only to facilitate a potential threat's access to the system.



[681]

Figure 6.3. Top 15 U.S. Internet Routes

However, one intervening variable that the architectural openness does create, though, is causal uncertainty. The openness allows any user an unusual degree of anonymity. The user is identified only by an address that he creates (within certain bounds). Therefore, without identifying oneself a user can say or make any demands without too much fear of attribution. Of course, sophisticated users can trace the address to the originating computer to at least learn from where the message originated. The originating user can make that process more difficult by routing the original message through literally

[681] Major U.S. Routers.

thousands of intermediary systems; theoretically, all of the other computers connected to the information infrastructure system).

This anonymity can cause causal uncertainty about exactly who is making a demand or interfering with a system's operations. When a threatening or demanding situation that has national security implications occurs, national policy makers are often unsure not only from where or from whom the threat or demand originated. Such uncertainty can create doubt about the legitimacy of the threat or demand, how to structure a response, and to whom to direct a response resulting, in the extreme, in decision paralysis. Roger Molander and others from RAND have postulated just such a scenario for a national security exercise conducted with national policy makers in The Day After...in the American Strategic Infrastructure.

Unfortunately, the very basis of the system's functionality, software, is as vulnerable, if not more, to exploitation. Given the conceptual complexity of large software programs (which are necessary to allow for the functions today's information infrastructure system provides) and the absolutely necessary task of accounting for all foreseen and unforeseen actions that may result from the proposed software's programmed actions, the prospect of developing software without defects (i.e., errors and faults) is pragmatically, but not theoretically, nil.

Having said that though, there are several practices in today's software development process that exacerbate production of defective software. The rush to market to maximize profits may be the most egregious. Commercial firms are in such a hurry to get new products offering new services or taking advantage of new technological breakthroughs to consumers that often the time to test adequately the software during development before release is truncated. In many cases, developers will know of a defect but not correct it before release because they consider it too unlikely to cause problems during normal programmatic operation. Further, the same conceptual complexity that practically guarantees defective software obtains for testing. Not only should testing ensure that the software correctly performs the programmed actions, but it must also ensure that **ALL** immanently possible actions have been envisioned and programmed for. Consequently, any piece of software will be released with known and unknown defects.

These problems seem conceptually intractable but some optimism does exist for software testing. The afore mentioned National Information Assurance Partnership (NIAP) (See Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy and Chapter 5. Information Infrastructure System Security and IIS Security R&D Funding) is designed partly to provide better testing. NIAP's primary goal is to "establish **cost-effective** (emphasis added to highlight the influence of NIST in the partnership) testing, evaluation, and certification programs through specifications-based criteria.[682] The partnership intends to use the Common Criteria Testing Program (CCTP) based on the Common Criteria for Information Technology Security Evaluation (CC and the Common Evaluation Methodology (CEM) being developed through the International Organization for Standardization (ISO).

Such a scheme should "increase trust in security-enhanced products that can arise through well-engineered, well-known, and well-understood security testing and

[682] These specifications will be derived from formal descriptions of security functionality and assurance requirements for different products or systems (National Information Assurance Partnership (NIAP), Introducing the National Information Assurance Partnership Webpage, February 9, 2003, http://niap.nist.gov/howabout.html).

evaluation strategies." The partnership then intends to transfer the testing and evaluation process to commercially certified laboratories.[683] It is hope that this will open security testing and evaluation to competition, will widen testing choices and alternatives, and should lower testing costs.

Exacerbating the defective software problem even more is the trend within the data systems community to consolidate more and more functions into single software programs and/or software/hardware combinations. From an efficiency perspective, this practice makes sense; it permits one program to execute from data provided by another program without additional human action. Not only does such practice take a potential human error-maker out of the chain of events for the activity, but it also reduces the number of people (and, hence, the cost) required to perform the tasks thereby reducing labor costs.

Unfortunately, the practice of integrating increasingly larger numbers of activities into a single software program or into software/hardware combinations creates very tightly coupled systems. These tightly coupled systems are great for productivity and efficiency, but at the same time remove slack from the resulting system. As Charles Perrow in Normal Accidents has shown, the practice of tightly coupling systems also has risks for the both the security, safety, and continued programmed function of the system created. Without a certain degree of slack to provide a buffer for (human) intervention to stop or correct unanticipated activity, damage, unintended activity, or system malfunction (a system accident) is more likely to occur.

[683] Dr. Paul J. Brusil and L. Arnold Johnson, "NIAP Readies Commercial Security Testing and Evaluation Industry in the United States" (Originally published Open Systems Standards Tracking Report (OSSTR), March 1998, http://niap.nist.gov/NiapWebPages/osstr0398.htm.

As of February 9, 2003, there are seven NIAP certified testing laboratories (National Information Assurance Partnership (NIAP), Common Criteria Testing Laboratories (CCTL) Webpage, February 9, 2003, http://niap.nist.gov/cc-scheme/TestingLabs.html).

Although highly unlikely, these types of accidents are not without precedence even in the information infrastructure system. The Christmas Day 1973 Harvard incident (See Appendix B. Denial of Service) clearly and dramatically demonstrates that an unanticipated activity (routing of all message traffic to the Harvard IMP thereby overwhelming the planned capability to handle message traffic) can have disastrous systemic results (eventual disruption all system message traffic). The system managers finally had to completely shut the entire system down and reconstruct it after correcting the initial software error in Harvard's link to the system that caused the malfunction because they had no way to intervene in the chain of events to stop the unanticipated activity.[684]

Such incidents at the information infrastructure system level are rare[685] (as Perrow predicts), but do occur more frequently at the subsystem level. American Airlines' early reservation system Sabre used eight separate IBM computers to ensure no single failure could disable the entire system. However, on an otherwise uneventful day in May 1989, technicians at American installed new memory disk drives into the system. The installation triggered a software error that erased some of the information in the memories. The airline could no longer determine which passengers were booked on which flights. Furthermore, the airline's elaborate defenses were superfluous as the software error jumped in rapid succession from computer to computer to quickly disable all eight. American officials said

[684] Denial of service and distributed denial attacks themselves are not considered system accidents because they are planned even though they are unanticipated. The perpetrators know what they are trying to accomplish even though the targets are unaware of the planned actions' effects.

[685] Of course, the United States and the rest of the world avoided the greatest possible system accident (Y2K) only through a gargantuan and costly effort. The Department of Commerce estimates that $100 billion (8.34 by the government alone) from 1995 to 2001 were spent on efforts by the United States government and businesses to prepare computer systems for the Year 2000. Newsweek estimated global Y2K spending at $500 billion (U.S. Congress, Senate, Y2K Aftermath: Crisis Averted: Final Committee Report, S. Prt. 106XX, Special Committee on the Year 2000 Technology Problem, 106th Congress, 2nd sess., February 29, 2000).

afterwards they couldn't have done a better job of disabling the system if they had set out to do so deliberately.[686]

As discussed in Chapter 3. Information Infrastructure System Vulnerabilities, Risks, and Threats, the currently constructed system appears to contain enough slack to be able to preclude such system accidents. The current construction of the system as an aggregation of discrete parts provides enough opportunities for human intervention to successfully stop a malfunction before collapsing the entire system. The more immediately pressing problem currently is more rapidly recognizing data that can lead to malfunctions. Managers and administrators would then be able to either preclude or more minimally contain damage that could be cause by such data.

Even if all new software could be developed and marketed without any defects, the vulnerability generated by defective software would not disappear. Enough computers and networks exist with defective legacy software to imperil even new defective-less programs. Not every user or administrator corrects known defects in these legacy programs and additional defects continue to be discovered in even the oldest programs still in use [See Chapter 3. Information Infrastructure System Vulnerabilities, Risks, and Threats for a discussion of UNIX's (one of the earliest and still widely used operating systems) pathologies]. These legacy vulnerabilities jeopardize not only the existing system but, in many cases, the newly released programs themselves. The vulnerabilities of the information system and their causal properties thus can be summarized in Figure 6.4. Comparison of Systemic Vulnerabilities below.

[686] Leonard Lee, 123-124.

In order to develop some scale of the seriousness of the vulnerabilities (necessary to develop the most effective strategy to correct or to mitigate the vulnerabilities and policy to protect the national security of the nation), each of the vulnerabilities is rank ordered according to their causal property and the seriousness of the effects of its exploitation. As can be seen, software is considered the prime, or first order, vulnerability. Without defects in software, an intruder's exploitation of the system (other than those associated with failure of the system's physical structures which was outside the defined scope of this research) more than likely would not be possible.

VULNERABILITY	**NECESSARY**	**SUFFICIENT**	**VULNERABILITY ORDER OF MAGNITUDE**
Software	Yes	No	1^{st}
Interconnectivity	Yes	No	2^{nd}
Complexity	No	Yes	2^{nd}
Scale-Free Network	No	Yes	2^{nd}
Open System Architecture	No	No	3^{rd} or >

Figure 6.4. Comparison of Systemic Vulnerabilities

The other properties (interconnectivity, open and scale-free architecture and complexity) serve to facilitate defective software exploitation and to increase the gravity of the exploitation's effect. Therefore, from a systems perspective the primary role software defects have in total system risk raise their seriousness to a higher order than the other vulnerabilities.

Interconnectivity is considered a second order vulnerability since it only serves as the means to facilitate and expand, but does not cause, a system exploitation. Interconnectivity facilitates exploitation by allowing a party or a vulnerability's exploitation effect to move from one subsystem to other subsystems within the total information infrastructure system relatively easily. Without interconnectivity, anyone with malicious intent or the effects of an exploited vulnerability would be restricted to the initially affected subsystem.

Complexity as a vulnerability involves not only the just discussed software complexity, but is also evident in the system's scale-free structure itself. The system's structural complexity is increasing in much the same way and for the same reasons as the system's functional complexity: efficiency and elimination of required human input from the system. This increasing structural complexity added to the increasing functional complexity of software and software/hardware integration provides additional opportunities for Perrow's system accidents.

Complexity, therefore, can be a sufficient condition to cause a compromise of one or more of the information assurance objectives, but of itself is not a necessary condition. Compromise can occur without complexity's vulnerability. Since complexity as a condition is only sufficient, but not necessary to cause a compromise of the IA objectives, it is considered a second order vulnerability.

The open nature of the system's architecture (ease of access) is neither a sufficient nor a necessary condition of compromise of the objectives. Ease of access has no effect on complexity's system accidents. As previously discussed, it only makes it easier, not necessary, for a potential user with malicious intent to gain access to the system. Since the open nature of the system's architecture is neither a necessary nor a sufficient condition for compromise of the IA objectives, it may not be a vulnerability at all or, if considered one, then only a third or greater order vulnerability that only facilitates the other higher order vulnerabilities.

In the classic national security model, risk was determined by a threat with the capability and intent to exploit a vulnerability. Even with the demise of the Soviet Union, those classic threats still exist. Those threats can be individuals, groups/organizations, or other nations and, as events on September 11, 2001, demonstrated, the United States does have individuals, groups, organizations, and other nations that wish it ill. If those individuals, groups, organizations, or nations can achieve the capability to exploit the just discussed vulnerabilities of the information infrastructure system, then the risk to the nation's nations security is greatly imperiled.

Unfortunately, evidence of the ability to exploit those vulnerabilities is legion. Intrusions into even the most sensitive subsystems (e.g., the U.S. military, Microsoft's operating system's root code, U.S. national security-related subsystems (the Hanover Hacker), the financial sector, EMS subsystems, etc.) connected to the greater information infrastructure system have occurred. The vulnerabilities are just too pervasive and too numerous.

Attribution for these intrusions so far has been only to individuals, groups, or organizations. Little unrestricted empirical evidence exists that other nations as a matter of state policy have been implicated in malicious intrusions[687] of American or any other information infrastructure networks. However, given that individuals, groups, and

[687] There is evidence that other nations have intruded into the American information infrastructure system to steal data, but not to alter or delete data or disrupt the system. (See Chapter 1. Introduction for a discussion of other nations' espionage activity against the U.S. information infrastructure system).

organizations can gain access to sensitive data no one should doubt that a nation that is willing to invest the necessary money and effort could achieve the same degree of, and probably greater, access to U.S. information infrastructure system networks as individuals or organizations. Such access permits any individual (Osama bin Laden?), any group or organization (al Qaida or some other terrorist organization?), or nation with malicious intent towards the United States to put the nation's national security at risk by altering, denying, eliminating, or creating uncertainty about the integrity or source of the data.

The research thus far establishes that the classic variables to create the information infrastructure system as a national security risk exist:

- Risk - The system is indispensable to the American economy, government, and way of life, if not the survival of the nation;
- Vulnerability - The system has a multitude of vulnerabilities that are exploitable;
- Capability – The capability to exploit the vulnerability are essentially the same as the capabilities required to access and use the system legitimately of which there are literally tens of millions; and
- Intent – No shortage of individuals, groups, organizations, and possibly other nations exist that would like to imperil the national security of the United States.

The research also establishes that the risk of the information infrastructure system to the national security of the United States is more complicated than the classic threat-based model of national security. The system is also threatened by disruption or denial of essential environmental operational requirements (temperature, humidity, energy, etc. from disruption of the other critical infrastructure systems) and system accidents resulting from too tightly coupled complex systems. These conditions need not be initiated by a threat but can result from naturally occurring events and will produce effects that interfere with the normal operations of the information infrastructure system as effectively as one deliberately initiated directly against the system. Therefore, risk to the information infrastructure system, and the United States' national security, is not only from an agent with mischievous or malicious intent as in the classic threat model but also from naturally occurring phenomena and unintended consequences.

6.4. What has the United States' federal government done through policy or direct or indirect action to obviate or reduce the risk of the system to the national security?

Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy answers the question in the introduction, "What policy or policies have the national government developed and implemented to secure this system and better protect the nation's security?" If a policy response is considered a comprehensive national information infrastructure system security policy, the U. S. government's policy response to the information infrastructure system as a national security risk has been less than overwhelming since first publicly recognized as such in the 1992 National Security Strategy of the United States. As of August 2002, the initial draft of a national policy (Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue) first published in January 2000 remains the only comprehensive policy document the government has produced.

The current Bush administration seems to have cooled to the idea of preparing a national comprehensive information infrastructure system policy. I suspect the administration has decided that other critical infrastructure risks considered more likely to be exploited by terrorists using weapons of mass destruction with more spectacular effects is a higher priority. That determination is understandable given the events of September 11, 2001. However, as detailed by the research the vulnerabilities of the information infrastructure system probably pose a greater national security risk for the nation as a whole given the significance of the effects from exploitation of its vulnerabilities than the relatively small-scale terrorist use of weapons of mass destruction. The seemingly overriding difference between the two risks would seem to be the public panic caused by use of weapons of mass destruction from both casualties and the mere threat of and possible presence of menacing nuclear, biological or chemical agents in the nation itself. Use of weapons of mass destruction within the territory of the United States is a direct attack on the core of the nation itself and the effects are much more visible than an attack on something as invisible and abstract as the information infrastructure system, but not more damaging to the nation's national security.

Given the number of intersecting factors involved, developing a national comprehensive information infrastructure system security policy is infinitely difficult, but not hopeless. One of the most difficult problems to solve is the ownership issue; the system is almost entirely owned by the private sector dedicated to making a profit while the government, by definition, is responsible for national security. Commercial firms in the private sector are more interested in efficiency than security since any requirement for security adds costs and slows the system's speed (one of the competitive advantages all commercial firms involved in data operations strive for and tout). Consequently, during the decade of the 1990s these commercial data operations suppliers were reluctant to add voluntarily security measures to their part of the operations or to agree to most security suggestions the federal government made.

This attitude began to change somewhat in 2000 and accelerated after September 11th with the formation of voluntary Information Sharing and Analysis Centers (ISACs) between appropriate government offices and commercial sector as part of critical infrastructure security. However, any security proposals by the government are still only suggestions to be adopted or ignored by the different information technology sector.

An issue strictly confined to the government is the issue of authority over information infrastructure system security. The research established that after the publication of PDD 29, Security Policy Coordination, in 1994, 31 different federal organizations, either directly or indirectly, had some statutory or administrative role in information infrastructure system security policy making. As the events of September 11 showed, sharing information between such a large number of organizations either efficiently or timely is nearly impossible. The organizational landscape has probably become even more muddled with the proposed creation of the Department of Homeland Security adding yet another layer and one more office of the federal bureaucracy that has some degree of responsibility for the nation's national security.

A compelling reason for such authority diffusion possibly is the issue area itself. Inclusion of the commercial sector (and they have to be included since the information infrastructure is almost exclusively owned by them) and a new technology that is not only pervasive but also critical to the nation's economy, government, defense, and citizen's well-being do not fit neatly within the existing Cold War era national security policy's boundaries. The critical question then becomes how to improve the security of the system for the benefit of the nation's national security; either voluntarily through cooperation or through federally regulated sector mandates. The Clinton administration chose to adopt the first option to retain the commercial sector as an unregulated industry maintaining and further contributing to the existing policy landscape (See Figure 4.1. Post-PDD 29 (>1994) IIS Security Policy Organization).

Such a diffusion of authority obfuscates the issue of "who's in charge?" With so many organizations mandated various degrees of authority by statute or administrative fiat, confusion of who actually has authority to do what is sure to exist. As bureaucratic battles for supremacy (often within relatively narrowly defined boundaries) between NSA (and DoD tacitly), NIST, DoJ, and DoC clearly demonstrate, much of the decade of the 1990s was spent doing just that to the detriment of any comprehensive national policy formulation. Halperin and Allison provide the classic explanation for these bureaucratic battles for authoritative supremacy in the bureaucratic politics model of decision making.

At the same time, Halperin provides a rationale for a counterintuitive phenomenon also identified by the research: bureaucratic organizations seemingly eschewing their mandate of responsibility in this issue area. At least four organizations (OSTP, NSTC, NCS, and FCC) seemingly chose to forego their mandate by not actively nor vigorously pursuing a significant role. According to Halperin's rationale, the information infrastructure system's national security mission was only tangential to these organizations' core mission and therefore their essence. An organization will not actively pursue, and, frequently, will even attempt to divest, a tangential mission that detracts from its essence. None of the four organizations are publicly associated with, nor actively involved in national security activities, but see their mission (and therefore their essence) as scientific and technology policy and technical operations only. Consequently, none of the four vigorously pursued the mandated role of information infrastructure system national security policy.

The information infrastructure system national security policy landscape is confusing enough when depicted by the traditional bureaucratic vertical authority line chart (See Figure 4.1. Post-PDD 29 (>1994) IIS Security Policy Organization). The same organizational structure can also be re-configured as a scale-free network (See Figure 4.5. IIS Security Policy Network). Several critical nodes are easily identified (DoC, CIAO, NSTISS) but none more critical than the National Security Council's National Coordinator for Security, Information Protection and Counter-Terrorism [NCO(SIP&C-T)]. Given the scale-free network's natural intrinsic vulnerability of critical node functional degradation degrading the overall performance of a system, one could reasonably conclude that inadequate performance (functional degradation) by the NCO(SIP&C-T) critical node was the primary cause of the lack of a comprehensive information infrastructure system national security policy.

Such an assessment might be too harsh given the other policy limitations but a certain degree of responsibility has to be borne by that office and the person occupying it. Further, also in defense of that office, it has very little direct authority over Executive Branch departments and agencies but as with other National Security Council portfolio holders serves primarily to initiate and coordinate national security policy.[688] Further in defense of the office, it is severely limited in what it can accomplish because of the limited number of personnel normally assigned to different portfolios in the National Security

[688] See Appendix D. Organizational Responsibilities and Authorities for a detailed account of the National Security Council's responsibilities in information infrastructure system security.

Council. However, these limitations should have been recognized and corrected by the Clinton administration early in the process.

If, on the other hand, a policy response is considered the summation of all that takes place, then the picture of "What policy or policies have the national government developed and implemented to secure this system and better protect the nation's security?" becomes much more favorable. Over the decade beginning with the establishment of the Computer Emergency Response Team at Carnegie Mellon University in 1988, individuals and organizations, either separately or in coordination with each other, have initiated many security measures. This was done primarily to increase their own systems' security but had the added effect of improving the information infrastructure system's security since the total security of a system is only as good as its weakest link.

Today, not only do many private sector and governmental organizations recognize the need for and have formal security policies in place but many security oriented fora and organizations exist to detect, report, collect and respond to vulnerabilities and exploitation of vulnerabilities.[689] Even though such extemporaneous activity is commendable and

[689] As an example, over the course of the decade of the 1990s the federal government in cooperation with the information technology commercial sector has initiated many different programs and offices to improve IT security, to include:

- Information Sharing and Analysis Centers
- Federal Bureau of Investigation
  - •• FBI Washington Field Office's Infrastructure Protection and Computer Intrusion Squad
  - •• The Awareness of National Security Issues and Response (ANSIR) Program
- U.S. Department of Justice
  - •• Computer Crime and Intellectual Property Section (CCIPS)
  - •• Critical Infrastructure Assurance Office
- Defense Information Systems Agency
- CERT Coordination Center
- Federal Computer Incident Response Capability (FedCIRC)

  FedCIRC is the central coordination and analysis facility dealing with computer security related issues affecting the civilian agencies and departments of the Federal Government.
- Forum of Incident Response and Security Teams (FIRST)
- U.S. Department of Commerce
  - •• National Institute of Standards and Technology (NIST), Computer Security Division

beneficial over the long term, it only highlights the weakness of the situation during the 1990s and continuing today: without a coordinated consensus of what needs to be done for the overall information infrastructure system's security all are working to secure their own little piece of the system according to their own vision of what needs to be done.

Obviously, no such consensus exists because no such national consensual plan exists. Therefore, one must conclude that the federal government's efforts to reduce the system's risk to the national security has been mixed: some actions have been implemented individually or cooperatively by federal departments or agencies and the commercial sector or but there is little evidence that any of these efforts have the total

The NIST, Computer Security Division provides users a service in obtaining information on computer vulnerabilities. The ICAT is a searchable index of information on computer vulnerabilities. It provides search capability at a fine granularity and links users to vulnerability and patch information.

••ICAT Vulnerability Database

• Computer System Security and Privacy Advisory Board (CSSPAB)

Use the Department of Commerce "search" for information on encryption issues.

• Federal Trade Commission

The FTC maintains a database on issues relating to consumer protection, business guidance, antitrust/competition, and privacy concerns

• Better Business Bureau and Fraud Review

These two respected, private sector organizations maintain a database on issues relating to consumer protection, business guidance, antitrust/competition, and privacy concerns.

• Center for Education and Research in Information Assurance and Security (CERIAS)

A new center with a comprehensive approach to network and computer security issues.

• National Security Institute (NSI)

A leading Internet resource for the security professional.

• Information Assurance Support Environment (IASE)

The mission of the IASE Information Desk is to assist U.S. Military or Government users with ANY Information Assurance question or issue. A network of over 100 Security Specialists are available to answer security related questions. The IASE web site is a clearinghouse for Information Assurance Information serving the DOD community

• Common Vulnerabilities and Exposures (CVE)

CVE is a "list of or dictionary of 1510 entries as of May 7, 2001 that provides common names for publicly known information security vulnerabilities and exposures."

• SANS Resources' "How to Eliminate the Ten Most Critical Internet Security Threats: The Experts' Consensus." Version 1.32. January 18, 2001.

The SANS document is a list of the ten most critical Internet security problem areas – clusters of vulnerabilities that system administrators need to eliminate immediately (United States Department of Justice, Related Sites Webpage, Federal Bureau of Investigation, National Information Protection Center, http://www.nipc.gov/sites.htm; Mitre Corporation; and SANS Institute).

support of all departments and agencies within the federal government or the commercial sector.

No comprehensive information infrastructure system national security plan exists to this day. There is an urgent need to rationalize or simplify the information infrastructure system's national security policy structure to provide timely, coordinated policy to facilitate coherent, effective implementation strategies to protect this critical national asset.

6.5. How Effective Has The Federal Government's Actions Proven To Be In Reducing The System's Risk To The National Security?

It is almost axiomatic within policy studies that an organization will elevate an issue considered critical to a high priority for both action and resources. Such was the case with homeland defense after September 11th. A good indication of how important the U.S. federal government considered information infrastructure system security can therefore be indirectly evaluated from the amount and percentage of federal government information system total resources spent on system security. Precise determination of those figures by examining either the complete federal budget or individual department's and agency's budgets for the years 1990-2000 is virtually impossible though (See Chapter 5. Information Infrastructure System Security and IIS Security R&D Funding for detailed picture of federal R&D IT security and information infrastructure security R&D funding).

Since all public government documents on the information infrastructure system as a national security risk advocate increased research and development spending to find technical solutions to the system's vulnerabilities, R&D funding for IT security can provide another indirect indicator of the government's priority for information infrastructure system security. Once again, a precise determination of that amount is impossible for many of the same reasons as total system security. Given the nature of the subject, the organizational environment, the major focus of both the commercial sector and government (at least initially) for efficiency over security, individual department's and agency's IT R&D security efforts are not specifically identified in budget documents or are hidden in other budget categories making it impossible to determine the extent of total federal effort over the decade. However, using the High Performance Computing and Communications program as an analogue[690] can provide a funding profile from which observations about the total can be inferred. DoD's (and DARPA's) and, presumably, the other federal departments' and agencies' IT security R&D funding is presumably by definition included in the HPCC program budget.

This discussion is not intended to diminish the efforts of individual departments and agencies. Federal IT security efforts actually began collaboratively with academia and the commercial sector in 1989 after the Morris worm incident with the establishment of the Computer Emergency Response Center. However, whether this can be considered a legitimate R&D effort or not is questionable. Further, this collaboration was primarily an effort between the Department of Defense and those elements and didn't extend to other parts of the federal government until later in the 1990s.

[690] The High Performance Computing and Communications program is an ideal analogue to provide a sample profile of federal government R&D funding for information infrastructure system security. The program was established to coordinate and provide focus for computing and communications (information infrastructure) R&D initiatives of all federal departments and agencies. Although only begun in 1991, the program is the only coordinated effort across the entire federal government to exist for IT R&D during the decade of the 1990s.

As the research in Chapter 5. Information Infrastructure System Security and IIS Security R&D Funding demonstrates, even within the HPCC program the level of federal funding for information infrastructure system security R&D funding during the 1990s did not approach the recommended Joint Security Commission's standard of 5-10 percent of all IT R&D funding for security.[691] Such a long-term recurring shortfall clearly suggests that the federal government was more interested in funding research and development for operational improvements (speed and efficiency) rather than for securing the system.

The above discussion on information infrastructure security policy making and R&D leads one to conclude that the United States' federal government has not been very effective in reducing or obviating the system's risk to the national security. No comprehensive security strategy has been developed and research and development funding was not provided at an adequate level to produce solutions to the system's technical vulnerabilities.

Such a conclusion is supported by both the number of incidents and vulnerabilities reported to CERT since its establishment in 1988 (See Tables 6.1. Number of Incidents Reported and 6.2. Vulnerabilities Reported below).

Table 6. 1. Number of Incidents Reported

Year	Incidents	Year	Incidents
1988	6	1995	2412
1989	132	1996	2573
1990	252	1997	2143
1991	406	1998	3734
1992	773	1999	9859
1993	1334	2000	21756
1994	2340	2001	52658

[691] IT security R&D funding from FY1996-98 was approximately 3 percent of all IT R&D funding. Only in FY 2000 did IT security R&D funding reach the JSC's recommended level of between 5-10 percent of IT R&D funding (11.2 percent). Hopefully, FY2000's allocation will become the long-term trend.

Table 6.2. Vulnerabilities Reported

Year	Vulnerabilities
1995	171
1996	345
1997	311
1998	262
1999	417
2000	1090
2001	2437 [692]

With the exception of a few anomalies, the number of incidents and vulnerabilities reported has risen each year indicating both an increase in the number of possibilities for exploitation and the actual exploitation of those possibilities. An alternate explanation for the rise could possibly be that more people and organizations are reporting both vulnerabilities and incidents. Both people and organizations are traditionally hesitant to report incidents to avoid embarrassment and erosion of customers' confidence in their ability to perform properly their advertised role and to protect data. Accepting that the alternative might possibly affect the conclusion that the number of incidents and vulnerabilities are steadily rising, the data does demonstrate a level or scale of the problem and a trend.

Not only are more incidents occurring, but the type of incidents is also expanding (e.g., distributed denial of service) indicating that those intent on mischievous or malicious activity are discovering both more and new vulnerabilities and exploiting them. This should come as no surprise since software developers are continuing to do business as usual by marketing new software with defects. Combined with the number of

[692] CERT, CERT/CC Statistics 1988-2002, Carnegie Mellon University, August 20, 2002, http://www.cert.org/stats/cert_stats.html.

uncorrected vulnerabilities in legacy systems, the possibilities for exploitation are limitless.

As a result of the research, the hypotheses can be answered as follows:

- The United States' national security can be imperiled by the inherent structural vulnerabilities of the information infrastructure system's:
  - interconnectedness within itself and with other critical infrastructures and
  - integration of software programs and software with hardware, but
  - not necessarily by the open architecture system.
- These three structural vulnerabilities can produce:
  - disruption of the information infrastructure system and/or data exploitation and
  - causal uncertainty of observed effects in the information infrastructure system.

Coda.

The research results lead to several other relevant observations. Both the information infrastructure system's vulnerabilities and its national security policy environment appear boundary-less or unbounded. Such a condition makes any effort to solve the issues more difficult, at least until new boundaries can be established. Vulnerabilities are not confined to one component or subsystem exclusively but affect the entire system because of interconnectivity. Policy issues cut across traditional bureaucratic boundaries creating tremendous competition to protect core departmental or agency functions making federal efforts to secure the nation's information infrastructure system much more difficult.

When examined as a system, information infrastructure security has two wholly different components that require different measures to achieve total system security: data protection for confidentiality and integrity and system functionality protection for data availability.[693] Exploitation of the system's vulnerabilities by intruders intent on accessing data for mischievous or malicious activity and by attackers intent on denying service clearly demonstrate these two different components and also the effects of exploited vulnerabilities for both purposes. Any information infrastructure system national security strategy and policy, therefore, should provide restricted access to data (if desired) to protect its confidentiality and integrity and system protection to protect the data's availability.

In order to achieve those ends, two different approaches accounting for each component's specific requirements should be adopted:

• System functionality (to insure data availability):

•• redundancy, resiliency, and diversity of system components, particularly network connections, to improve system survival[694],

[693] The information assurance objectives of confidentiality, availability, integrity, authentication, and non-repudiation implicitly recognize this observation.

[694] Redundancy increases survivability by providing more components that perform the same role and conceptually are available if the primary component fails for some reason. There is some justification to providing the same degree of redundancy to this critical infrastructure system as to other safety critical systems such as the Shuttle Space fleet that uses a total of five computers to perform simultaneously the same function and nuclear power generating plants.

Resiliency provides the system with the ability to absorb an attack or malfunction and continue to function, albeit in a possibly reduced mode. The system has shown over its history that it possesses a certain degree of resiliency since it has never (with the possible exception of the Christmas Day Harvard incident) suffered a complete failure.

Diversity provides greater options for performing the same task. Reducing the number of critical nodes will increase the survivability of the network by decreasing the number of single point vulnerabilities and incrementally changing the structure of the network from a scale-free to a more exponential structure.

- - systemic slack to provide more opportunities for intervention and more time to correct or mediate the effects of mischievous or malicious activity or systemic accidents, and
  - physical protection of critical system components to prevent malicious or mischievous activity
- support for research and development to increase data confidentiality and integrity.

The research and development should focus simultaneously on both those vulnerabilities most easily corrected and those that can create the greatest damage to the system. A sense of which those are can be gained from the analysis of vulnerabilities in Chapter 3. Information Infrastructure System Vulnerabilities, Risks, and Threats and the comparison of systemic vulnerabilities discussed earlier in this chapter. The most pressing need is to improve the software development process in order to produce less defective, and hopefully eventually defect-less, programs. As the research demonstrates, defective software programs are the most likely systemic vulnerability and essentially the root of most other secondary vulnerabilities. Given the state of software design and development, however,. dramatic results in eliminating defects from complex software systems are not anticipated in the short-, and probably the mid-, term absent a technological breakthrough. Producing software with less errors and faults, though, would make illicit intrusion to gain access to data or to deny service much more difficult; at least from a non-“insider” intruder.

Given the technical difficulty and expense of accomplishing these two recommended courses of action, survivability efforts pioneered by CERT should be continued and receive greater emphasis. The CERT researchers define survivability as

> "the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents."[695]

Survivability practices are risk management strategies that focus on the effects of a vulnerability exploitation instead of the causes of the vulnerability. They are a concession to the reality that "no practical systems can be built that are invulnerable to attack" and strive to overcome a vulnerability exploitation's effects to maintain system functionality without trying to identify and "fix" the vulnerability itself. These strategies are combinations of technical and executive decisions that acknowledge the conclusion of this research (and most other researchers of the issue): that "despite industry's best efforts, there can be no assurance that systems will not be breached."[696]

Education should be an integral part of survivability efforts. A concerted effort should be undertaken to educate users of the system's vulnerabilities and remedial "best practices" the effects affiliated with the vulnerabilities. Efforts like the CVE and SANS projects to publicize and hopefully obviate common software vulnerabilities should continue until these legacy vulnerabilities are eliminated. System security certification training and academic information-related disciplines should continue to provide more expansive techniques to detect and correct exploitation effects. Other innovative approaches should be developed to ensure that all users are aware of the risks not only to their own data and component, but also to the system as a whole. As previously stated, because of the nature of systems the security of the entire system is only as good as the weakest component of the system.

[695] Ellison, et.al, Foundations for Survivable Systems Engineering and Ellison, et.al., Survivability: Protecting Your Critical Systems.

[696] Ellison, et.al., Foundations for Survivable Systems Engineering and Ellision, et.al., Survivability: Protecting Your Critical Systems.

In order to generate consensus for a coordinated effort to accomplish these security objectives, a comprehensive national information infrastructure system national security policy needs to be developed. Absent government regulation of the IT industry, such an effort requires greater cooperation between both industry and the federal government and between departments and agencies within the federal government. The federal government should give serious consideration to enacting some type of anti-trust and Freedom of Information Act protection. Given current legislation, industry is prudent to be reluctant to provide vulnerability and exploitation information.

As discussed in Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy; NSD 42, National Policy for Security of National Security Telecommunications and Information Systems (established the NSTISSC); EO 13011, Federal Information Technology; and the Clinger-Cohen Act have a national security exemption. The problem is that the definition of national security systems is too restrictive: within this definition, a national security system cannot include "any system used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). This definition obviously does not correspond to many commercial information infrastructure systems. Congress should give serious consideration to broadening the definition so private sector vendors will be willing to be more forthcoming with information system infrastructure security vulnerability and exploitation data.

At the same time, Congress should devise some way to relieve the federal agencies that receive sensitive information from the private sector from having to comply with all requests for information under the Freedom of Information Act. Without some statutory relief on both issues, the private sector will continue to be reluctant to provide voluntarily information infrastructure system security data to the federal government.

Given the evidence of the involved parties' past behavior on both policy and research and development (See Chapter 4. Policy Dis-Organization: An Organizational Analysis of U.S. Government Information Infrastructure System Security Policy), one cannot be overly optimistic about the prospects for success on either count. As Michael Vatis, Director of the NIPC, indicated in March 2000,

> "People have been saying for a long time that it's going to take an electronic Pearl Harbor for people to take security seriously. There's a kernel of truth there because we live in an event-driven society."[697]

U.S. airport and airline security did not receive the priority to become truly effective until after the September 2001 terrorist events. One can only hope that the events of September 11th provided the galvanizing impetus for greater cooperation between the contending stakeholders to improve the information infrastructure system's security for the national good without the need for an "electronic Pearl Harbor."

In hindsight, September 11, 2001 would seem to be the more obvious endpoint of this research than the termination of the Clinton administration. The horrific events of that day forever changed the American public's and government's attitude and outlook on threats to nation's security. The events of 9/11 should have provided the impetus for a more invigorated effort to secure the nation against all of the diffuse risks to the nation's well-being, economy, and defense.

The early Bush administration essentially continued the same information infrastructure system national security policy process established and pursued by the Clinton administration, i.e., working within the policy environment already established but

[697] Zuckerman.

focused on the PD 63 structure and process dependent on collaborative planning and action by the government and the information technology industry. The effort to finalize and publish a national security document for information infrastructure system security extended the deadline for comment on the draft Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue but did little else to initiate new activities or programs.

But, the post-9/11 change by Americans in the nation's vulnerability has not provided the impetus for information infrastructure system protection that it has for threats that are capable of creating more spectacular results, i.e., specifically, use of a weapon of mass destruction within the nation or use of a transportation means to create mass casualties and attack a symbol of the nation and its way of life. Although potentially much more of a risk to the national well-being, economy, defense, etc. than the current primary foci of attenuated homeland defense efforts, information infrastructure degradation or destruction unfortunately does not appear to the public and policy makers to have the seriousness of a weapon of mass destruction or mass casualty attack.

Unfortunately, new efforts in information infrastructure system national security are few. The long awaited The National Strategy to Secure Cyberspace is still a draft. In fact, one could also argue that the administration has continued the policy pattern established during the 1990s: increasing the complexity of the policy environment. Not only has a new executive position, President's Special Advisor for Cybersecurity been created, but an entirely new Executive Branch department has been added to the picture without any statutory or administrative relief of the already existing policy structures or processes. So although September 11th would seem to be the more logical cutoff point for a discussion of any aspect of American national security, dramatic change has not occurred for information infrastructure system national security the way it did for other aspects of defending the homeland. The federal government has essentially adhered to the policy model established by the Clinton administration during the decade of the 1990s.

APPENDICES

APPENDIX A

KEVIN POULSON

> “It's no news that the phone system is not secure. The phone company has made a cold-hearted financial decision that it is cheaper and easier to spread around the cost of the phone calls people complain about than to pay programmers to improve the auditing.”[698]

The case of Kevin Poulson dramatically illustrates the folly of the quote’s sentiments within the telecommunications sector. Poulson was not only able to access any file he chose, but he was also able to control and manipulate the transmission medium of the information infrastructure system, in this case, the phone system. It is legitimate to include the phone system in the research’s discussion of the information infrastructure system (the object of this analysis) since, by definition, the information infrastructure system is the integration of computing and transmission assets (See Chapter 2. Information Infrastructure System).

Nothing in this case should be misconstrued as a vindication or glorification of hacking or of Poulson’s feats. My sole purpose for publicizing Poulson's exploits is to demonstrate the vulnerability of and risks to the information infrastructure system to unauthorized access.

Trying to achieve objectivity is difficult when describing any hacker’s exploits because most information of such activity comes from sources sympathetic to the hacker. In this case, independent corroborating and conflicting data where available have been used to

[698] Doug Fine, "Why is Kevin Lee Poulson Really in Jail?" fine@well.com, September 3, 1993, 18.

achieve as much objectivity as possible.[699] Even without being completely objective though, the case presents overwhelming and persuasive evidence of the vulnerability of and risks to the information infrastructure system to intruders, albeit through a highly unorthodox method for intruders.

I specifically chose this case to demonstrate the ease of unauthorized access because Poulson's case:

- represents, perhaps, the worst of worst-case scenarios for an unauthorized intrusion (generally dependent only upon the intruder's knowledge of and exploitation of the computer system's vulnerabilities);
- demonstrates that nothing within the information infrastructure system is "safe" from unauthorized users; and also because
- Poulson's intent generally was not malicious, at least initially.[700]

Poulson's case is compelling not so much because of what he was able to accomplish (although that was impressive in itself), but because of how he accomplished it. Like many successful hackers, Poulson had almost free reign on those computer networks he chose to access. Unlike any other hacker, however, he did not rely entirely on defects in software and computer networks to provide him unauthorized access. Poulson primarily relied on his

[699] An account of Poulson's life, The Watchman by Jonathan Littman, was used as the original source for much of the data in this case study. Mr. Littman developed his data from interviews with Poulson himself, as many of his associates as possible, the investigators and authorities who prosecuted him, court records, police records, and telephone records. Mr. Littman is not overly sympathetic to Poulson. He never excuses his deeds but does present Poulson's point of view in an attempt to explain his behavior. In fact, Mr. Littman castigates Poulson for becoming a "master burglar, associating with hardened criminals, hacking for profit, and pimping electronically." Mr. Littman also dismisses Poulson's claim that he was providing a service for society by exposing the abuses of privacy and freedom by the government and the telephone company because of his criminal and personal motives clouded whatever good intentions he may have once had (Littman, 284-288).

[700] Poulson seemed to value the sheer excitement of the act of gaining access to prohibited venues more than using that access for some personal gain, fame (or, notoriety) or criminal/malicious intent (Littman, 4 and 11). My research of the other sources corroborates that his motivation was primarily for the thrill of eluding authorities charged with keeping people out of places they are not authorized access.

unparalleled knowledge of the public switch network and the switches themselves to provide access, practically with impunity, [701] to the information infrastructure system and then the computer networks and data he sought.

As Winn Schwartau says in Information Warfare,

> ".... he who controls the switch wields immense power. He can listen to and tape conversations, turn a home phone into a pay phone or have the calls forwarded to another number. The switch contains billing records, payment histories, addresses, and other pertinent personal data for everyone with a phone. Every call you make, every call you receive, is on record in the telephone companies' computers."[702]

Poulson was capable and able to use this power to his advantage. By gaining control of the switches, he was able to access successfully confidential personal, institutional, and national government files. If a lone hacker, albeit a "superhacker,"[703] can accomplish Poulson's feats without resources other than his own wit, knowledge, and perseverance, then a group or nation intent on accessing the U.S. information infrastructure system to execute malicious activity should be able to so also.

Poulson personifies the hacker who uses research to understand the system he is attacking. It is as if his whole life revolved around intimately knowing and using the technical communications systems that had become an everyday part of modern life. Poulson went to great pains to increase his knowledge of the telephone network and **any** (emphasis added by author) switch in operation within the public switch telecommunications system.

[701] Judy Petersen, a Pac Bell spokesperson, said, "there isn't much the phone company can do about a hacker of Kevin Poulson's sophistication" (Fine, 18). Poulson seemed to value the sheer excitement of the act of gaining access to prohibited venues more than using that access for some personal gain, fame (or, notoriety) or criminal/malicious intent.

[702] Schwartau, Information Warfare: Chaos on the Electronic Superhighway, 123.

[703] A superhacker does not brag or post information on the bulletin boards; rather, he watches what others are doing and absorbs information about new and different ways to compromise a system. If he decides that he wants on your system, he will eventually get there, and if he decides to do something to your system, he will do it, usually without you knowing it. Fortunately, the number of hackers who fall into this category is a microscopic percent of the total number of hackers (Pipkin, 5).

Poulson's fascination with the telecommunications systems began at an early age. At thirteen, he was "phreaking"[704] the phone system by imitating the pulses switches recognized for different numbers with different pitched whistles. Once into the public switch network, he was in a position to acquire free access to any telephone number in the world.

But, Poulson was not content to stop at being able to manipulate the public switch network. He wanted to understand how he was able to do it and to search for other techniques for manipulating the system. He spent his free time studying Bell Labs' technical histories of the evolution of the telephone network and journals that detailed each new technical advance. He also searched dumpsters at the local central office for anything that had to do with network operations.[705]

Poulson became so knowledgeable of the network's operations that he was able to recognize the type of switch by its ring and busy signal, and sometimes just by its idiosyncratic clicks. He understood the hierarchical ranking of switches and the mechanics of both old and new switches and the improvements made to them. Through his dumpster searches, Poulson found the telephone numbers for internal phone company administrative and maintenance lines. Poulson also disassembled a touch-tone phone and re-wired it to exploit the ghost key column designed primarily to give the military override capability over other phone service to give himself that same override capability.[706]

From phone phreaking to hacking was a natural progression. Poulson sharpened his skills with early Radio Shack model computers, but once again he was not content to learn

[704] Phreaking is using the tonal peculiarities of the telecommunications system to receive free service (Littman, 11-12 and Poulson, Letter to the Honorable Manuel L. Real).
[705] Littman, 13-14.
[706] Littman, 15.

only how to use them. He studied the BASIC language manual learning how to write his own programs.[707] In 1983, he succeeded in accessing the computer at UCLA and gained its full menu of options, to include its Internet connections.

He continued to hone his hacking skills through a junior programming job at Science Research, Inc. (SRI). Although an entry-level position, Poulson used his free time to study security manuals, UNIX code and programming, and the latest computers and their source codes.[708] At the same time, he was learning more about the peculiarities of the old electromagnetic switches and Steppers. He discovered that the newer ones have a direct-dial number into the switch that could then be converted into free conference lines.[709]

By physically breaking into more than two dozen telephone central offices and corporate headquarters after hours, Poulson gained greater insight into how the different types of newer switches worked, stole passwords and test trunk sets, collected discarded Crossbars, and began to accumulate a library of switch technical manuals.[710] He even hauled home a 300 pound 1960s long distance operator (Traffic Service Position System) console used to patch through long distance calls so he could study it. When not breaking into central offices, Poulson hacked into the phone company's Computer System for Mainframe Operations (COSMOS) to learn more secrets about the way the company did business: how it initiated or modified phone service, added or removed custom calling features, checked for lines marked for repair, and looked up unlisted numbers.[711] With his knowledge of switches, Poulson could then order anything he wanted from the Cosmos system.

[707] Littman, 18.
[708] Littman, 48-49.
[709] Littman, 23and 56.
[710] Littman, 57-58, 62, and 73.
[711] Littman, 72.

Each day before he began hacking, Poulson electronically searched the offices that serviced his, his parents', and his acquaintances' phones to see if they have been tapped. By now, Poulson could do just about anything he wanted with the phone system:

> "One evening, he hacked a Pac Bell network in nearby Hayward and "leapfrogged" to a local network at San Ramon, Pac Bell's massive administrative headquarters. Once inside the Sam Ramon net, he changed a variable, shifting the way the system interprets keystrokes to trick it into launching a simple editing program that enabled him to slip into yet another network. From San Ramon, Kevin scanned for files named "dial-up," and found one that didn't require a password since it was designed to go only from Pac Bell's most secure network to its less secure network. Kevin cleverly turned off the dial-up and reversed it, connecting himself to the Bell Application Network Control System (BANCS). Within BANCS Poulson could run nearly every Pac Bell ordering or maintenance program - Premis (linked addresses to telephone numbers), Lmos, Sword, and Word (a Pac Bell system that tracked private circuits). He could retrieve everything from customer names to telephone numbers, addresses, and billing and credit information."[712]

He developed computer programs to access these proprietary Pac Bell systems in order to detect test numbers and out-of-service numbers, and then established those numbers as his own.[713]

To earn some money, Poulson initiated a scheme to insure he won radio contests.[714] He took out several of the targeted station's series of incoming "in hunt" lines by programming Mizar (a front end to the central office's switching computer) to disconnect the hunt sequence for incoming lines seconds before the contest begins. His handpicked contestants now had a better chance of connecting with the station and winning. Poulson manipulated the station's lines remotely from his apartment while his contestant waited to be three-wayed to the station for the winning call.[715]

Later in his career, Poulson's techniques for winning radio contests became much more sophisticated. For one contest sponsored by KPWR in Los Angeles, he arranged for

[712] Littman, 82.

[713] Fine, 11.

[714] Kevin is known to have fraudulently won two Porsches, $22,000 in cash and at least two trips to Hawaii (Schwartau, Information Warfare: Chaos on the Electronic Superhighway).

[715] Littman, 114.

someone else at a location other than his apartment to be the winning caller. Poulson seized two of the station's lines and then bridged both of them to the arranged winner's location through his computer's communications ports and a couple of modems.[716]

On one of his forays into a central office, Poulson discovered the control terminal and manual for numbered test trunks and SAS units that allow the phone company to tap phone lines.[717] Poulson then deciphered the security callback sequence between the controller and the SAS unit allowing him to take control of a SAS unit's wiretap.[718] Later, Poulson stole a SAS directory that listed every Pac Bell SAS service area in Southern California. With his knowledge of Cosmos and the SAS security callback sequence, he now had access to every wiretap in Southern California. He also could tap any line in Southern California![719]

On a visit to the Mutual of Omaha building at the corner of Wilshire and La Brea, Poulson electronically tapped a Telnet circuit to his home phone by ordering a new circuit and bridge lifter through Cosmos. With two computers, he was able to listen to both sides of the digital conversation gleaning passwords and accounts typed in by users, as well as the system information logged by the host computer. He was able to learn the passwords to the Bank of America's home banking system, TRW Credit, Information America, Nexis/Lexis, and the California Department of Motor Vehicles. With this information, Poulson could find names, birth dates, weight, height, eye color, addresses, and warrants. He even found what seemed to be passwords and codes for electronic money transfers between major banks. With persistence, Poulson learned that three different people in three different

[716] Littman, 190-191.
[717] Littman, 122-123.
[718] Littman, 125.
[719] Littman, 129.

departments have to issue approvals to transfer money to a set list of payees and then discovered the passwords for those three different people. At first, he did nothing with this information.[720]

At some point, Poulson learned that you could activate a dead phone line taken out of service because of unpaid bills with a password. Of course, he could retrieve the password from the phone company's files and activate as many lines as he wanted while at the same time not disturbing the data entry for the dead line in the phone company's records. This, in effect, gave him as many private, unassigned lines as he wanted. With this knowledge, Poulson set up a phone network for a prostitution ring complete with over a dozen voice drops on a line tapped from a branch office of American Voice Retrieval after he mastered the office's password and login commands. Then he "created new digital DMS phone numbers, dialed each new number with SAS, and punched the 72# command, forwarding the lines to a North Hollywood choke point before the mass of incoming calls fed into his voice mail. There were no bills, no records, no sign of existence." To further obscure his identity, Poulson always randomly dialed someone else's voice mailbox before entering his number to step neatly over to his box. If anyone put a trap on his box, all they would trace is a call to another random box.[721]

When a competitor of Poulson's pimp convinced a telephone company employee to steal some of the lines Poulson had stolen and route them to the competitor's business, Poulson used Cosmos to switch them to his pimp on the weekend and then re-attached them

[720] Littman, 135-136.

There are allegations and suspicions in the other corroborating references that Poulson did engage in electronic theft of money from institutions at different times during his exploits. However, no one has ever been able to prove the allegations and Poulson has never publicly admitted to such activity.

[721] Littman, 141-145.

back to the competitor on Monday, effectively depriving the competitor of the lucrative weekend trade.[722]

Poulson also began a search through Cosmos for every Pac Bell DNR tap in the state of California. He wrote a program to streamline the process and have Pac Bell's computer do the work for him. His program searching millions of telephone lines ran on twenty Cosmos machines, half of them in San Diego and the other half in Hayward. In just ninety minutes, Poulson discovered roughly seven Pac Bell wiretaps scattered around the state. Using SAS he checked each one (essentially tapping the tappers) recording a description of each. [723]

On another of his late night central office visits, Poulson discovered a thin metal device with phone wires going in one end and out the other that intrigued him. Back at his apartment, he checked the circuit number listed on the device through Word and found that a Mark Yelchak in security at 180 New Montgomery was listed in the files as the contact person. Checking the building in various Pac Bell systems, Poulson discovered that a single floor was dedicated to a department called Electronic Operations with fifty phone lines. The files on each line contained a reference to the Pac Bell Computer Security System and revealed that each line had a tape recorder attached to it. He then tapped each line with SAS and monitored any activity over each, writing a summary of what he found. He discovered that there were seven working wiretaps.[724]

Next, Poulson repeated his statewide Cosmos Pac Bell wiretap search. He listened to each of those and discovered that they contained the same voices and had the same data as the seven he had discovered at 180 New Montgomery. He accidentally had discovered

[722] Littman, 188.
[723] Littman, 164-165.
[724] Littman, 165-167.

that each Pac Bell tap had two different monitoring lines, one in the local central office attached to the suspect's line and one at 180 New Montgomery attached to a tape recorder and the Pac Bell Computer Security System. Security investigators could dial any of the fifty original numbers and enter a one- to eight-digit security code to activate a tap. Learning the code would allow Poulson to activate the taps not in use so he could tap the tappers without SAS.[725]

Poulson also discovered that most AFLA-designated circuits were federal wiretaps. In this case, they terminated in the federal building at 1100 Wilshire, the Los Angles headquarters of the FBI. Poulson's discovery meant that the FBI allowed the phone company to track its wiretaps on-line, available for anyone with the knowledge to find and see. By checking "AFLA" circuits with another Pac Bell system, he discovered that the FBI was not the only federal agency to order wiretaps. The DEA and Secret Service, under the cover of Acme and Busy Bee answering services, also had wiretaps running to their Los Angeles headquarters.[726]

Next, Poulson set out to find who was being tapped. Using the B box of the tap gotten from the Pac Bell computers, he systematically checked the lines of the businesses with the building or block the B box identified. Once he located what seemed to be a likely suspect, Poulson could remotely tap the tapped line in the B box with SAS shores, then dial the suspected number or call every number in the targeted building or block. If he heard his own phone ringing on the federally tapped line through his own tap, he would have the phone number of the target of a federal investigation and could, if he wanted to, listen in. Each day Poulson polled the Southern California systems, checking dozens of central offices

[725] Littman, 167.
[726] Littman, 167-168.

at a time, to verify the federal wiretaps. He even knew future wiretaps before they were put in place because Pac Bell entered the circuit identifier and subscriber information into its computers as soon as it received a federal court order. But it was often days or weeks before the court ordered tap was installed.[727]

By now Poulson could systematically find any wiretap in Southern California. He conceptually could possibly extend the same capability to the rest of the nation and potentially the world. By now through Pac Bell's own on-line, Net accessible records, he had learned that Pac Bell had tapped thirteen telephone lines of the South African consulate in Beverly Hills, ten lines of the Israeli consulate in Los Angeles, fourteen lines of the Chinese consulate in Los Angeles, something near the Concord Naval Weapons Station,[728] the Splash restaurant (a reputed organized crime business), and a reputed mob boss, Ronald Lorenzo.[729] From 1989 to 1991, Poulson had access to nearly every federal and national security wiretap in California through his ability to hack into Pac Bell's computers, considered by hackers at the time to be among the most secure in the telecommunications business.[730]

Poulson displayed his tremendous knowledge and sophistication of the telephone system when he tapped one of his acquaintances that he believed was informing the authorities about his activities. Since the acquaintance's phone service was through an old electromagnet switch, Poulson knew that a SAS tap would have a noticeable click that would alert the acquaintance. Instead he installed a metal federal tap he stole from a B box

[727] Littman, 165 and 168-169.

[728] Presumably, the Soviet Consulate in San Francisco since a printout of the Consulate's phone service was among Poulson's data files confiscated and catalogued after he was arrested (Littman, 103).

[729] Littman, 170-171 and 277.

[730] Littman, 280.

As the Pac Bell investigators shifted through the evidence confiscated from Poulson's condominium, they found Cosmos printouts with handwritten notes and a diagram detailing wiretaps run through the Menlo Park office (Littman, 106 and 108).

in the phone closet of a random business in Hollywood. He then connected the side that would normally run to the federal building to a phone line that he activated, "bridge lifted" that line to his acquaintance's telephone company's central office where he wired it to the acquaintance's own phone line in a place on the frame where the splice would never be found. Finally, Poulson completed the tap by dialing the new line he had created at the phone closet with SAS.[731]

In 1989, as investigators began to close in on him, Poulson used his knowledge of the telephone system to make virtually untraceable phone calls. No one knew his address or phone number and the only method of contacting him was to leave a voice mail, which he retrieved (of course without any clues to his true location). Poulson could initiate a phone call by activating a trunk test set, pushing the pause button twice, and then dialing the number he actually wanted to reach. He had set up a number in Cosmos so that when he picked up his line, instead of getting a dial tone, his call traveled to a random Van Nuys trunk. He then toggled the test set's "on" button and his call bounced back and forth between random Van Nuys and Sherman Oaks trunks, until the test set allowed the number he was actually calling to finally connect. The call could be traced by the phone company, but would be time consuming and involve querying the different offices to locate the trunk activated and where the call originally initiated. To further disguise his calls, Poulson created a secret number and assigned it to a large federal agency in Los Angeles at the phone company's central office switch. Then he programmed that number to dial automatically an incoming trunk at the federal agency's private branch exchange. Once on the local PBX, the new route index sent it a 9 and Poulson had an outside line. Now he

[731] Littman, 178.

could call anyone and make it seem as if the call was originating from inside the federal agency.[732]

Poulson was finally indicted by a federal grand jury on January 17, 1990 for "engaging in a widespread pattern of breaking into government and telephone company computers and obtaining classified information from a military computer."[733] However, the authorities could not locate Poulson. In an effort to produce some leads, NBC's Unsolved Mysteries ran a story about him on October 10, 1990. Poulson had anticipated the show and had disconnected every 1-800 phone line that ran into the thirty-operator telecommunications center the show used for phoned-in tips from the show.[734]

Now that the authorities were looking for him, Poulson bolstered his efforts to insure his telephone calls could not be traced. He still made his calls through a trunk test set, changing the route index, bouncing the calls back and forth between random trunks to disguise their origin, but now he connected a pair of phone lines from the ESS computer at his local central office to the frame. Every fifteen minutes, the ESS computer forwarded an updated list of traps and traces to his on-line computer.[735]

But even this was not enough for Kevin. He wired his computer into all five of his residence's phone lines and attached relay switches to each line. He then wrote a program that continuously searched the ESS computer for the trace command. As soon as a Pac Bell technician keyed the trace command, his computer anticipated the command, the relay

[732] Littman, 196.
[733] Littman, 208.
[734] Littman, 246.
[735] Littman, 257.

switches activated, and the five phone lines went dead. He then reactivated his lines through his normal test set trunk-switching procedure.[736]

And of course, Poulson used encryption to prevent detailed searches of his files should they be captured. Even his encryption technique demonstrated the knowledge and sophistication Poulson had gained of the entire field of telecommunications and computers and the lengths he willing to go to preserve his own privacy. He chose for a key something he could remember without writing it down and, although not random, meant something only to himself; KPfofipOST, the keys he struck on his test trunk to make an untraceable call and the extra letters on a sixteen-button phone. To any other person, the letters would probably appear to be random. He then used Sun's and IBM's versions of DES (the Defense Encryption Standard), a fifty-six key technique used by federal agencies at the time. To doubly ensure the encryption was more difficult to decipher, Poulson encrypted his files two, three, and occasionally five times.[737]

Poulson was finally captured by the authorities on April 10, 1991,[738] not through electronic snooping or surveillance, but through old-fashioned detective work and betrayal by his friends. With his knowledge and expertise of the telecommunications medium, Poulson was virtually immune to the cyberforensics of his day and probably even today's more sophisticated ones. He did not need to use the tools hackers of today have to obfuscate their activity; he completely disguised his activity within the normal administrative and operational activities of the phone company. He was charged in two federal courts with

[736] Littman, 257-258.

[737] Littman, 258.

The system was apparently so successful that when his computers and files were finally captured, NSA spent several months using their Cray supercomputer in a "brute force" attack to crack them. The government printed out nearly ten thousand pages of material (Littman, 176).

[738] Littman, 103.

crimes from his hacking and tried in federal and state court, found guilty of some of the charges brought against him, and sentenced for those charges.

Most of Kevin's manipulation of the telephone lines and switches were attempts to maintain anonymity and to locate information files. He still had to use many of the same software vulnerabilities discussed in Chapter 3. Information Infrastructure System Vulnerabilities, Risks, and Threats to access the computer networks and computers once he had located them. But with his knowledge of computers and programming and persistence, few, if any, files he wanted to access were safe. Poulson surely demonstrates the ease of access and ease of movement within and between different system levels of the infrastructure's open, interconnected system organization as well as the ubiquity of software vulnerabilities.[739]

[739] "It goes beyond hacking with Kevin. He knew how to allow himself to see some really serious things.... It's like, if you can access the phone lines, I'm not kidding, you can access anything. You can move $1 million from one bank account to another" (A former friend of Poulson's quoted in Fine, 3).

APPENDIX B

DENIAL OF SERVICE

B.1. Introduction.

There is a difference between denial of service (DoS) and denial of service attacks. Denial of service is any type of incident resulting from an action or series of actions that prevents any part of an information system from functioning.[740] Denial of service occurs when a majority of the system resources are consumed to the extent that other users lack proper resources to perform desired functions. This inability to use some or all parts of the computing or information system is, and has been, an integral part of digital systems since their inception. In the early days of computer and network system development, this stoppage was generally called "crashing the computer (or system)," was unintentional, and was caused by an inherent hardware or software error or fault (initially called a "bug"). In such cases, the denial of service was annoying but was an accepted inconvenience of using the early computers and incipient networks.

Minor denial of service occurrences, e.g., a cursor that does not behave as expected, can be inconvenient or frustrating, but is not generally damaging to the data stored in a computer. A more severe incident could lead to destruction of, loss of confidentiality of, alteration of, or the inability to process data.[741] Because of this loss of data system

[740] United States National Security Agency, National Information Systems Security (INFOSEC) Glossary.
[741] Katherine Fithen, "Tech-Wise: Countering the Threat Posed by Distributed Denial-of-Service Tools," Infosec Outlook 1, no. 1 (April 2000), http://www.cert.org/infosec-outlook.

resources, denial of service is primarily a risk to the information assurance (IA) objective of availability, but can obviously also be a risk to the other four IA objectives (confidentiality, integrity, authentication, and nonrepudiation) as well (See Chapter 1. Introduction for a more detailed discussion on the five information assurance objectives).

A denial of service attack (whether it is simple or distributed), by contrast, is an explicit attempt to prevent **legitimate** users of a service from using that service. A denial of service attack can be simple (a single source targeting a single target only) or more sophisticated [single source attacks against multiple targets, multiple source attacks [distributed denial of service attacks (DDoS)] against single and/or multiple targets (a relatively recent phenomenon that only began to appear in June 1999).[742] Both simple and multiple source attacks that can combine two modes (using the system to deliver the initial attack and the targets' software to further propagate the attack) exploit the structural, hardware, or software vulnerabilities discussed in Chapter 3. Information Infrastructure System Vulnerabilities, Risks, and Threats.

Generally, a DoS attack floods a system's network with packet streams[743] of useless data preventing legitimate traffic, including attempts to trace the attack, from traversing the network.[744] However, a DoS attack can also attempt to:

- disrupt connections between information infrastructure hardware,
- prevent a particular individual from accessing a service,

[742] Neumann, "Denial of Service" and Houle and Weaver, 19.

[743] "Packet flooding" (e.g., TCP packet flooding, ICMP packet echo request/reply (ping floods), and UDP packet flooding) is the most common attack currently and works by sending a large number of packets to a destination causing an excessive amount of endpoint, and possibly transit, bandwidth to be consumed (Houle and Weaver, 2-3).

[744] Krause, "Resolving Internet Security" in Ruthberg and Tipton, S-249-250; Needham, 45; Carnegie Mellon University, Results of the Distributed-Systems Intruder Tools Workshop, November 2-4, 1999, CERT Coordination Center, Software Engineering Institute, Pittsburgh, PA., December 7, 1999, 1 and 3; and Neumann, "Denial of Service Attacks."

- disrupt service to a specific system or person.

An attacker attempts to accomplish these effects by:

- consuming scarce, limited, or non-renewable resources;[745]
- destroying or altering configuration information; or
- physically destroying or altering network components.[746]

As troubling as the direct effects of a denial of service attack can be, collateral secondary effects are increasingly becoming a serious concern.

- Increases in security monitoring or service activity logging during a DDoS attack, even in those systems not under attack, can consume such a high amount of resources that the attack achieves its objective in an untargeted system.
- Increase in traffic during a denial of service attack can have a direct financial effect, particularly on measured use circuits, by increasing circuit costs.
- Effects from the DoS target can "cascade" to other interconnected hosts and/or users.
- Networks with relatively high numbers of infected and active sources can become saturated by address resolution protocol storms. Scanning activity from a worm

[745] Scarce, limited, and non-renewable resources required to operate computers and networks include:

- network bandwidth,
- memory and disk space,
- central processor unit (CPU) time
- data structures,
- access to other computers and networks, and
- environmental resources, e.g., power, cool air, water (Neumann, "Denial of Service Attacks").

DDoS networks generally are able to overwhelm the available bandwidth effectively collapsing the target, especially when using legitimate or expected protocols or services as the vehicles for packet streams (Houle and Weaver, 17).

[746] Neumann, "Denial of Service Attacks."

Clearly, as mentioned earlier and similar to other infrastructure exploitations discussed in Chapter 1. Introduction, a denial of service attack can be caused by physical destruction of the information infrastructure system's hardware. Once again, I will exclude this means of affecting the function of the system from further discussion for the same reasons previously stated in Chapter 1. In this discussion of denial of service I intend to limit my research to methodology that exploits the system's technical, architectural, and software vulnerabilities.

deployed by a highly automated attack tool (e.g., Code Red, Code Red II, and Nimda) can lead to isolated loss of service and damage to various networked devices such as printers and DSL modems.

- Disconnecting from a network or the Internet to prevent internal system infection by the worm can, in effect, unintentionally achieve the attack's desired effect.[747]

What make denial of service attacks potentially so perilous is the possibility of massive outages (to include the even the largest networks)[748] through both direct and collateral effects and the absence of general preventive solutions available today or likely in the near future.[749] Since the network is a system, network security is highly interdependent and, to a large extent, every node's security is dependent upon the state of security of every other node on the network.[750]

DDoS attacks are particularly difficult to detect since they

- come from many sources, including multiple unwitting intermediary systems ("zombies");
- use unprotected Internet nodes around the world to coordinate the attacks, and
- can cross several autonomous system boundaries in highly distributed attacks.

[747] Houle and Weaver, 18-19.

[748] Fithen.

"A single, simple, command ...could result in tens of thousands of concurrent attacks on one or a set of targets" (Carnegie Mellon University, Results of the Distributed-Systems Intruder Tools Workshop, 1 and 3).

[749] Neumann, "Denial of Service"; Houle and Weaver, 18; Carnegie Mellon University, Results of the Distributed-Systems Intruder Tools Workshop, 1,3, 7-8, and 12; Fithen; and Needham, 45.

[750] Houle and Weaver, 2 and Carnegie Mellon University, Results of the Distributed-Systems Intruder Tools Workshop, 2.

Each attacking node has limited information on by whom and from where the attack is initiated, and no node need have a list of all attacking systems.

Traffic flows near a target may appear to be from a small number of source addresses and with relatively few physical network paths. When tracing from a victim back to multiple attack sources, traffic flows will probably disaggregate into many separate source addresses and physical network paths. Most attackers will also often hide the identity of the machines used to execute an attack by falsifying (spooking) the source address of the network communication. All of these techniques significantly increase the difficulty of identifying the source and responding. Further, as attack scripts become increasingly available, DDoS attacks will more than likely become even more trivial to launch making them more frequent, more annoying, and more costly.

B.2. Distributed Denial of Service (DDoS).

Basic denial of service attack methodology has changed little since 1999 and there is little incentive for perpetrators to search for new or improved methods since the tools employed since then are still very effective. Today, most DoS attacks take advantage of the distributed structure of the information infrastructure system's network architecture. A distributed system attack uses the now prominent distributed client/server structure of the information infrastructure system against itself (See Figure B-1. Typical Distributed-Systems Attack Methodology for illustration of a distributed denial of service attack's dynamics).

Typically, such an attack will involve a large number of sites simultaneously and be focused to attack one or more victim hosts or networks. The attacker will control a small number of "masters," which in turn control a larger number of "daemons."[751] The machines on which these daemons are installed are increasingly being connected as an "attack" network ranging in size from tens to hundreds of nodes. Of course, given the interconnected nature of the information infrastructure system's structure these masters and daemons are normally installed on different servers or routers that can be located anywhere geographically.[752] The individual machines/nodes in the "attack" network can also be automatically updated by the master machines, enabling rapid evolution of tools on an existing base of compromised machines.

These daemons will then be used to launch packet flooding or other attacks against victims targeted by the attacker. Upon a command from the attacker, the master can issue attack requests (e.g., victim addresses, attack duration, and other attack parameters) to the daemons in its list. Upon receipt of the attack request, the daemon proceeds to execute the attack, usually by flooding the victim with packets. However, a truly sophisticated attacker might use the echo and chargen services to create oscillation attacks that will bounce data between machines indefinitely.[753] Once activated, these technologies typically proceed without further communication from the perpetrator (attacker).

What changed in 1999 is the employment methodology of DoS tools:

- ubiquity of automated self-propagating worms,[754]

[751] Daemons are essentially software "programs used in the attack" (Fithen).

[752] Fithen.

[753] Fithen.

[754] Houle and Weaver, 10.

Although the 1988 Morris worm used a form of automated (autonomous) propagation, DoS attackers did not routinely use automated propagation again for another 12 years with the appearance of the Ramen worm in January 2001. One reason might have been the general difficulty and time required in executing a DoS attack and the relative ease with which the perpetrators could be determined and disrupted. (Houle and Weaver, 7, 11, and 15-16).

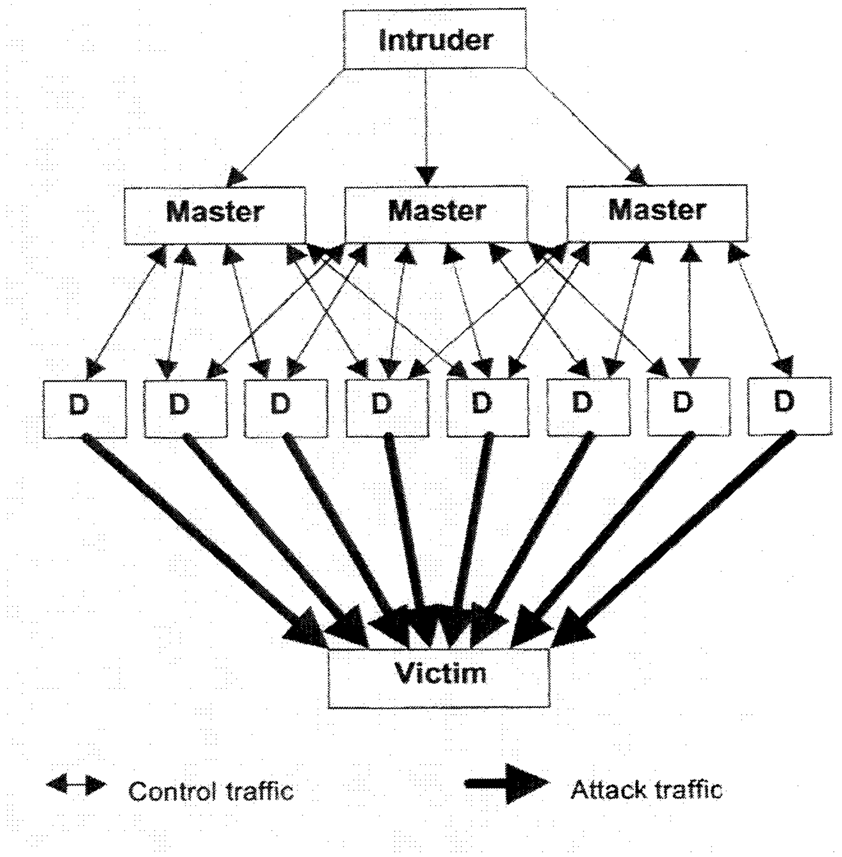


Figure B.1. Typical Distributed-System Attack Methodology[755]

[755] Carnegie Mellon University, Results of Distributed-Systems Intruder Tools Workshop, 5.

- blind targeting of specific vulnerabilities,[756]
- selective targeting of Windows end-users and routers,[757]
- use of Internet Relay Chat (IRC) networks and protocols as the DDoS attack agents' control infrastructure, and
- use of encryption to obfuscate attempts to disrupt an attack or locate a "master."

Another new trend began with the May 2000 VBS/LoveLetter incident: social engineering (an e-mail attachment in this instance that the recipient had to open to activate the DoS agent) to install the DoS agent instead of exclusive reliance on purely technological deployment of the agent.[758] The end result of this automated, simultaneous attack from all daemon nodes at once is to flood the "network normally used to communicate and trace the attacks" to an extent that legitimate traffic is prevented from entering and traversing the network.[759]

B.3. History of DoS.

Although DDoS seems to be the attack of choice these days,[760] what has happened with denial of service occurrences over the history of computing is symptomatic of why and how existing information infrastructure system vulnerabilities are exploited. Bob Kahn, a

[756] Blind targeting is non-specific opportunistic targeting based on a basic random number generation algorithm, highly automated, often highly vulnerability-specific, and involves little human interaction during the execution of the attack (Houle and Weaver, 12).
[757] Targeting of the Windows operating system represents a qualitative shift in attack strategy. Traditionally, most DoS attacks have targeted the notoriously vulnerable UNIX system (See earlier discussion of vulnerabilities in Chapter 3. Information Infrastructure System Vulnerabilities, Risks, and Threats) but with Microsoft's healthy share of both the personal computer and server operating system market, attack of the Windows system opens up an entirely new, fertile, and unexplored vulnerable front with a relatively easy identifiable population of end-users for potential DoS attacks. Windows users are perceived by potential attackers as less technically sophisticated, less security conscious, and less likely to be protected against or prepared to respond to attacks than the professional system and network administrators more likely to responsible for UNIX-hosted components (Houle and Weaver, 10, 13-14, and 17).
[758] Neumann, "Denial of Service"; Houle and Weaver, 3, 9, and 19-20; and Fithen.
[759] Fithen.
[760] See Houle and Weaver, 4-9, for a timeline highlighting some of the major trends in the increasingly sophisticated evolution of attack technology.

member of the original Bolt Beranek and Newman (BBN) team chosen in 1969 by the Defense Department's Advanced Research Projects Agency (ARPA) to design and implement the first network connecting computers (the precursor to the current Internet), was always worried about "flow control of packets from one side of the network to the other." Even though the network was designed to choose the most optimal route (link) between nodes, any given "link would only accept one message at a time on a given link." Messages were not transmitted by the network until the transmitting Interface Message Processor (IMP) received an acknowledgement that the previous message had arrived error-free at the destination host. Messages waiting to enter the network were stored in a queue in a memory buffer in the IMP decreasing the total memory available to handle messages. That meant it was impossible to send a continuous stream of messages over any single link in the system from one host to another.

Kahn was convinced that this "Ready for Next Message (RFNM)" strategy would cause "fatal congestion of the network's arteries" (links). Although the adopted strategy prevented the IMP's from overload, it also reduced overall system service and, more importantly, would cause the both the sending and destination IMPs' buffers to "fill up." The transmitting IMP would fill up with messages in the queue waiting to be transmitted thereby effectively restricting the amount of memory to receive all packets of an incoming message. "...incomplete messages would be sitting in the receiving IMPs waiting for their final packets to arrive so the entire message could be reassembled" and the "RFNM message transmitted, but "there would be no room for the packets to arrive."

However, Kahn's views were not entirely embraced by the rest of the BBN design team. The team acknowledged that the initial flow control scheme for the network was not designed for a huge network, but "with only a small number of nodes they thought they could get by with it." With much the same attitude of today's software and network developers, the rest of the team "just wanted to get the network up and running on schedule." The design team never thought the system was going to be perfect, but, because of the technical challenges, only wanted it to work. As the network grew, the team reasoned that they would have time to improve its performance and correct the problems of the initial network.[761]

Kahn did have his vindication though once the initial four nodes of the network were installed and operational. He convinced his supervisor, Frank Heart, to let him test the system to determine if his intuition and calculations were correct. Just as he predicted, by besieging the IMPs with packets, within a few minutes the system was "catatonic,"[762] the first denial of service attack of a digital information network system in history.

BBN redesigned the flow scheme to reserve enough space in the IMP memory buffers for reassembly of incoming packets. "A specific amount of reassembly space for each message would be reserved at a destination IMP before the message would be allowed to enter the network. The sending IMP would check, and if told that there was insufficient space available in the destination IMP's buffers, the RFNM was delayed." Through simulations, the design team determined that the new scheme would succeed in limiting network traffic to only the quantity the system could handle.[763]

The network system that evolved out of the initial effort by ARPA/BBN did in fact experience denial of service episodes. Because of the relative simplicity of the network

[761] Hafner and Lyon, 129-131 and 158.
[762] Kahn recalls that it only took twelve packets to overload the system and bring it to a halt (Hafner and Lyon, 157).
[763] Hafner and Lyon, 173

compared to today's systems, relatively few network-wide "crashes" (denials of service), none of which were very long lasting, occurred. One of the most famous (or infamous) was the Christmas Day 1973 incident that also demonstrated the synergistic effects a vulnerability exploitation could have on an interconnected information system. A fault in the Harvard IMP caused the machine to "read out all zeros into all of the system's other IMPs' routing tables, even BBN's, thereby informing all other IMPs that Harvard had just become the shortest route – zero hops – to any destination on the ARPANET." All traffic on the system, even BNN's used to diagnose, control, and debug data traffic, was transmitted to Harvard. With nothing being transmitted from Harvard, the entire system eventually was completely shut down. BBN finally had to "cauterize" (cut off) Harvard from the network to debug the Harvard IMP and the rest of the system and then reconstitute the network.[764]

Instances of denial of service continued to occur on the network,[765] but they were unintentional or accidental. These incidents annoyed and concerned researchers and users because of the disruption, but most users did not consider denial of service a security violation, more a fact of life of using the new tools for data storage, manipulation, and exchange. Denial of service, though, did become a security issue when such occurrences became deliberate and/or malicious attempts to deny the use of a computer or some part of the information data system to users.

[764] Hafner and Lyon, 195.

The April 1997 MAI incident could have possibly produced the same effect but for early human intervention (See Chapter 3. Information Infrastructure System Vulnerabilities, Risks, and Threats for discussion of MAI incident).

[765] The ARPANET also "crashed" on October 27, 1980, but was the result of "bits being dropped in the time stamp of one status word" (Robert D. Houk, "Single-bit Error Transmogrifications," The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 73 (November 9, 1988), http://catless.ncl.ac.uk/Risks/7.73.html).

Generally, the first acknowledged instance of such an event was the November 1988 Morris virus.[766] A 23-year-old Cornell University doctoral student, Robert T. Morris, created a worm, "injected" it into the ARPANET system, and subsequently infected "thousands of computers nationwide." The basic object of the worm was to get a shell on another machine so it could reproduce further. The worm eventually slowed and eventually halted approximately 6000 computers nationwide by "replicating itself and taking up memory space, but did not destroy any data."[767]

Some controversy surfaced at the time of whether Morris's intent was truly malicious or whether the effect was an accidental programming error. According to Morris, the intent of the worm was to only copy itself from computer to computer via the ARPANET simply to prove that it could be done.[768] A team at MIT also determined through reverse engineering that there was no code in the worm designed to harm files. The MIT team further found very little effort on Morris' part to hide the behavior of the code making it easy to identify subroutines.[769] However, in the process of trying to make the worm survivable even after detection and removal, Morris used a "parameter invoking a one-in-15 reinfection"[770] that eventually degraded each attacked system.[771] Regardless of intent, the worm Morris introduced into the ARPANET wreaked havoc on the system.

[766] van Wyk.

[767] Brian M. Clapper, "Suspect in Virus Case," The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 71 (November 6, 1988), http://catless.ncl.ac.uk/Risks/7.71.html and van Wyk.

[768] John Markoff, "The Computer Jam – How It Came About," New York Times, November 8, 1989 and van Wyk.

[769] Mark W. Eichin, "Internet Virus," The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 71 (November 6, 1988), http://catless.ncl.ac.uk/Risks/7.71.html.

[770] Markoff originally reported that the worm was designed to re-infect every ten queries. Eichen alleges that Markoff misunderstood his original comments about the methodology of the worm's attack. The code actually was "BACKWARD, so it re-infected with a *14* in 15 chance (Mark W. Eichen, "Re: NYT/Markoff: The Computer Jam – How It Came About," The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 73 (November 9, 1988), http://catless.ncl.ac.uk/Risks/7.73.html).

[771] Peter G. Neumann, "Re: Worm/Virus Mutations," The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 71 (November 6, 1988), http://catless.ncl.ac.uk/Risks/7.71.html and

The Morris worm propagation throughout the Internet was limited to only UNIX systems, actually the Berkeley version of UNIX. Morris initiated his program from his computer at Cornell sending it to a computer in the MIT artificial intelligence laboratory to which he had "log on" privileges. Morris used what are now three classic means of propagation for his program:

- the finger service ("via a bug in the '/etc/fingered' command"),
- the sendmail service ("via the 'debug' command"), and
- "password guessing and the shell /rexec/rsh/etlnet logins."

The program exploited a secret backdoor[772] in sendmail that allowed any message written in C-code to be mailed like any other message. The original writer of the sendmail program had intentionally written the backdoor into the code to facilitate code writing and updating. This C-code message, if written correctly, would have access to the computer's internal control files and not just the personal files residing on the computer. By including two object or binary files, Morris made the program easier to execute on both Sun Microsystems or Digital Equipment VAX computers without additional translation. One of the binary files had the capability of guessing the passwords of users on the newly infected computer by first reading the list of users and then systematically using permutations of the users' names or a list of commonly used passwords. If successful, the program signed on to the computer and used the privileges of that user to gain access to additional computers in the ARPANET system.[773] Or, the program could use the finger command's known error[774]

van Wyk.

[772] Only a small select group of computer experts, including Morris, knew of this 'backdoor" (Markoff, "The Computer Jam – How It Came About").

[773] Markoff, "The Computer Jam – How It Came About."

[774] A computer's control programs can be accessed if an excessively long message is sent to "finger" (Markoff, "The Computer Jam – How It Came About").

to gain access to users' computers that had logged on to the infected machine through the network. The worm also could use the ".rhosts" and "/etc/hosts.equiv" files to determine trusted hosts to which to migrate. Finally, if these three methods were not successful in gaining access to another computer, the worm would open "/usr/dict/words" and try every word in the dictionary to gain access.[775]

Whichever method used, the worm attempted to run a "/bin/sh" on the infected machine, then fed it a set of commands to build a new program, "sucked over an unlinked VAX or Sun image," linked this with the system's local libraries, and then "executed it."

Once the worm was running on the new site, it chose paths from:

- routing tables,
- interface tables,
- user ".forward" files,
- user ".rhosts" files (but only as a source of hostnames), and
- the "/etc/hosts.equi" command

to find new hosts to which to propagate.[776]

The program also signaled its location back through the network to a computer at the University of California at Berkeley to mislead researchers into thinking that the program had originated there instead of Cornell.[777] Further, the program signaled other computers to determine if they had been infected. If not, the program would infect it, or would infect a machine once every 15 times it queried the machine regardless of the response received.

[775] van Wyk.

See van Wyk for a much more detailed description of each of the three different methods Morris' worm used to attack other computers.

[776] Eichin, "Internet Virus."

[777] There is speculation that the signals to the computers at Berkeley ("ernie.berkelyey.edu") were intended to monitor the spread of worm (van Wyk).

This one in 15 infection choice was too short though. The speed of the ARPANET bounced Morris' program back and forth through the network in "minutes, copying and recopying itself hundreds or thousands of times on each machine, eventually (using all of the computer's capacity) thereby stalling the computer and then jamming the entire network."[778]

The Morris worm is noteworthy not only for its DoS effects but also because warnings of the worm were forced to be sent over the Internet. Emergency response personnel did not have the telephone numbers of colleagues in other organizations to which the warnings needed to be sent. In many cases, these electronic warnings carried the worm with them and aided the propagation of the worm.[779]

The Morris worm graphically demonstrated to the computer science and information networking community the real dangers of the networked system's vulnerabilities. As a result, efforts began to systematically record incidents that compromised the network's security and to search for solutions to the vulnerabilities that provided the means for compromise. DARPA formed the original Computer Emergency Response Team (CERT) at Carnegie Mellon University to "repair security lapses that exist in the current UNIX software" and to "educate users about what they can do to prevent security lapses."[780] Since this initial expert center in 1988/89, the number of centers devoted to recording security lapses of the network, correcting network vulnerabilities, and promoting better security practices has proliferated tremendously.

[778] Markoff, "The Computer Jam – How It Came About."

[779] United States Department of Defense, Report of the DSB Task Force on Information Warfare (Defense), Section 3 – "Observations."

[780] Brian M. Clapper, "Computer Emergency Response Team (CERT)," The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 8, no. 14 (January 24, 1989), http://catless.ncl.ac.uk/Risks/8.14.html.

Since the Morris worm, DoS attacks, like everything else connected with the information infrastructure system, have become progressively more sophisticated. Individuals or organizations intent on causing the system's users inconvenience or damage have evolved the deployment, use, and impact of DoS tools (the means by which attackers initiate and propagate the DoS attack). As previously mentioned, deployment of these tools has become increasingly automated self-propagating agents,[781] employing blind targeting in general, and/or selective targeting of Windows-based system and routers. These newly employed techniques increase the ability of potential attackers to easily deploy large DDoS attack networks.[782]

Of particular concern is an increase in intruder compromise and use of routers for DDoS attacks, particularly those that interconnect the networks comprising the Internet. Compromise of routers is not only troublesome from potential DoS attacks, but provides an intruder the same opportunities for more conventional intruder mischief or maliciousness as Kevin Poulson's telephone system switch since routers are essentially nothing more that complex switches. Intruders apparently

- recognize the importance of routers in the network scheme,
- are using them "as platforms for scanning activity, proxy points for obfuscating connections to IRC networks, and launch points for packet flooding DoS attacks," and

[781] Automation incorporates the entire range of deployment:

- scanning to identify vulnerabilities in victims' systems,
- attempted exploitation of identified vulnerable hosts,
- agent propagation both singularly or multiply (Houle and Weaver, 10).

Indications are that each of the above steps of deployment are now being performed in "batch" mode against many machines in one "session;" essentially automation of automation (Fithen).

[782] Houle and Weaver, 10.

- "are discussing router protocol attacks in intruder circles."[783]

Targeting of the interconnecting routers is extremely troublesome and problematic since they represent the most highly connected vital nodes of the scale-free network configured information infrastructure system with its previously discussed structural vulnerabilities. Given the structural and operational significance of routers in general and the interconnecting routers specifically, for some inexplicable reason they apparently are "often less protected by security policy and monitoring technology than computer systems" thereby enabling intruders greater opportunity for undetected activity. Security of routers is so lax that "intruders reportedly used vendor-supplied default passwords on poorly configured and deployed routers to gain unauthorized access to and control of routers." [784]

To make matters even worse, there is a "shrinking time-to-exploit" between vulnerability discovery and widespread exploitation, employment of anti-forensic tools in the design of intruder tools,[785] employment of encryption technology into the communications channels to conceal the DDoS attack,[786] and use of Internet Relay Chat (IRC) protocols and networks to make identification of DDoS networks more difficult[787].

[783] Houle and Weaver 14 and Carnegie Mellon University, Results of the Distributed-Systems Intruder Tools Workshop, 1-2.

There is a somewhat organized development effort in the intruder community that takes an open-source approach to development with a large, reusable code base. As a result, intruder tools become increasingly more sophisticated, user friendly, and widely available. Publicly available documents exist that even provide novice intruders with basic advice and commands to execute after comprising a router to modify a router's configuration (Houle and Weaver, 14 and Carnegie Mellon University Results of the Distributed-Systems Intruder Tools Workshop, 1, 3).

[784] Houle and Weaver, 14.

[785] Houle and Weaver, 14-15.

[786] Encryption tools began with the employment of Stacheldraht tool in August 1999 (Houle and Weaver, 4).

[787] Use of IRC networks allows the potential attacker to "get lost" in the high volume of traffic using this service and provides a standard service port in legitimate use to deploy (D)DoS tools in a relatively benign environment since little security (e.g., access controls) is employed in IRC services due to their immense popularity with end-users (Houle and Weaver, 15-16).

This evolution of sophistication began during the summer of 1999. The first distributed denial of service tools (trinoo and Tribe Flood Network) were discovered by researchers in August. Both used large networks of hosts to launch large coordinated denial of service attacks from many sources against one or more targets with the structural methodology of a distributed denial of service attack discussed earlier in the appendix.[788] Both trinoo and TFN executed a denial of service in two phases.

In the initial "mass-intrusion phase," an attacker carefully tested for and selected hosts with high bandwidth availability manually, then remotely root compromised large numbers ("in the several hundred to several thousand" ranges) of machines/systems, installed automated DDoS tools on these compromised systems, and linked the compromised machines together with a handler(s) to form attack networks as discussed earlier in this appendix. In the second "attack phase," these comprised machine agents then listened for inbound commands from the handler via custom TCP, UDP,[789] and ICMP protocols to produce UDP floods, TCP SYN floods, and ICMP echo request floods.[790]

[788] Carnegie Mellon University, "Distributed Denial of Service Tools," CERT Incident Note IN-99-07 (Last updated, January 15, 2001), CERT Coordination Center, Software Engineering Institute, Pittsburgh, PA., http://www.cert.org/incident_notes/IN-99-07.html."

Dittrich postulates that over 2000 systems worldwide were compromised by trinoo and TFN during the summer and fall of 1999 (David Dittrich, "The "Stacheldraht" Distributed Denial of Service Attack Tool," University of Washington, December 31, 1999). Investigators later determined that over 2,200 computer systems at more than 300 universities in the U.S. had unwittingly become zombies. These zombies generated so much activity across the system that the universities were denied access to legitimate activity for at least two days (M. J. Zuckerman, "Asleep at the Switch? How the Government Failed to Stop the World's Worst Internet Attack," USA Today, March 9, 2000).

[789] User Datagram Protocol - An Internet Standard protocol [R0768] that provides a datagram mode of packet-switched computer communication in an internetwork (R. Shirey, "Request for Comments: 2828," Internet Security Glossary, Network Working Group, GTE/BBN Technologies, May 2000, ftp://ftp.isi.edu/in-notes/rfc2828.txt).

[790] Houle and Weaver, 4 and Dittrich.

Both tools employed the classic DDoS methodology discussed earlier in this appendix. See Carnegie Mellon University, "Distributed Denial of Service Tools," CERT Incident Note IN-99-07, for a much greater technical discussion of both trinoo and Tribe Flood Network tools and their specific attack methodology.

As indicated earlier, those individuals and organizations perpetrating DDoS attacks continually improved their tools. Researchers quickly discovered a new tool named Stacheldraht. According to an analysis of the tool by David Dittrich of the University of Washington, it "combined features of the trinoo distributed denial of services tool with those of the original TFN and adds encryption of communication between the attacker and Stacheldraht masters to autonomously update the agents;"[791] An updated trinoo/TFN DDoS tool with encryption. It employed trinoo's handler/agent features and, at the same time, shared TFN's distributed network denial of services through "ICMP flood, SYN flood, UDP flood, and "Smurf" style attacks by exploiting buffer overrun bugs."

Similar to trinoo and TFN, Stacheldraht methods for installing the agent/handler program on a compromised system were the "same as installing any program on a compromised UNIX system, with all the standard options for concealing the programs and files." Two features of Stacheldraht not shared by trinoo and TFN were the ability to upgrade the agents on demand and symmetric key encryption between the clients and the handler(s).[792]

Another new DoS tool (TFN2K) was released on December 21, 1999,[793] and was believed to be a competitor to Stacheldraht. TFN2K was designed to work on various UNIX, UNIX-like systems, and Windows NT (an advancement over the original TFN which attacked only UNIX systems). TFN2K also included features designed specifically to make its traffic difficult to recognize and filter, to remotely execute commands, to obfuscate the true source of the traffic, to transport TFN2K traffic over

[791] Dittrich.
[792] Dittrich.
[793] Dittrich.

multiple transport protocols including UDP, TCP, and ICMP, and features to confuse attempts to locate other nodes in a TFN2K network by sending "decoy" packets. TFN2K obfuscated the true source of attacks by spoofing IP addresses. In networks that employed ingress filtering, TFN2K could forge packets that appeared to come from neighboring machines.

Like its parent Tribal Flood Network, TFN2K flooded networks by sending large amounts of data to the victim machine. Unlike TFN, TFN2K included attacks designed to crash or introduce instabilities in systems by sending malformed or invalid packets.[794] The one common element of all of these new, and improved denial of service tools, though, was a need for the attacker to compromise a part of the system first in order to gain access for installation of the denial of service tools. Of course, the compromise was accomplished by exploiting known software vulnerabilities.[795]

Then during a one-week period in early February 2000, a Canadian **teenager** (nicknamed “mafiaboy”) (emphasis added to bring attention to the age of the perpetrator) very graphically demonstrated to the entire world the inherent structural weakness of the information infrastructure system’s scale-free network configuration. He deliberately[796] targeted servers (highly connected nodes) of CNN.com, Dell, Yahoo!, Ebay,

[794] Carnegie Mellon University, “Denial-of-Service Tools,” CERT® Advisory CA-1999-17 (Last Updated: March 3, 2000), CERT Coordination Center, Software Engineering Institute, Pittsburgh, PA., http://www.cert.org/advisories/CA-1999-17.html.

[795] Carnegie Mellon University, “Denial-of-Service Development,” CERT® Advisory CA-2000-01, CERT Coordination Center, Software Engineering Institute, Pittsburgh, PA., January 2, 2000, http://www.cert.org/advisories/CA-2000-01.html.

[796] Mafiaboy’s intentions may not have been malicious, but they surely were deliberate. “The FBI had obtained chat room logs showing that Mafiaboy asked others what sites he should take down — before the sites were attacked. Mafiaboy was saying ‘What should I hit next? What should I hit next?’ and people on the channel were suggesting sites, and Mafiaboy was saying, ‘OK, CNN.’ And shortly thereafter the people on the channel would be talking about CNN going down. If you look at the time stamps on the logs, they also coincide with CNN going down. The log files show similar discussions prior to the Feb. 9 attacks on E*TRADE and several other smaller sites” (Jonathan Dube and Brian Ross, “‘Mafiaboy’ Arrested,” ABCNews.com, April 19, 2000, http://abcnews.go.com/sections/tech/DailyNews/webattacks000419.html).

Amazon.com, Excite, and Etrade with distributed denial of service attacks. The teen compromised a University of California – Santa Barbara computer and instructed it to send large amounts of traffic to targeted systems. The resultant flood of data from innumerable intermediate zombie systems resulted in the global Internet being slowed by 20 % and the targeted commercial services being slowed or disrupted for hours costing them an estimated $1.7 billion in damages. The attacks shook the e-commerce industry because of the ease with which major sites were made inaccessible.[797]

The next significant advancement in the evolution of DDoS methodology first began to appear on May 4th, 2000. A young Filipino student released the LoveLetter virus (actually a worm).[798] Although not the first denial of service tool that required social interaction[799] to propagate or the first macro virus,[800] Loveletter was particularly

[797]Peter G. Neumann, "Distributed Denial-of-Service Attacks," The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 20, no. 87 (April 28, 2000), http: //catless.ncl.ac.uk/Risks/20.87.html; "Canadian Teen Held in Web Attacks," NewsScan, April 19, 2000, The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 20, no. 87 (April 28, 2000), http://catless.ncl.ac.uk/Risks/20.87.html; "Canadian Juvenile Charged in Connection with February 'Denial of Service' Attacks," Technology: Computing, CNN.com, April 18, 2000, http://www.cnn.com/2000/TECH/computing/04/18/hacker.arrest.01/index.html; "'Mafiaboy' Hacker Jailed," Science/Tech, BBC News, September 13, 2001, http://news.bbc.co.uk/hi/english/sci/tech/newsid_1541000/1541252.stm; and Zuckerman.

[798]LoveLetter is an Internet worm programmed in VBScript (a cut-down version of Visual Basic) and requires the Windows Scripting Host installed in order to run ("PC Patrol," Viruzlist, http://www.tonyaustin.com/viruzlist/loveletter.html).

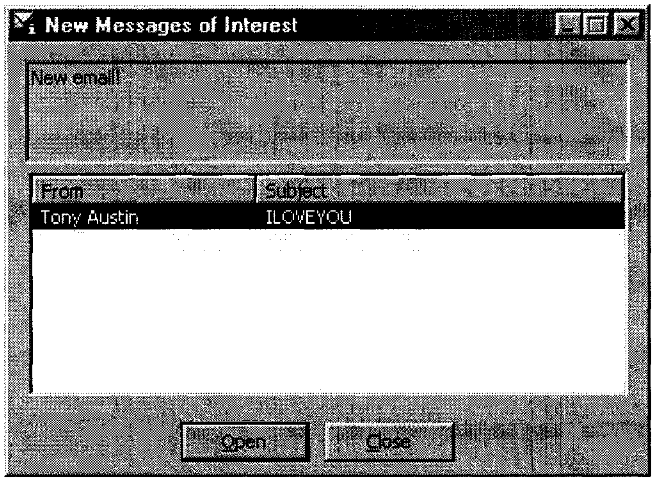
[799]Although humans (users and operators/providers) are not components of my defined research information infrastructure system (see Chapter 2. Information Infrastructure System for defined research system and rationale), I include the LoveLetter DoS incident as an example of the different methodologies DoS attackers use to attack the information infrastructure system.

The difference between socially engineered e-mail and e-mail attachment DoS attacks and more technical DoS and DDoS attacks are in the means of installation of the attack program only. The E-mail attacks are dependent upon human interaction for installation while the technical attacks require no human intervention. The programs' action accomplishes the same effect: such massive transmission of data that a host's computer/system or some other integral part of the information infrastructure system is overwhelmed and part of the system's operation is disrupted.

The Melissa virus a year earlier used similar social interactive methodology (an e-mail message that had to be opened by the recipient) to propagate eventually costing information infrastructure system users an estimated $80 million (Vibert).

BubbleBoy, another virus also embedded within an email message, was even more insidious than Melissa and Loveletter. Its virus was in the body of the e-mail message in HTML format so therefore did not require an attachment to be opened to infect the host machine. In MS Outlook, BubbleBoy did require significant because of the speed[801] and variety of methods with which it spread, the number of machines it affected worldwide, and the damage it eventually caused (an estimated $6-10 billion, primarily in lost productivity and cleanup efforts).[802]

The victim would receive an e-mail like the one shown below.



New Messages of Interest

New email!

From	Subject
Tony Austin	ILOVEYOU

that you "open" the email. However, in MS Outlook Express, the worm would activate if "Preview Pane" is used; in effect, infecting your machine without "opening" the e-mail. Once the worm had infected a machine, it was programmed to

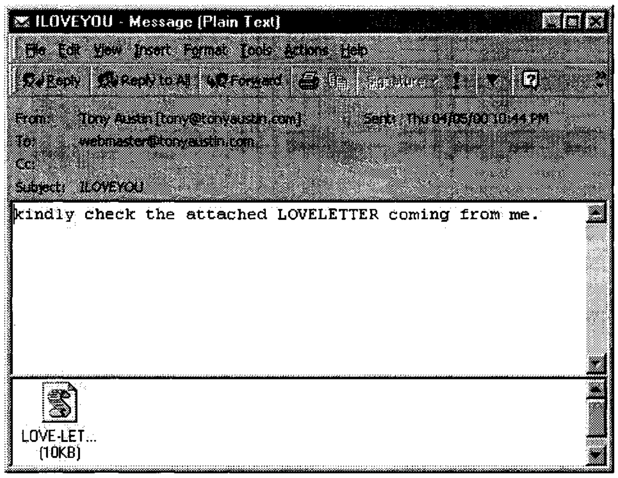
- change the registered owner via the registry to "BubbleBoy,"
- change the registered organization to "Vandelay Industries,"
- send itself embedded in an email message to every contact in the address book of Microsoft Outlook, and
- set the registry key to indicate that the email distribution has occurred to prevent itself from continuously re-sending the emails ("PC Patrol," Viruzlist, November 9, 1999, http://www.tonyaustin.com/viruzlist/loveletter.html).

[800] According to the Department of Energy's Computer Incident Advisory Capability (CIAC), macro viruses for Microsoft Word appeared as early as 1995, with over 1000 variants for Word and other products by 1998. See http://www.ciac.org/ciac/bulletins/i-023.shtml for more information (Carnegie Mellon University, Frequently Asked Questions About the Melissa Virus (Last Update, May 24, 1999), CERT Coordination Center, Software Engineering Institute, Pittsburgh, PA., http://www.cert.org/tech_tips/Melissa_FAQ.html).

[801] By May 8th, the CERT Coordination Center had received reports from more than 650 individual sites indicating more than 500,000 individual systems were affected (Carnegie Mellon University, CERT Advisory CA-2000-04 (Last revised May 9, 2000), CERT Coordination Center, Software Engineering Institute, Pittsburgh, PA., http://www.cert.org/advisories/CA-2000-04.html and Carnegie Mellon University, CERT Summary CS-2000-02 (Last revised May 9, 2000), CERT Coordination Center, Software Engineering Institute, Pittsburgh, PA., May 31, 2000, http://www.cert.org/summaries/CS-2000-02.html).

[802] Clean up was particularly difficult since the worm overwrote, instead of merely deleting, the files it infected (Carnegie Mellon University, "Love Letter Worm").

If the message was opened, the recipient was greeted with a message (similar to the one shown below) that contained an attachment. If the attachment was opened, the LoveLetter virus distributed itself to everyone in the recipient's address book (if using Outlook) and everyone in any Internet Chat Relay (IRC) channels the recipient visits using mIRC.[803] Once LoveLetter had infected a machine, it searched all drives mapped to the infected computer, including networked drives, to replace files with set extensions (vbs, vbe, js, jse, css, wsh, sct, hta, jpg, jpeg, mp3, mp2) on these drives with a copy of the LoveLetter virus. The virus would then send copies of itself to all of the addresses it was successful in identifying resulting in both dispatching and receiving e-mail servers being overwhelmed with excessive traffic (including the web servers of numerous anti-virus firms). While sending an e-mail, the worm updated the last entry each time thereby increasing the size of the registry. Or, users could be infected from their Internet chat rooms or from any files shared with another user already infected by the virus.


ILOVEYOU - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
Signature
LOVE-LET...
(10KB)

From: Tony Austin [tony@tonyaustin.com]
Sent: Thu 04/05/00 10:44 PM
To: webmaster@tonyaustin.com
Cc:
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

[803] The speed with which LoveLetter spread can partly be attributed to the recipient receiving the e-mail containing the worm from a known familiar address along with the inclusion of the three other means of propagation.

Finally, the LoveLetter virus would attempt to download a password-cracking program into a file called WIN-BUGSFIX.exe from the Internet. This program would try to determine as many passwords as possible from the recipient's machine and network before sending them to the LoveLetter virus' author in the Philippines via email.[804] As insidious, by the end of May at least 30 different variants [including one entitled “Mother's Day” (making it even easier to socially engineer a recipient to open since Mother's Day occurs during May)] of the LoveLetter virus had appeared, each requiring a new and different solution to correct the new and different vulnerability exploited.

DoS and DDoS attacks since trinoo, Tribal Flood Network, LoveLetter have essentially demonstrated evolutionary improvements in technical methodology and social engineering these three attack tools employed.

- the Trinity DDoS tool (August 2000) improved the attack methodology of using the IRC as the core DDoS network control infrastructure on compromised UNIX systems;
- November 2000 marked a shift from UNIX to Windows as the host platform for DDoS agents as multiple Windows-based agents were actively deployed;
- Ramen worm (January 2001) improved intruder tool distribution propagation;
- the cheese worm and w0rmkit (May 2001) focused on using backdoors from previous DoS attacks;
- the sadmill/IIS worm (May 2001) propagated using two separate vulnerabilities on two separate operating system platforms simultaneously;

[804] “PC Patrol,” Viruzlist, http://www.tonyaustin.com/viruzlist/loveletter.html; Carnegie Mellon University. “CERT Coordination Center Fights Love Letter Virus,” CERT Coordination Center, Software Engineering Institute, Pittsburgh, PA., May 4, 2000, http://www.cert.org/about/loveletter5-2000.html; and Vibert.

- the Leaves worm (July 2001) was able to update and change its functionality during propagation;
- Code Red (July 2001) could launch a TCP SYN DoS attack against a specific target and could also cause isolated DoS conditions from high scanning and propagation rates;
- Nimda combined attacks from e-mail attachments, SMB networking, backdoors from previous attacks, exploitation of an Internet Explorer vulnerability, and exploitation of an IIS vulnerability; and
- the VBS/OnTheFly (Anna Kournikova), W32/Sircam and Nimda continued to vividly demonstrate the effectiveness of social engineering to install and propagate DoS attacks.[805]

B.4. Conclusion.

As the above discussion demonstrates, denial of service incidents are not new to digital data systems. What has changed is the sophistication of their methodology[806] and the reason for their occurrence: from inadvertent software defects or human error to deliberate and/or malicious intent. What has not changed is their potential to disrupt the system's operations and the difficulty in preventing such incidents. Today, a user's system may be subject at any time to distributed denial of service attacks that are

[805] Houle and Weaver, 4-9.

[806] "Evolution in intruder (DoS) tools is a long-standing trend and it will continue"(Houle and Weaver, 20). "Intruders have harnessed the power of the Internet itself, building automated tools to coordinate large-scale attacks involving hundreds of hosts aimed at Internet sites. These tools are well documented and freely available on the Internet. Members of the intruder community share programs and improve on each other's work" [Larry Roger, "Cybersleuthing: Means, Motive, and Opportunity," Infosec Outlook 1, no. 3 (June 2000)].

extremely difficult to trace or defend against and for which only partial solutions are available.[807]

Also, what has not changed is the risk of (and the ability of an intruder/attacker to exploit) the information infrastructure's earlier identified vulnerabilities:

- Software -
  - •• with the exception of human engineering,[808] DoS tools are almost exclusively installed by taking advantage of known software vulnerabilities;[809]
- Open network architecture -
  - •• many network configurations inadequately implement well known "best practices" and/or facilitate intruders' obfuscation techniques to conceal their identity;[810]
- Interconnectivity -
  - •• facilitates both initial attack and propagation [coordinated attacks have occurred across national boundaries (e.g., LoveLetter)];
- Systemic properties -
  - •• because a system is a unitary functional unit (and the information infrastructure is a system as established earlier in the body of Chapter3. Information Infrastructure System Vulnerabilities, Risks, and Threats), its operation is dependent upon the cumulative reliable operation of every

[807] Houle and Weaver, 20.

[808] Although outside of the defined information infrastructure system's defined boundaries, the LoveLetter, VBS/OnTheFly (Anna Kournikova), W32/Sircam, and Nimda viruses/worms demonstrated targeting and exploitation of users' and operators'/maintainers' human/social tendencies and weaknesses by DoS attackers.

[809] "A nearly inexhaustible supply of computers with well-known software vulnerabilities susceptible to compromise and DoS tools installation exist today" (Fithen).

[810] Fithen.

part. When some factor interferes with one part's operation, the entire system suffers functional degradation or disruption (loss of the information assurance objective of availability). Depending upon the specific part(s) (e.g., server, router, etc.) affected by a DoS attack, a user, LII, NII, or even the GII[811] could be disrupted or degraded;

- Scale-free network topography -

  •• the information infrastructure system 's behavior during a DDoS attack mimics the degradation of a scale-free network in Albert, Jeong, and Barabasi's experiments discussed earlier in Chapter3. Information Infrastructure System Vulnerabilities, Risks, And Threats.

Once denial of service attackers learned how to use the distributed system's properties against itself (see Figure B-1. Typical Distributed-System Attack Methodology), such attacks became more insidious. Attackers were able to randomly (as is the case with most DDoS incidents) or deliberately (see Mafiaboy discussed earlier) affect specific parts (generally users/organizations) of the system. Since the distributed system decentralizes connection to the information infrastructure system, the connecting software (generally a server) is not required to have the capacity of a centralized connection. Attackers are now able to generate enough data transmissions to overwhelm individual connections to the system. These overwhelmed connections are not able to transmit or receive data over the greater infrastructure system. The result may be reduced or unavailable network connectivity for extended periods of time, possibly days or even weeks, depending upon the number of sites attacking and the number of possible attack

[811] To date, only users and LIIs (the organizations and systems affected by Mafiaboy can be considered both users and LIIs) have been disrupted to a degree that they become inoperable by a DoS attack, but, conceptually, one or more NIIs or the GII could be disrupted.

networks that are activated in parallel or sequentially. With the targeting of the most highly connected nodes (e.g., routers which effectively serve as switches for the information infrastructure system), greater portions (larger LIIs or even an NII) of the system can be degraded or disrupted.[812]

The CERT-sponsored Distributed-Systems Intruder Tools Workshop of November 1999 's conclusion that "there is essentially nothing a site can do with currently available technology to prevent becoming a victim" of a denial of service attack still obtains.[813] DDoS tools and attacks demonstrate that a network that optimizes its technology for speed and reliability at the expense of security may experience neither speed nor reliability, as intruders abuse the network or deny its services. DDoS attackers use the network system's very properties to facilitate and exacerbate an exploitation's effects. An attacker uses the (in)security of individual sites and the ability to implant remotely the denial of service tools and, subsequently, to control and direct multiple systems worldwide.

In today's DoS attacks, the attack methodology is so complex there is no single-point solution or "silver bullet" for resolution and restoration of systems. Although an organization may be able to "harden" its own systems to help prevent having its systems used as part of a distributed attack, there is essentially nothing a site can do with currently available technology to prevent becoming a victim of, for example, a coordinated

[812] See Figure 2.3 - Representative Complex Information System, for graphic representation of some of the information infrastructure system's highly connected nodes and how deletion of these nodes could adversely affect the operation of the system as a system.
[813] Carnegie Mellon University, Results of the Distributed-Systems Intruder Tools Workshop and Zuckerman.

network flood.[814] The same properties that facilitate ease and efficiency, particularly in widely used products such as Microsoft, are often exploited by virus/worm authors.

The traditional approach employed for dealing with computer viruses is reactive, expensive, and does not solve the virus problem, but rather focuses on the symptoms. The existing response model for viruses is based upon identifying each new virus and variant after it appears and has an impact and remedying the vulnerability that allowed that particular incident to happen. Such a model requires that:

- a virus can be diagnosed and a cure developed quickly;
- the cure can be sent to the infected parties as soon as possible;
- the infrastructure for delivering the cure functions properly; and
- the customer is able to distribute the cure internally in an efficient and timely manner.

This reactive approach provides remedies, but only after a virus has had the opportunity to cause damage.[815]

Preventing DDoS attacks will require a long-term research and development effort to initially define and then implement effective solutions.[816] Peter Neumann echoes Fithen's call for research and development to find more and better solutions to the denial of service problem.

> "We also need network protocols that are less vulnerable to attack and that more effectively accommodate emerging applications (interactive and noninteractive, symmetric and asymmetric, broadcast and point-to-point, etc.) – for example, blocking bogus IP addresses; ...firewalls and routers that are more defensive; cryptographic authentication among trustworthy sites; systems with fewer flaws and fewer risky features; monitoring that enables early warnings and automated reconfiguration; constraints on Internet service

[814] Fithen.
[815] Vibert.
[816] Fithen.

> providers to isolate bad traffic; systems and networks that can be more easily administrated; and much greater collaboration among different system administrations."[817]

Neumann proposes technical, managerial, and educational improvements. However, since software vulnerabilities are most culpable for DDoS attack tools installation, the long-term effort should focus primarily on producing error-free software while, at the same time, on identifying and correcting errors in legacy software. Since intruders also use software vulnerabilities to gain access to the information infrastructure system and its various components, such an effort will have the synergistic effect of making the entire system more secure by also removing the vulnerabilities that allow them to threaten the system's data.

A second line of research should search for solutions to the network's identified structural vulnerabilities. Methods should be developed to alter or mediate the system's scale-free network architecture to nature's more robust exponential choice. By diffusing or adding redundancy to some or all of the current network's highly connected nodes, the inherent weakness of the system targeted by DoS attacks will be moderated or corrected. Without both foci, all other efforts will provide only short-term and transitory security from denial of service attacks.

[817] Neumann, "Denial of Service Attacks."

APPENDIX C

GLOSSARY

CIAO - Critical Infrastructure Assurance Office

CIOC - Chief Information Officers Council

CSSPAB - Computer System Security and Privacy Advisory Board

DOC - Department of Commerce

FCC - Federal Communications Commission

HCS WG - High Confidence Systems Working Group

IITF - Information Infrastructure Task Force

INTER-AGENCY WG ON CIP R&D - Interagency Working Group on Critical Infrastructure Protection Research and Development

ISAC - Information Sharing and Analysis Center

ISPAC - Information Security Policy Advisory Council

LSN WG/NGI - Large Scale Networking Working Group/Next Generation Internet

NCSIP&C-T - National Coordinator for Security, Information Protection and Counter-Terrorism

NEC - National Economic Council

NIAC - National Information Assurance Council

NIPC - National Infrastructure Protection Center

NIST - National Institute of Standards and Technology

NRIC - Network Reliability and Interoperability Council

NCS - National Communications System

NSC - National Security Council

NSTAC - National Security Telecommunications Advisory Committee

NSTC - National Science and Technology Council

NSTISSC - National Security Telecommunications and Information Systems Security Committee

NTIA - National Telecommunications and Information Administration

OMB - Office of Management and Budget

OPM - Office of Personnel Management

OSTP - Office of Science and Technology Policy's

PACHPCCITNGI - President's Advisory Committee on High Performance Computing and Communications, Information Technology, and the Next Generation Internet

PCCIP - President's Commission on Critical Infrastructure Protection

PCAST - President's Committee of Advisors on Science and Technology Policy

PITAC - President's Information Technology Advisory Committee

USAC (NII) - United States Advisory Council on the NII

USSPB - United States Security Policy Board

APPENDIX D

ORGANIZATIONAL RESPONSIBILITIES AND AUTHORITIES

1. **Assistant to the President for National Security Affairs (National Security Advisor).**

The "focal point" for information assurance (after a March 1995 NSTAC request for a national central official) (United States Congress, The National Security Act of 1947 (PL 235 – 61, Stat. 496; 50 U.S.C. 402) as amended, 80th Congress, 1st sess., July 26, 1947).

2. **Chief Information Officers Council (CIOC).**

An intergovernmental forum of chief information officers chaired by the Deputy Director for Management of OMB (CIO) to "improve the design, modernization, use, sharing, and performance of information resources" (United States White House, Executive Order (EO) 13011, Federal Information Technology, Washington, D.C., July 16, 1996 and United States Congress; Clinger-Cohen Act of 1996 (also known as Information Technology Management Reform Act of 1996 (Public Law 104-106, Division E), United States Code, Title 40, Section 1401), 104th Congress, 2nd sess., January 3, 1996).

3. **Computer System Security and Privacy Advisory Board (CSSPAB).**

Advises the Secretary of Commerce and Director of NIST on computer security and privacy issues pertaining to sensitive unclassified federal computer systems (**only**) by "identifying emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy" (United States Congress, Computer Security Act of 1987 (Public Law 100-235), Section 3, 100th Congress, 2nd sess., January 8, 1988).

4. Counterintelligence Policy Board (CIB).

Considers, develops and recommends for implementation to the Assistant to the President for National Security Affairs policy and planning directives for U.S. counterintelligence. It is the principal mechanism for reviewing and proposing to the NSC staff legislative initiatives and executive orders pertaining to U.S. counterintelligence. The Board will coordinate the development of interagency agreements and resolve conflicts that may arise over the terms and implementation of these agreements (United States White House, Presidential Decision Directive (PDD) 24, U.S. Counterintelligence Effectiveness, The White House, Washington, D.C., May 3, 1994 and United States Counterintelligence Policy Board, Agencies and Functions of the Federal Government Established, Abolished, Continued, Modified, Transferred, or Renamed by Legislative or Executive Action During Calendar Year 1994 (within the executive branch of the Federal Government), http://www.nara.gov/fedreg/agency94.html.

5. Critical Infrastructure Assurance Office (CIAO) (formerly National Plan Coordination (NPC) staff)

Provide support to National Coordinator's work with government agencies and private sectors in integrating the various sector plans into a National Infrastructure Assurance Plan for critical infrastructure, to include the information infrastructure system. The office will coordinate analyses of the U.S. government's own dependencies on critical infrastructures, help coordinate a national education and awareness program, and develop and coordinate legislative and public affairs (United States White House, Presidential Decision Directive (PDD) 63, Protecting America's Critical Infrastructure, Washington, D.C., May 22, 1998 and United States Department of Justice, CIAO Homepage, Critical Infrastructure Assurance Office, http://www.info-sec.com/ciao).

6. Critical Infrastructure Coordination Group (CICG).

Coordination group created to implement PDD 63 and to sponsor an expert review process for every federal department's and agency's plan for protecting its own critical infrastructure, including, but not limited to its cyber-based systems (United States White House, Presidential Decision Directive (PDD) 63, Protecting America's Critical Infrastructure, Washington, D.C., May 22, 1998).

7. Federal Communication Commission (FCC).

The Commission has the mandate to "regulate, license and monitor the operations of communications services (to include digital and analogue applications and transmission facilities) to insure reliable and competitive nationwide and international communications." FCC functions include ensuring that communications capabilities are provided for the promotion of life and property and for the national defense (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C. July 4, 1996).

8. Information Infrastructure Task Force (IITF).

Formed by the Clinton administration in 1993 to "articulate and implement the administration's vision for the National Information Infrastructure (NII). Its representatives from the different federal agencies will "develop comprehensive technology, telecommunications, and information policies"... that best meet the needs of the agencies and the nation, specifically:

- NIST's efforts to identify Federal security products, techniques, and practices that will be useful in the NII;
- NIST's efforts to coordinate private Forum of Incident Response and Security Teams (FIRST) with federal government efforts to ensure a "911" capability for the NII;
- National Communications System's (NCS) and the National Security Telecommunications Advisory Committee's (NSTAC) efforts to ensure that National Security/Emergency Preparedness needs are accommodated in the NII;
- the National Security Telecommunications and Information Systems Security Committee's efforts to identify useful security tools and techniques in the national security community that may be applicable to the NII;
- the High Performance Computing and Communications (HPCC) Program to assure development and testing of new technologies for computer security suitable for the high performance environment; and
- the Federal Network Council's (FNC) efforts to explore specific issues relating to security of the Internet (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C. July 4, 1996, A155-161 and United States Information Infrastructure Task Force (IITF), Information Infrastructure Task Force (IITF) Homepage, http://www. iitf.nist.gov/committee.html).

9. **Information Security Oversight Office.**

Responsible for administering the "uniform system for classifying, safeguarding, and declassifying national security information"... defined... "as knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that pertains to the national defense or foreign relations of the United States" (United States White House, Executive Order (EO) 12356, National Security Information, Washington, D.C., April 2, 1982 and amended by United States White House, Executive Order (EO) 12958, Classified National Security Information, Washington, D.C., April 17, 1995).

10. **Information Security Policy Advisory Council (ISPAC).**

A Presidentially appointed council that advises the President, National Security Advisor, and Director of OMB through the Director of the Information Security Oversight Office on classifying, safeguarding, and declassifying national security information (United States White House, Executive Order (EO) 12958, Classified National Security Information, Washington, D.C., April 17, 1995).

11. **Information Sharing and Analysis Center (ISAC).**

Serves as a mechanism for gathering, analyzing, appropriately sanitizing, and disseminating private sector information to both industry and the NIP (United States White House, Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, White Paper, Washington, D.C., May 1998, http://www.info-sec.com/ciao).

12. **Joint Security Commission (JSC).**

Founded in 1993 by the Secretary of Defense and Director of Central Intelligence "to review the security practices and procedures under their authorities. The Commission concluded that the problems of fragmentation and inconsistency in security policy development, implementation, and oversight must be resolved in order to make meaningful improvements in the overall effectiveness of U.S. government security" (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C. July 4, 1996, A175).

13. **The National Communications System (NSC).**

A confederation of 23 federal departments' and agencies' telecommunications assets governed by the NSC's Committee of Principals with a mandate to manage national security and emergency preparedness capabilities of those assets (United States White House, Executive Order (EO) 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, Washington, D.C., April 3, 1984; United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C. July 4, 1996, A163; and United States White House, National Security Decision Directive (NSDD) 97, National Security Telecommunications Policy, Washington, D.C., June 13, 1984).

14. **National Coordinator for Security, Infrastructure Protection and Counter-Terrorism (NCS,IP,C-T).**

Staff member of NSC that is charged to ensure interagency coordination for policy development and implementation and will review crisis activities concerning infrastructure events with significant foreign involvement (United States White House, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, White Paper, Washington, D.C., May 1998, http://www.info-sec.com/ciao).

15. **National Information Infrastructure (NII) Security Issues Forum (NIISIF).**

Coordinates security (the confidentiality, availability, and integrity of information and of the systems carrying the information) efforts across the committees and Working Groups of the IITF (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C. July 4, 1996, A155-161 and United States Information Infrastructure Task Force (IITF), Information Infrastructure Task Force (IITF) Homepage, http://www. iitf.nist.gov/committee.html).

16. **National Information Protection Center (NPIC).**

Provides timely warning of intentional threats and law enforcement investigation and response and, in appropriate cases, analyses and reports to relevant federal, state and local agencies; to owners and operators of critical infrastructures; and to any private sector information sharing and analysis center (United States White House, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, White Paper, Washington, D.C., May 1998, http://www.info-sec.com/ciao).

17. **National Infrastructure Assurance Council (NIAC).**

The NIAC will "enhance the partnership of the public and private sectors in protecting our critical infrastructure, propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems, monitor the development of Private Sector Information Sharing and Analysis Centers (PSISACs), and provide recommendations to the National Coordinator and National Economic Council on how these organizations can best foster improved cooperation among the PSISACs, the National Information Protection Center (NIPC), and other Federal Government entities" (United States White House, Executive Order (EO) 13130, National Infrastructure Assurance Council, Washington, D.C., July 14, 1999).

18. **National Institute of Standards and Technology (NIST).**

NIST develops government-wide computer system security standards and guidelines and security training programs for the protection of sensitive unclassified information maintained in Federal government computer systems. NIST's primary responsibility is to work with industry to develop measurements and standards to improve product quality and ensure product reliability (United States Congress, Computer Security Act of 1987 (Public Law 100-235), 100th Congress, 2nd sess., January 8, 1988 and United States Congress, Clinger-Cohen Act of 1996 (also known as Information Technology Management Reform Act of 1996) (Public Law 104-106, Division E), United States Code, Title 40, Section 1401, 104th Congress, 2nd sess., January 3, 1996).

19. **National Science and Technology Council (NSTC).**

The "principle means for the President to coordinate science, space, and technology policies across the Federal Government."

In addition to other responsibilities, President Clinton has directed the NSTC to:

- Coordinate the science and technology policy making and implementation process across Federal agencies;

- Ensure that science and technology policy decision are consistent with the President's stated goals; and
- Ensure that science and technology issues are considered in the development and implementation of Federal policies and programs (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A168).

20. **National Security Agency (NSA).**

Responsible for government classified information systems-based data, primarily through protection against exploitation through interception, unauthorized access, or related technical intelligence threats (United States Congress, Computer Security Act of 1987 (Public Law 100-235), 100th Congress, 2nd sess., January 8, 1988 and United States Congress, Senate. Select Committee on Governmental Operations with Respect to Intelligence Activities, Foreign and Military Intelligence — Book I, 94th Congress, 2nd sess., 26 April 1976, 325-335).

21. **National Security Council (NSC).**

"Provide policy direction for the exercise of the war power functions of the President under the National Communications Act of 1934...Advise and assist the President in coordinating the development of policy, plans, programs, and standards within the Federal government for the use of the Nation's telecommunications resources... during those crises or emergencies in which the exercise of the President's war power function is not required or permitted by law; and provide policy direction for the exercise of the President's non-wartime emergency telecommunications functions...; coordinate the development of policy, ... for the mobilization and use of the Nation's commercial, government, and privately owned telecommunications resources, in order to meet national security and emergency preparedness requirements; and provide policy oversight and direction of the activities of the NCS...for the execution of the responsibilities assigned to the Federal departments and agencies" (United States White House, Executive Order (EO) 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, Washington, D.C., April 3, 1984).

"Duty of the National Security Council (NSC) to consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security and to make recommendations to the President in connection therewith (United States Congress, The National Security Act of 1947 (Public Law 235 – 61, Stat. 496, 50 U.S.C. 402) as amended, 80th Congress, 1st sess., July 26, 1947 and United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A91-92).

The Defense Policy and Arms Control Office has the lead for information operations and assurance (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A91-92).

22. National Security Telecommunications Advisory Committee (NSTAC)

"Provide industry perspective advice and information to the President and the Executive Branch through OSTP, OMB, and the NSC with respect to national security the exercise of the President's non-wartime emergency telecommunications functions...; coordinate the development of policy, ... for the mobilization and use of the Nation's commercial, government, and privately owned telecommunications resources, in order to meet national security and emergency preparedness requirements; and provide policy oversight and direction of the activities of the NCS...for the execution of the responsibilities assigned to the Federal departments and agencies" (United States White House, Executive Order (EO) 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, Washington, D.C., April 3, 1984).

"Duty of the National Security Council (NSC) to consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security and to make recommendations to the President in connection therewith (United States Congress, The National Security Act of 1947 (Public Law 235 – 61, Stat. 496, 50 U.S.C. 402) as amended, 80th Congress, 1st sess., July 26, 1947 and United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A91-92).

The Defense Policy and Arms Control Office has the lead for information operations and assurance (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A91-92).

22. National Security Telecommunications Advisory Committee (NSTAC)

"Provide industry perspective advice and information to the President and the Executive Branch through OSTP, OMB, and the NSC with respect to national security telecommunications policy and enhancements to NS/EP telecommunications." The NSTAC has an Information Assurance Task Force, an NII Task Force, and a Network Security Group (United States National Security Council (NSC), NSC Homepage, http://www.nsc.gov; United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A177; and United States White House, Executive Order (EO) 12382, President's National Security Telecommunications Advisory Committee, Washington, D.C., September 13, 1982).

23. **National Security Telecommunications and Information Systems Security Committee (NSTISSC).**

"Considers technical matters and develops operating policies, guidelines, instructions, and directives, as necessary, to implement the provisions of National Security Directive 42" (United States White House, National Security Directive (NSD) 42, National Policy for Security of National Security Telecommunications and Information Systems, Washington, D.C., July 5, 1990; United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A171; and United States National Security Telecommunications and Information Systems Security Committee (NSTISSC), Homepage, http://www.nstissc.gov/html/overview.html).

24. **National Telecommunications and Information Administration (NTIA).**

Organizationally a part of the Department of Commerce, the NTIA serves as "the principal executive branch advisor to the President on telecommunications and information policy." Designated by the Department of Commerce as the lead agency for physical and cyber protection of the Information and Communications (I&C) sector of the PD 63, Critical Infrastructure Protection, organization (United States National Telecommunications and Information Administration, Homepage, www.nce.gov/ncs/html/ntia.html; United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A112; and Critical Infrastructure Assurance: Information and Communications, Homepage, February 8, 2003, http://www.ntia.doc.gov/osmhome/cip).

25. **Network Reliability and Interoperability Council (NRIC)** (Previously known as the Network Reliability Council).

a federal advisory committee charter by the Federal Communications Commission (FCC) in 1992 to advise on the reliability of the public switch network after several service outages in 1990 and 1991 affected large numbers of users and the air traffic control system. The Council published "Network Reliability: A Report to the Nation" in 1993. In 1994, the FCC requested the Council to evaluate network services and evaluate potential risks from new interconnection arrangements (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A201-202; United States Code of Federal Regulations, Title 47: Telecommunications, Part 63: Extension of Lines, New Lines, and Discontinuous, Reduction, Outage, and Impairment of Service by Common Carriers and Grants of Recognized Private Operating Agency Status, Section 100: Notification of Service Outage, October 1, 2001; and United States Congress, Telecommunications Act of 1996, (Public Law No. 104-104), United States Code, Title 110, Section 56, 104th Congress, 2nd sess., January 3, 1996).

26. **Office of Management and Budget (OMB).**

Provides oversight of Executive Branch compliance of the Computer Security Act of 1987 through the Paperwork Reduction Act of 1995 giving the Director responsibility for information security policies, principals, standards, guidelines, oversight, and compliance. The Act further directs OMB to require federal agencies to apply a risk management process for collected and/or automated information (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, 2-34, A95-96; United States Congress, Paperwork Reduction Act of 1980 (Public Law 511), United States Code, Title 44, Sections 3501-2520, 95th Congress, 2nd sess., December 11, 1980; United States Congress, Computer Security Act of 1987 (Public Law 100-235), 100th Congress, 2nd sess., January 8, 1988; and United States Congress, Paperwork Reduction Act of 1995 (Public Law 104-13), United States Code, Title 44, Chapter 35, 104th Congress, 1st sess., May 22, 1995).

27. **Office of Science and Technology Policy (OSTP).**

Serves as the "source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal government" and "to define coherent approaches for applying science and technology to critical and emerging national and international problems and for promoting coordination of the scientific and technological responsibilities and programs of the Federal departments and agencies in the resolution of such problems (United States Code. Title 42: The Public

Health and Wealth, Chapter 79: Science and Technology Policy, Organization, and Priorities (Office of Science and Technology Policy), Section 6614: Policy Planning; Analysis; Advice; Establishment of Advisory Panel, 1982).

Also, by Executive Order, the Director of OSTP is assigned responsibility for directing the exercise of the President's wartime authorities over domestic telecommunications, and in emergencies or crises in which the exercise of the President's war power functions is not required or permitted by law, the OSTP Director is charged with the responsibility to advise and assist the President and Federal departments and agencies with the provision, management, or allocation of telecommunications resources (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A101 and United States Code of Federal Regulations, Title 47: Telecommunications, Chapter II: Office of Science and Technology Policy and National Security Council, Part 201: Executive Policy and Part 202: Emergency Security and Emergency Preparedness Planning and Execution, October 1, 2001).

Within OSTP, the National Security and International Affairs Division is responsible for "science and technology policies in national security and the commerce-security nexus," to include critical infrastructure protection and information security. As such, the National Security and International Affairs Division is responsible for all of OSTP's activities in the areas of national security/emergency preparedness, emergency telecommunications, the National Communications System, The National Security Telecommunications Advisory Committee, Continuity of Government programs and infrastructure protection programs United States Office of Science and Technology

Policy (United States Office of Science and Technology Policy, Homepage, National Security and International Affairs Division, http://www.whitehouse.gov/WH/EOP/OSTP/Security/html/Security.html and United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A101).

28. **Overseas Security Policy Board** (formerly the Department of State's Overseas Security Policy Group).

Responsible for policies, standards and agreements on overseas security operations, programs, and projects that affect all U.S. Government agencies under the authority of a chief of mission abroad (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A175-180, 183 and United States White House, Presidential Decision Directive/National Security Council (PDD/NSC) 29, Security Policy Coordination, Washington, D.C., September 16, 1994).

29. **President's Committee of Advisors on Science and Technology Policy (PCAST).**

Provides nonfederal sector advice to the President and the National Science and Technology Council on the nation's investment in science and technology through the Assistant to the President for Science and Technology (United States White House, Executive Order (EO) 12882, President's Committee of Advisors on Science and Technology Policy, Washington, D.C., November 23, 1993, and extended by Executive Orders (EO's) 12974 and 13062 through September 30, 1999).

30. **The President's Information Technology Advisory Committee (PITAC).**

"Provides the President with an independent assessment of the Federal government's role in HPCC, information technology, and Next Generation Internet R&D" (United States Office of Science and Technology Policy, High Performance Computing and Communications: Information Technology Frontiers for a New Millennium, A Report by the Subcommittee on Computing, Information, and Communications Research and Development, National Science and Technology Council, Supplement to the President's FY 2000 Budget, April 8, 1999 and United States National Coordination Office for High Performance Computing and Communications, High Performance Computing and Communications: FY 1998 Implementation Plan, September 3, 1998).

31. **United States Advisory Council on the NII (USAC(NII)).**

Formed to "identify appropriate government action and advise the Secretary of Commerce on matters related to the development of the NII, one of which was security through its Security Committee. The USAC(NII) disbanded in 1997 (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A206-209; United States White House, Executive Order (EO) 12864, United States Advisory Council on the National Information Infrastructure, Washington, D.C., September 15, 1993 and United States White House, Executive Order (EO) 13062, Continuance of Certain Federal Advisory Committees and Amendments to Executive Orders 13038 and 13054, Washington, D.C., September 29, 1997).

32. **United States Commission on National Security/21st Century(USCNS/21.**

Also known as the Hart-Rudman Commission and originally organized as the National Security Study Group within DoD, the USCNS/21 is a Federal Advisory Commission still organized under the SECDEF and "charged with thinking comprehensively and creatively about how the United States should provide for its national security in the first quarter of the 21st century."

33. **United States Security Policy Board (USSPB).**

Responsible for not only what to protect (classification management) but also how to protect it (security countermeasures).

The Board receives policy guidance from the National Security Council and is assisted by the:

- **Security Policy Advisory Board** (an independent and non-governmental advisory body) which reports to the President through the Assistant to the President for National Security Affairs and the
- **Security Policy Forum** (retained from the Joint Security Executive Committee) "to consider issues raised by its members or any other means; develop security policy initiatives and obtain Department and Agency comments on these initiatives for the Policy Board; evaluate the effectiveness of security policies; monitor and guide the implementation of security policy to ensure coherence and consistency; and oversee the application of security policies to ensure they are equitable and consistent with national goals" (United States Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, The Joint Staff, Washington, D.C., July 4, 1996, A-

175-180 and United States White House, Presidential Decision Directive/National Security Council (PDD/NSC) 29, Security Policy Coordination, Washington, D.C., September 16, 1994).

34. **National Research Council, National Academy of Sciences.**

Provides great weight to the policy debate with well-reasoned, authoritative research through its Computer Science and Telecommunications Board. Two such reports were Computers at Risk: Safe Computing in the Information Age and Cryptography's Role in Securing the Information Society.

35. **General Accounting Office (GAO).**

Congressional organization that is not formally involved in formulating policy, but at the same time much weight is given to its audits and evaluations, particularly by the Congress.

36. **Office of Technology Assessment (OTA).**

Although disbanded in 1996 because of lack of funding, had significant impact on the early policy making through its 1994 report Information Security and Privacy in Network Environments.

37. **Defense Science Board (DSB).**

has great weight in the policy arena with its Summer Study research reports, specifically, Information Warfare - Defense.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. ABCNews. "Computers: World Wide Warfare." ABC Nightline. December 8, 1997.

2. Adams, Charlotte. "DoD Security Software: Good Year for COTS." Military & Aerospace Electronics 9, no. 2, February 1998.

3. Albert, Reka, Hawoong Jeong, and Albert-Laszlo Barabasi. "Error and Attack Tolerance of Complex Networks." Nature, no. 406 (July 27, 2000).

4. Allison, Graham T. Essence of Decision: Explaining the Cuban Missile Crisis. Boston: Little, Brown. 1971.

5. Amir, Elan. Computer Science Division. University of California at Berkeley, http://www.cybergeography.org/atlas, January 1, 2001.

6. Anderson, Dave. "Sometimes a Nickname Has a Price." New York Times. May 3, 2001.

7. Anthes, Gary H. "DoD on Red Alert to Fend Off Info Attacks." Computerworld, 31, no.1 (January 6, 1997).

8. Armed Forces Staff College. National Defense University. Formulation of National Strategy (Class 83). Volume 1: Student Guidance, Part 1. Norfolk, VA., January 1988.

9. Armed Forces Staff College. National Defense University. Formulation of National Strategy (Class 83). Volume II: Faculty Guidance. Norfolk, VA., January 1988.

10. "ARPA Moves on `Spoofing'." 1998 Exchange Telecommunications Newsletter. September 4, 1998.

11. "At Nortel, Coverification Is an Ongoing Effort." Electronic Engineering Times, no. 989 (January 19, 1998).

12. Bacharowski, Walter. "EJTAG Port Can Simplify Prototyping." Electronic Engineering Times, no. 992, February 9, 1998.

13. Bader, Jenny Lyn. “Ideas & Trends; Paranoid Lately? You May Have Good Reason.” NY Times, March 25, 2001.

14. Bangemann, Martin. "A New World Order for Global Communications: The Need for an International Charter." Speech to Telecom Interactive `97. International Telecommunications Union. Geneva, Switzerland, September 8, 1997.

15. BBC News. “’Mafiaboy’ Hacker Jailed.” Science/Tech, September 13, 2001, http://news.bbc.co.uk/hi/english/sci/tech/newsid_1541000/1541252.stm.

16. Berger, S. Arnold. "Co-Verification Handles More Complex Embedded Systems, Part I." Electronic Design 46, no. 6 (March 9, 1998).

17. Bicknell, David. "US Defence Calls For Security Testing." Computer Weekly, January 9, 1997.

18. Black, Steven K., LtCol., USAF. A Sobering Look at the Contours of Cyberspace. Ridgway Viewpoints. No. 96-3. Matthew B. Ridgway Center for International Security Studies. University of Pittsburgh. June 1996.

19. Blair, Jayson, and William K. Rashbaum. “Man Broke Into Accounts of Celebrities, Police Say.” NY Times, March 21, 2001.

20. Boehm, Barry W. Software Risk Management. Los Alamitos, CA: IEEE Computer Society Press, 1993.

21. Borland, John. "Feds Work to Block Domain-Name Hackers." TechWeb News. August 26, 1998, http://www.techweb.com/wire/story/domnam/TWB19980825S0013.

22. ________. "Trojan-Horse Security Flaw Found in Eudora." TechWeb News. August 7, 1998, http://www.techweb.com/wire/story/TWB19980807S0007.

23. Boulding, Kenneth. "General Systems Theory: The Skeleton of Science." Management Science 2, 1956.

24. Brooks, Clinton. NSSD 145 and the Computer Security Act of 1987. Memorandum obtained by Electronic Privacy Information Center under the Freedom of Information Act, http://www.epic.org/crypto/csa/brooks.gif.

25. Brown, William J., Raphael C. Malveau, et.al. AntiPatterns: Refactoring Software, Architectures, and Projects in Crisis. New York: John Wiley & Sons, Inc., 1998.

26. Brusil, Dr. Paul J. and L. Arnold Johnson. “NIAP Readies Commercial Security Testing and Evaluation Industry in the United States” (Originally published

Open Systems Standards Tracking Report (OSSTR), March 1998, http://niap.nist.gov/NiapWebPages/osstr0398.htm.

27. Buzan, Barry. People, States, and Fear: The National Security Problem in International Relations. Chapel Hill, N.C.: The University of North Carolina Press, 1983.

28. Caisse, Kimberly. "Cisco Software Bug Exposes Routers to Hackers." TechWeb News. August 24, 1998, http://www.techweb.com/wire/story/TWB19980824S0010.

29. Campbell, Donald T., and Julian C. Stanley. Experimental and Quasi-experimental Designs for Research. Chicago: Rand McNally & Company, 1963.

30. "Canadian Juvenile Charged in Connection with February 'Denial of Service' Attacks." Technology: Computing. CNN.com, April 18, 2000, http://www.cnn.com/2000/TECH/computing/04/18/hacker.arrest.01/index.html.

31. "Canadian Teen Held in Web Attacks." April 19, 2000. NewsScan. The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 20, no. 87 (April 28, 2000), http://catless.ncl.ac.uk/Risks/20.87.html.

32. Carnegie Mellon University. CERT/CC Statistics 1988-2002. CERT. August 20, 2002, http://www.cert.org/stats/cert_stats.html.

33. ________. "CERT Coordination Center Fights Love Letter Virus." CERT Coordination Center. Software Engineering Institute. Pittsburgh, PA., May 4, 2000, http://www.cert.org/about/loveletter5-2000.html.

34. ________. CERT Summary CS-2000-02 (Last revised May 9, 2000). CERT Coordination Center. Software Engineering Institute. Pittsburgh, PA., May 31, 2000, http://www.cert.org/summaries/CS-2000-02.html.

35. ________. "Denial-of-Service Development." CERT® Advisory CA-2000-01. CERT Coordination Center. Software Engineering Institute. Pittsburgh, PA. January 2, 2000, http://www.cert.org/advisories/CA-2000-01.html.

36. ________. "Denial-of-Service Tools." CERT® Advisory CA-1999-17 (Last Updated: March 3, 2000). CERT Coordination Center. Software Engineering Institute. Pittsburgh, PA., http://www.cert.org/advisories/CA-1999-17.html.

37. ________. "Distributed Denial of Service Tools." CERT Incident Note IN-99-07 (Last updated, January 15, 2001). CERT Coordination Center. Software Engineering Institute. Pittsburgh, PA., http://www.cert.org/incident_notes/IN-99-07.html.

38. ________. Frequently Asked Questions About the Melissa Virus (Last Update, May 24, 1999). CERT Coordination Center. Software Engineering Institute. Pittsburgh, PA., http://www.cert.org/tech_tips/Melissa_FAQ.html.

39. ________. "Love Letter Worm." CERT Advisory CA-2000-04 (Last revised May 9, 2000). CERT Coordination Center. Software Engineering Institute. Pittsburgh, PA., http://www.cert.org/advisories/CA-2000-04.html.

40. ________. Process Maturity Profile of the Software Community 2000 Year End Update. Software Engineering Institute, March 2001, http://www.sei.cmu.edu/sema/pdf/2001mar.pdf.

41. ________. Results of the Distributed-Systems Intruder Tools Workshop, November 2-4, 1999. CERT Coordination Center. Software Engineering Institute. Pittsburgh, PA., December 7, 1999.

42. Claffy, K., Tracie E. Monk, and Daniel Mc Robb. "Internet Tomography." Nature: Web Matters, January 7, 1999, http://www.nature.com/nature/webmatters/tomog/tomog.html.

43. Clapper, Brian M. "Computer Emergency Response Team (CERT)." The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 8, no. 14 (January 24, 1989), http://catless.ncl.ac.uk/Risks/8.14.html.

44. ________. "Suspect in Virus Case." The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 71 (November 6, 1988), http://catless.ncl.ac.uk/Risks/7.71.html.

45. Clark, David, and Joseph Pasquale, et.al., "Strategic Directions in Networks and Telecommunications." ACM Computing Surveys: ACM 50th Anniversary Issue: Strategic Directions in Computing Research 28, no. 4 (December 1996).

46. Cole, Bernard. "Methodologies Focus on Core Integration." Electronic Engineering Times, no. 1013 (June 22, 1998).

47. "Conference on the Nat'l Competitiveness Act (HR820/S.4): Inconclusive First Session of Conference." FINS Special Report 2-36. Federal Information News Syndicate (FINS), September 27, 1994. http://sunsite.utk.edu/FINS/Special_Reports/Fins-SR2-36.txt.

48. Costlow, Terry, and Alexander Wolfe. "Embedded Systems May Harbor Hidden Glitches." TechWeb News, January 14, 1998, http://www.techweb.com/wire/story/TWB19980114S0002.

49. Cupito, Mary Carmen. "Creating Web Windows May Leave Doors to Data Unsecure." Health Management Technology 18, no. 10 (September 1997).

50. da Silva, Peter. "Re: 'UNIX' Worm/Virus." The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 71 (November 6, 1988), http://catless.ncl.ac.uk/Risks/7.71.html.

51. Devost, Matthew G. Political Aspects of Class III Information Warfare: Global Conflict and Terrorism. Presentation Notes. Second International Conference on Information Warfare. Montreal, Canada, January 18-19, 1995.

52. Dittrich, David. "The "Stacheldraht" Distributed Denial of Service Attack Tool." University of Washington, December 31, 1999.

53. Dube, Jonathan, and Brian Ross. "'Mafiaboy' Arrested." ABCNews.com. April 19, 2000, http://abcnews.go.com/sections/tech/DailyNews/webattacks000419.html.

54. Eddy, Andy. "Buffer Overflow Bugs Here to Stay: Recent Microsoft, Netscape Software Problems Nothing Out of the Ordinary." Network World, August 10, 1998.

55. Eichin, Mark W. "Internet Virus." The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 71 (November 6, 1988), http://catless.ncl.ac.uk/Risks/7.71.html.

56. ________. "Re: NYT/Markoff: The Computer Jam – How It Came About." The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 73 (November 9, 1988), http://catless.ncl.ac.uk/Risks/7.73.html.

57. Electronic Privacy Information Center. Computer Security Act of 1987. January 1, 2003, http://www.epic.org/crypto.csa.

58. Ellison, Robert, Richard Linger, Howard Lipson, Nancy Mead, and Andrew Moore. Foundations for Survivable Systems Engineering. CERT Coordination Center. Software Engineering Institute. Carnegie Mellon University. Pittsburgh, PA., (undated).

59. Ellison, Robert J., David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff and Nancy R. Mead. "Survivability: Protecting Your Critical Systems." In Proceedings of the International Conference on Requirements Engineering, April 6-10, 1998.

60. Evidence Eliminator Homepage. Robin Hood Software Ltd. November 21, 2001, www.evidence-eliminator.com.

61. Fine, Doug. "Why is Kevin Lee Poulson Really in Jail?" fine@well.com, September 3, 1993.

62. Fithen, Katherine. "Tech-Wise: Countering the Threat Posed by Distributed Denial-of-Service Tools." Infosec Outlook 1, no. 1 (April 2000), http://www.cert.org/infosec-outlook.

63. Friedman, Thomas L. "Confronting Microsoft's Arrogance." Pittsburgh Post-Gazette, June 11, 2000.

64. Geer, Daniel E., Jr. "Risk Management is Where the Money Is." Risks-Forum Digest 20, no. 6, (October 12, 1998).

65. Glave, James. "U.S. Computer Security Called Critical Mess" (Original article written October 28, 1997). Inforwar.Com & Interpact, Inc. WebWarrior@Infowar.Com, March 22, 2001, http://www.infowar.com/civil_de/civil_103097a.html-ssi.

66. Goering, Richard. "New Tools Will Force Embedded Designer to Link Hardware/Software Efforts -- Codesign Turns Workplace on Its Head." Electronic Engineering Times, no. 988 (January 12, 1998).

67. Greve, Frank. "French Techno-Spies Bugging U.S. Industries." San Jose Mercury News, October 21, 1992.

68. Hafner, Katie, and Matthew Lyon. Where Wizards Stayed Up Late: The Origins of the Internet. New York: Simon & Schuster, 1996.

69. Halperin, Morton. Bureaucratic Politics and Foreign Policy. Washington, D.C.: The Brookings Institute, 1973.

70. ________. "Why Bureaucrats Play Games." Foreign Policy 2 (Spring 1971).

71. Halperin, Morton, with the assistance of Priscilla Clapp and Arnold Kantor. "The "X" Factor in Foreign Policy: Highlights of Bureaucratic Politics And Foreign Policy." Brookings Research Report 140. Washington, D.C.: The Brookings Institute, 1975.

72. Hatton, Les. Safer C: Developing Software for High-integrity and Safety-critical Systems. London: McGraw-Hill Book Company, 1995.

73. Hayes, Brian. "The Infrastructure of the Information Infrastructure." American Scientist 85, no. 3 (May-June 1997).

74. Hewlett-Packard Company. Floppy Disk Controller Patch Homepage. http://www.hp.com/cposupport/nonjsnav/patch_faq.html.

75. Horton, Forest, Jr., ed. Towards The Global Information Superhighway: A Non-Technical Primer for Policy Makers (Special Centennial Publication). FID Occasional Paper 11. Prepared by The FID Task Force on Global Information

Infrastructures and Superhighways (FID/GIIS) and Collaboration Organizations. The Hague, Netherlands: International Federation for Information and Documentation (FID), 1995.

76. Houk, Robert D. "Single-bit Error Transmogrifications." The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 73 (November 9, 1988), http://catless.ncl.ac.uk/Risks/7.73.html.

77. Houle, Kevin J. and George M. Weaver. Trends in Denial of Service Attack Technology. CERT Coordination Center. Pittsburgh, PA: Carnegie Mellon University, October 2001.

78. Howard, John D. "An Analysis of Security Incidents on the Internet 1989-1995." Ph.D. diss., Carnegie-Mellon University, April 1997.

79. Information Technology Association of America (ITAA). "Information Security from the Private Perspective: Obstacles, Opportunities, and Responsibilities." iMP Magazine, September 22, 1999. http://www.cisp.org/imp/september 99/09 99itaa-insight.htm.

80. ________. "Response to PCCIP Report." ITAA's InfoSec Home Page. Arlington, VA., http://www.itaa.org/es/cne/cippccip.html.

81. ________. "Statement of Principles." ITAA's InfoSec Home Page. Arlington, VA., http://www.itaa.org/infosec/principles.html.

82. Institute of Electrical and Electronics Engineers. IEEE Standard Glossary of Software Engineering Terminology (Std. 610.12-1990). Standards Committee. Computer Society of the IEEE, September 28, 1990.

83. ________. IEEE Standards Status Report: Glossary of Computer Security & Privacy Terminology (Std. 610.9). Computer/Standards Coordinating Committee. Computer Society of the IEEE, 8 December 1998 (date provided by e-mail from Jodi Haasz, Senior Administrator, IEEE-SA Governance and Electronic Processes, Standards Activities, j.haasz@ieee.org, through Paul R. Croll, Chair, IEEE Software Engineering Standards Committee, pcroll@csc.co).

84. The Internet: 2001. Peacock Maps, Inc. http://209.9.224.243/peacockmaps.

85. Jackson, K.M., and J. Hruska (eds.). Computer Security Reference Book. Boca Raton, FL: CRC Press, Inc., 1992.

86. Keller, TW. "Achieving Error-Free Man-Rated Software" in 2nd International Software Testing, Analysis, and Review Conference. Monterey. CA., 1993.

87. Klein, D. V. "Foiling the Cracker; A Survey of, and Improvements to Unix Password Security" (original paper). Proceedings of the United Kingdom Unix User's Group. London, July 1990.

88. Kopetz, H. (Hermann). Software Reliability. London: Macmillan, 1979.

89. Lakhina, A., J.W. Byers, M. Corvella, and I. Matta. On the Geographic Location of Internet Resources. Technical Report 2002-15. Computer Science Department, Boston University. Boston, MA., May 2002. http://www.cs.bu.edu/techreports/pdf/2002-015-internet-geography.pdf.

90. Landwehr, Carl E., Alan R. Bull, John P. McDermott, and William S. Choi. "A Taxonomy of Computer Program Security Flaws." ACM Computing Surveys 26, no. 3 (September 1994).

91. Lange, Larry. "More Microsoft Security Woes." TechWeb News. March 28, 1997, http://www.techweb.com.

92. Lee, Leonard. The Day the Phones Stopped: The Computer Crisis - The What and Why of It, and How We Can Beat It. New York: Donald I. Fine, Inc., 1991.

93. Lee, Mara. "Creating the Ultimate Network." Washington Technology: Tech Business. December 7, 1995.

94. Lew, Jacob. "Incorporating and Funding Security in Information Systems Investments." Memorandum for the Heads of Departments and Agencies. Office of Management and Budget. Washington, D.C., February 28, 2000.

95. Littman, Jonathan. The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulson. Boston: Little, Brown and Company, 1997.

96. Machlis, Sharon. "Military Beefing Up Its Hacker Defenses; Concerned About Risks to National Security." Computerworld 31, no. 14, (April 7, 1997).

97. Major U.S. Routers. TeleGeography, Inc. Washington, DC, info@telegeography.com.

98. Malhotra, Yogesh; Abdullah Al-Shehri and Jeff J. Jones. National Information Infrastructure: Myths, Metaphors And Realities, 1995. http://www.brint.com/papers/nii/.

99. Markoff, John. "The Computer Jam – How It Came About." New York Times, November 8, 1989.

100. ________. "Pentagon Severs Military Computer From Network Jammed by Virus." New York Times, November 30, 1988.

101. Marks, Paul. "Faults Highlight Problems of Nuclear Software." New Scientist 135, no. 1836 (August 29, 1992).

102. Matlack, William H., Jr. "Interoperability the Rage at Forum." Electronic Engineering Times, no. 10 (August 24, 1998).

103. McWilliams, Brian. "Hacker Reveals Serious Security Hole in IE4." PC World News Radio. November 12, 1997, http://www.pcworld.com/news/article/0,aid,5605,00.asp.

104. Meinel, Carolyn P. "How Hackers Break In...." Scientific American 279, no. 4 (October 1998).

105. "Mentor Graphics and IKOS Deliver Verification Environment to Accelerate Telecom and Datacom System Design." PR Newswire, March 30, 1998.

106. Microsoft Corporation. "Cumulative Patch for IIS." Microsoft Security Bulletin MS01-044. Microsoft TechNet Online, August 15, 2001, (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp).

107. ________. "Erroneous Verisign-Issued Digital Certificates Pose Spoofing Hazard." Microsoft Security Bulletin MS01-017. Microsoft TechNet Online, March 22, 2001, http://www.microsoft.com/technet/security/bulletin/ms01-017.asp.

108. ________. "Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise." Microsoft Security Bulletin MS01-033. Microsoft TechNet Online, June 18, 2001, http://www.microsoft.com/telnet/security/bulletin/MS01-033.asp.

109. Miller, Harris N. Fighting Cyber Crime. Testimony before the House Committee on the Judiciary. Subcommittee Crime. Oversight hearing on Fighting Cyber Crime: Efforts by Private Business Interests. June 14, 2001. http://www.itaa.org/govt/cong/61401testim.pdf.

110. Mitre Corporation. Common Vulnerabilities and Exposures (CVE) Homepage. http://cve.mitre.org, May 9, 2001.

111. Molander, Roger, Andrew S Riddile, and Peter A. Wilson. "Strategic Information Warfare: A New Face of War." MR661. Santa Monica, CA.: The RAND Corp., 1996.

112. Molander, Roger, Peter A. Wilson, Andrew S. Riddile and Michelle K. Van Cleave. The Day After...in the American Strategic Infrastructure. Santa Monica, CA.: The RAND Corp., January 9, 1998.

113. Musa, John D., and A. Frank Ackerman. "Quantifying Software Validation: When to Stop Testing." IEEE Software 6, no. 3 (May 1989).

114. Myerson, Marian. Risk Management Processes for Software Engineering Models. Boston: Artech House, 1996.

115. National Academy of Sciences. Computers at Risk: Safe Computing in the Information Age. System Study Committee. National Research Council. National Academy Press. Washington, D.C., 1990.

116. ________. Cryptography's Role in Securing The Information Society (CRISIS). Committee to Study National Cryptography. Computer Science and Telecommunications Board. Commission on Physical Sciences, Mathematics, and Applications. National Research Council. Academy Press. Washington, D.C., 1996.

117. ________. Growing Vulnerability of the Public Switched Network. National Research Council. Washington, D.C.: National Academy Press, 1989.

118. ________. Revolution in the U.S. Information Infrastructure. National Academy of Engineering. Washington, D.C.: National Academy Press, 1995.

119. ________. The Unpredictable Certainty: Information Infrastructure Through 2000. NII 2000 Steering Committee. Computer Science and Telecommunications Board. Commission on Physical Sciences, Mathematics, and Applications. National Research Council. Washington, D.C.: National Academy Press, 1996.

120. Needham, Roger M. "Security Cyberspace: Denial of Service: An Example." Communications of the ACM 37, no. 37 (November 1994).

121. Neumann, Peter G. Computer-Related Risks. Reading, MA: Addison-Wesley Publishing Company, 1995.

122. ________. "Denial of Service Attacks." Communications of the ACM 43, no. 14 (April 2000).

123. ________. "Distributed Denial-of-Service Attacks." The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 20, no. 87 (April 28, 2000), http: //catless.ncl.ac.uk/Risks/20.87.html.

124. ________. "Re: Worm/Virus Mutations." The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 71 (November 6, 1988), http://catless.ncl.ac.uk/Risks/7.71.html.

125. NUA Internet Surveys, NUA.com, http://www.nua.ie/surveys/how_many_online/index.html, January 9, 2001.

126. orgnet.com. Logic Programming Associates (LPA) Homepage. November 21, 2001 (Last Updated: June 21, 2001), http://www.orgnet.com/netindustry.html.

127. Osgood, Robert E., and Robert W. Tucker. Force, Order, and Justice. Baltimore: The Johns Hopkins Press, 1967.

128. "Panel Warns U.S. on Terror." Pittsburgh Post-Gazette. July 15, 1999.

129. Patrizio, Andy. "Security Firm Exposes Back Orifice Functions." TechWeb News, August 10, 1998, http://www.techweb.com/wire/story/TWB19980807S0012.

130. Perrow, Charles. Normal Accidents: Living with High-Risk Technologies. New York: Basic Books, Inc., Publishers, 1984.

131. Peters, Paul Evan. "National Information Infrastructure Act of 1993 (HR1757) Passes House." Coalition for National Information, July 30, 1993, http://www.cni.org/Hforums/cni-announce/1993/0046.html.

132. "PC Patrol." Viruzlist, November 9, 1999, http://www.tonyaustin.com/viruzlist/loveletter.html.

133. Pipkin, Donald L. Halting the Hacker: A Practical Guide to Computer Security. Upper Saddle River, N.J.: Prentice Hall PTR, 1997.

134. Pluth, Ron, and Taimur Aslam. "Cosimulation Targets Early Integration." Electronic Engineering Times, no. 1013 (June 22, 1998).

135. Pollack, Andrew W. "3 Men Accused of Violating Computer and Phone Systems." New York Times, January 18, 1990.

136. Poulson, Kevin L. Letter to the Honorable Manuel L. Real. United States District Judge. Los Angeles, CA. Re: United States v. Kevin Poulson, CR 93-276R, February 9, 1995.

137. The RAND Corporation. "Strategic Warfare Rising." MR-964-OSD. Santa Monica, CA.: The RAND Corp, 1998.

138. Randell, B., J-C. Laprie, H. Kopetz, and B. Littlewood, eds. Predictably Dependable Computing Systems. Berlin: Springer, 1995.

139. Rochlin, Gene I. Trapped in the Net: The Unanticipated Consequences of Computerization. Princeton, N.J.: Princeton University Press, 1997.

140. Roger, Larry. "Cybersleuthing: Means, Motive, and Opportunity." Infosec Outlook 1, no. 3 (June 2000).

141. "Rough Sailing for Smart Ships." Scientific American 279, no. 5 (November 1998).

142. Rourke, John T. International Politics on the World Stage. Seventh Edition. Guilford, CT.: Dushkin/McGraw-Hill, 1999.

143. Ruthberg, Zella G., and Harold F. Tipton. Handbook of Information Security Management: 1995-96 Yearbook. Boston: Auerbach, 1995.

144. SANS Institute. "How to Eliminate the Ten Most Critical Internet Security Threats: The Experts' Consensus." Version 1.32. SANS Resources, January 18, 2001, http://www.sans.org/topten.html.

145. Schirrmeister, Frank, and Timothy Rhodes. "Felix Ties System Behavior, Architecture." Electronic Engineering Times, no. 1013 (June 22, 1998).

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

147. ________. Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age, 2nd edition. New York: Thunder's Mouth Press, 1996.

148. Schwartz, Stephen I. U.S. Nuclear Weapons Cost Study Project. Education Foundation for Nuclear Science. Bulletin of the Atomic Scientists, July 5, 2000, http://www.thebulletin.org/issues/1995/nd95/nd95.schwartz.html.

149. Scott, Richard W. Organizations: Rational, Natural, and Open Systems. Englewood Cliffs, N.J.: Prentice Hall, 1992.

150. Shafer, Kevin. Dictionary of Networking. San Jose: Novell Press, 1997.

151. Sheldon, Tom. Encyclopedia of Networking. Berkeley: Osborne McGraw-Hill, 1998.

152. Shirey, R. "Request for Comments: 2828." Internet Security Glossary. Network Working Group. GTE/BBN Technologies, May 2000, ftp://ftp.isi.edu/in-notes/rfc2828.txt.

153. Siedsma, Andrea. "Spy vs Spy." T Sector: Everything Tech San Diego, January 2001.

154. Slabodkin, Gregory. "FBI Suspects Two Teens in DoD Systems Attack." Government Computer News 17, no. 5 (March 9, 1998).

155. The Stanley Foundation. Beyond Cold War Thinking: Security Threats and Opportunities (Report of the Twenty-Fifth United Nations of the Next Decade Conference), June 24-29, 1990.

156. Steinberg, Don. "EDI Evolution Continues with Integration into Business Applications." PC Week 5, no. 6 (February 9, 1998).

157. Suresh babu, R.M., B.B. Biswas, and G. Govindarajan. "Developing Highly Reliable Software." IEEE Micro 17, no. 5 (September/October 1997).

158. Targowski, Andrew S. Global Information Infrastructure: The Birth, Vision, and Architecture. Harrisburg, PA.: Idea Group Publishing, 1996.

159. Templeton, Brad. "Risks of Getting Opinions From Semi-Biased Sources." The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 71 (November 6, 1988), http://catless.ncl.ac.uk/Risks/7.71.html.

160. Thomas, Doug. "Why Hackers Hate Microsoft." Online Journalism Review. Annenberg School for Communication. University of Southern California, April 29, 1998, http://www.ojr.org/ojr/technology/1017969479.php.

161. Tu, Yuhai. "How Robust is the Internet?" Nature, no. 402 (July 27, 2000).

162. United States Code. Title 42. The Public Health and Wealth. Chapter 79. Science and Technology Policy, Organization, and Priorities. Office of Science and Technology Policy. Section 6614. Policy Planning; Analysis; Advice; Establishment of Advisory Panel, 1982.

163. ________. Title 47 Telegraph, Telephones, and Radiotelegraphs. Chapter 8. National Telecommunications and Information Administration. Section 901, Definitions, Findings, Policy [National Telecommunications and Information Administration Organization Act (P.L. 102-538)], Oct. 27, 1992.

164. United States Code of Federal Regulations. Title 47. Telecommunications. Chapter II. Office of Science and Technology Policy and National Security Council. Part 201. Executive Policy, October 1, 2001.

165. ________. Title 47. Telecommunications. Chapter II. Office of Science and Technology Policy and National Security Council. Part 202. Emergency Security and Emergency Preparedness Planning and Execution, October 1, 2001.

166. ________. Title 47. Telecommunications. Part 63. Extension of Lines, New Lines, and Discontinuous, Reduction, Outage, and Impairment of Service by Common Carriers and Grants of Recognized Private Operating Agency Status. Section 100. Notification of Service Outage, October 1, 2001.

167. United States Congress. Clinger-Cohen Act of 1996 (also known as Information Technology Management Reform Act of 1996 (Public Law 104-106, Division E). United States Code. Title 40. Section 1401. 104th Congress, 2nd sess., January 3, 1996.

168. ________. Computer Security Act of 1987 (Public Law 100-235). 100th Congress, 2nd sess., January 8, 1988.

169. ________. High Performance Computing Act of 1991 (Public Law 102-194), 102nd Congress, 1st sess., December 9, 1991

170. ________. National Science and Technology Policy, Organization and Priorities Act of 1976 (Public Law 94-282). 94th Congress, 2nd sess., May 11, 1976.

171. ________. National Public Telecommunications Infrastructure Act of 1994, 103d Congress, 2d sess., June 15, 1994.

172. ________. National Security Act of 1947 (PL 235 - 61 Stat. 496; 50 U.S.C. 402), as amended, 80th Congress, 1st sess., July 26, 1947.

173. ________. Paperwork Reduction Act of 1980 (Public Law 511). United States Code. Title 44. Sections 3501-2520. 95th Congress, 2nd sess., December 11, 1980.

174. ________. Paperwork Reduction Act of 1995 (Public Law 104-13). United States Code. Title 44. Chapter 35. 104th Congress, 1st sess., May 22, 1995.

175. ________. Telecommunications Act of 1996 (Public Law No. 104-104). United States Code. Title 110. Section 56. 104th Congress, 2nd sess., January 3, 1996.

176. United States Congress. House of Representatives. "Opening Statement of Chairwoman Constance A. Morella." Computer Security. Hearing. Subcommittee on Technology. Committee on Science. 105th Congress, 1st sess., February 11, 1997.

177. United States Congress. Senate. S.1086, National Telecommunications Infrastructure Act of 1993, 103d. Congress, 1st sess., June 9, 1993.

178. ________. Senate. Y2K Aftermath: Crisis Averted: Final Committee Report. S. Prt. 106XX. Special Committee on the Year 2000 Technology Problem. 106th Congress, 2nd sess., February 29, 2000.

179. ________. Select Committee on Governmental Operations with Respect to Intelligence Activities, Foreign and Military Intelligence — Book I. 94th Congress, 2nd sess., 26 April 1976.

180.________. Select Committee on Intelligence. "Worldwide Threat Assessment," Testimony of John Deutch, Director of Central Intelligence, 104th Cong., 2nd sess., February 22, 1996.

181. United States Department of Commerce. Commerce Announces Streamlined Encryption Export Regulations. Fact Sheet. Washington, D.C., January 12, 2000.

182.________. Homepage. United States National Telecommunications and Information Administration, www.nce.gov/ncs/html/ntia.html.

183. United States Department of Defense. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. The Joint Staff. Washington, D.C. July 4, 1996.

184.________. Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield. Defense Science Board. Washington, D.C., October 1994.

185.________. Report of the Defense Science Board Task Force on Information Warfare (Defense). Defense Science Board. Washington, D.C., January 8, 1997.

186.________. Technology, Society, and National Security (Predecision Draft). United States National Security Study Group (NSSG) (since renamed U.S. Commission on National Security/21st Century (USCNS/21 and also known as also known as the Hart-Rudman Commission), May 1, 1999.

187. United States Department of Justice. Awareness of National Security Issues and Response (ANSIR) Program Homepage. Federal Bureau of Investigation, April 6, 1998. http://www.fbi.gov/hq/nsd/ansir/ansir.htm#threatlist.

188.________. CIAO Homepage. Critical Infrastructure Assurance Office, http://www.info-sec.com/ciao.

189.________. Related Sites Webpage. Federal Bureau of Investigation. National Information Protection Center, http://www.nipc.gov/sites.htm.

190. United States District Court. Central District of California. United States of America vs. Kevin Lee Poulson, No. CR 93-376-R. Reporter's Transcript of Proceedings, Sentencing. Los Angeles, California, February 24, 1995.

191. United States Chief Information Officers Council. CIO Council Homepage, March 24, 2000, http://cio.gov.

192.________. CIO Council Strategic Plan. Washington, D.C., January 1998, http://cio.gov/content/fy1998.htm.

193.________. Strategic Plan, Fiscal Year 2000. Washington, D.C., (undated), http://www.cio.gov/content/fy2000.pdf.

194. United States Information Infrastructure Task Force (IITF). Homepage, http://www. iitf.nist.gov/committee.html.

195. United States Joint Security Commission. Redefining Security. A Report to the Secretary of Defense and the Director of Central Intelligence. Washington, D.C., February 28, 1994.

196.________. Report of the Joint Security Commission II. Washington, D.C. August 24, 1999.

197. United States National Coordination Office for Computing, Information, and Communications. IT R&D Handout for FY2001 Budget Rollout by the National Coordination Office. Washington, D.C., February 7, 2000.

198. United States National Coordination Office for High Performance Computing and Communications. High Performance Computing and Communications: FY 1995 Implementation Plan, April 8, 1994.

199.________. High Performance Computing and Communications: FY 1997 Implementation Plan, December 1996.

200.________. High Performance Computing and Communications: FY 1998 Implementation Plan, September 3, 1998.

201.________. High Performance Computing and Communications: FY 1999 – FY 2000 Implementation Plan. Interagency Working Group on Information Technology Research and Development. Office of Science and Technology Policy. Washington, D.C., April 2000.

202. National Information Assurance Partnership (NIAP). Common Criteria Testing Laboratories (CCTL) Webpage, February 9, 2003, http://niap.nist.gov/cc-scheme/TestingLabs.html.

203.________. Introducing the National Information Assurance Partnership Webpage, February 9, 2003, http://niap.nist.gov/howabout.html.

204. United States National Science and Technology Council. Council Committees Purposes Webpage, May 17, 1999, http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/committee/ct_purpose,.html.

205.________. Homepage, May 17, 1999, http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/NSTC_Home.html.

206. United States National Security Agency. National Information Systems Security (INFOSEC) Glossary. NSTISSI No. 4009. Ft. Meade, MD: NSTISSC Secretariat (142), September 2000.

207. United States National Security Agency/National Institute of Standards and Technology. Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235 24 March 1989.

208. ________. Letter of Partnership. National Information Assurance Partnership (NIAP), August 22, 1997.

209. United States. National Security Council (NSC). Homepage. http://www.nsc.gov.

210. United States National Security Telecommunications Advisory Committee (NSTAC). Issue Review: A Review of NSTAC Issues Addressed Prior to NSTAC XIX. The President's National Security Telecommunications Advisory Committee. Washington, D.C., March 1997.

211. ________. "Report on the NS/EP Implications of Intrusion Detection Technology Research and Development." Washington, D.C., December 1997.

212. ________. Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration. A Symposium Sponsored by the President's NSTAC in Conjunction with the Workshop on Security in Large-Scale Distributed Systems, Purdue University, West Lafayette, IN, October 20-21, 1998.

213. United States National Security Telecommunications and Information Systems Security Committee (NSTISSC) NSTISSC Homepage. http://www.nstissc.gov/html/overview.html.

214. United States Office of Management and Budget (OMB). "Analytical Perspectives" and "Promoting Research." Budget of the United States. Fiscal Year 2001. Washington, D.C.: GPO, February 7, 2000.

215. ________. Management of Federal Information Resources. Circular No. A-130. Washington, D.C., February 8, 1996.

216. ________. "Report on Information Technology Investments (Exhibit 53) FY2001 Budget." Preparation, Submission, and Execution of the Budget. Circular No. A-11. Washington, D.C., 2000.

217. United States Office of Science and Technology Policy. High Performance Computing and Communications: Toward a National Information

Infrastructure. A Report by the Committee on Physical Mathematical and Engineering Sciences. Federal Coordinating Council for Science, Engineering, and Technology. Supplement to the President's FY 1994 Budget, 1993.

218. ________. High Performance Computing and Communications: Technology for the National Information Infrastructure. Committee on Information and Communications. National Science and Technology Council. Supplement to the President's FY 1995 Budget, May 1994.

219. ________. High Performance Computing and Communications: Foundation for America's Information Future. A Report by the Committee on Information and Communications. National Science and Technology Council. Supplement to the President's FY 1996 Budget, September 1995.

220. ________. High Performance Computing and Communications: Advancing the Frontiers of Information Technology. A Report by the Committee on Computing, Information, and Communications. National Science and Technology Council. Supplement to the President's FY 1997 Budget. November 1996.

221. ________. High Performance Computing and Communications: Technologies for the 21st Century. Committee on Computing, Information, and Communications. National Science and Technology Council. Supplement to the President's FY 1998 Budget, November 1997.

222. ________. High Performance Computing and Communications: Networked Computing for the 21st Century. Committee on Computing, Information, and Communications. National Science and Technology Council. Supplement to the President's FY 1999 Budget, August 1998.

223. ________. High Performance Computing and Communications: Information Technology Frontiers for a New Millennium. A Report by the Subcommittee on Computing, Information, and Communications Research and Development. National Science and Technology Council. Supplement to the President's FY 2000 Budget, April 8, 1999.

224. ________. Homepage, May 17, 1999, http://www.whitehouse.gov/OSTP.

225. ________. Home Page. National Security and International Affairs Division, http://www.whitehouse.gov/WH/EOP/OSTP/Security/html/Security.html.

226. United States White House. Administration Updates Encryption Export Policy. Fact Sheet. Office of the Press Secretary. Washington, D.C., September 16, 1999.

227.________. Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. White Paper. Washington, D.C., May 1998, http://www.info-sec.com/ciao.

228.________. Critical Foundations: Protecting America's Infrastructures. Report of the President's Commission on Critical Infrastructure Protection. Washington, D.C., October 1997.

229.________. Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue. Washington, D.C., January 2000.

230.________. Executive Order (EO) 12333. United States Intelligence Activities. Washington, D.C., December 4, 1981.

231.________. Executive Order (EO) 12356. National Security Information. Washington, D.C., April 2, 1982.

232.________. Executive Order (EO) 12382. President's National Security Telecommunications Advisory Committee. Washington, D.C., September 13, 1982.

233.________. Executive Order (EO) 12472. Assignment of National Security and Emergency Preparedness Telecommunications Functions. Washington, D.C., April 3, 1984.

234.________. Executive Order (EO) 12864. United States Advisory Council on the National Information Infrastructure. Washington, D.C.,, September 15, 1993.

235.________. Executive Order (EO) 12882. President's Committee of Advisors on Science and Technology Policy. Washington, D.C., November 23, 1993.

236.________. Executive Order (EO) 12958. Classified National Security Information. Washington, D.C., April 17, 1995.

237.________. Executive Order (EO) 13010. Critical Infrastructure Protection. Washington, D.C., July 15, 1996.

238.________. Executive Order (EO) 13011. Federal Information Technology. Washington, D.C., July 16, 1996.

239.________. Executive Order 13035. President's Information Technology Advisory Committee. Washington, D.C., February 17, 1999.

240.________. Executive Order (EO) 13130. National Infrastructure Assurance Council. Washington, D.C., July 14, 1999.

241.________. "Investing in Science and Technology." The President's 7-Year Balanced Budget Plan. Chapter 7, December 7, 1995, http://www.ostp.gov/html/budget.html.

242.________. National Science and Technology Council Annual Report, 1997. National Science and Technology Council. Washington, D.C., April 1998.

243.________. National Science and Technology Council Annual Report, 1998. National Science and Technology Council. Washington, D.C., March 1999.

244.________. National Security Decision Directive (NSDD) 84, Safeguarding National Security Information, Washington, D.C., 1982.

245.________. National Security Decision Directive (NSDD) 97. National Security Telecommunications Policy. Washington, D.C., June 13, 1983.

246.________. National Security Decision Directive (NSDD) 145. National Policy on Telecommunications and Automated Information Systems Security. Washington, D.C., September 17, 1984.

247.________. National Security Directive (NSD) 42. National Policy for the Security of National Security Telecommunications and Information Systems. Washington, D.C., July 5, 1990.

248.________. National Security Strategy of the United States. Washington, D.C., January 1987.

249.________. National Security Strategy of the United States. Washington, D.C., January 1988.

250.________. National Security Strategy of the United States. Washington, D.C., August 1991.

251.________. National Security Strategy of the United States. Washington, D.C., January 1993.

252.________. National Security Strategy of Engagement and Enlargement. Washington, D.C., February 1995.

253.________. A National Security Strategy For a New Century. Washington, D.C., December 1999.

254.________. President Clinton Announces Nearly A $3 Billion Increase in Twenty-First Century Research Fund. Office of the Press Secretary. Washington, D.C., January 21, 2000.

255.________. Presidential Decision Directive (PDD) 24. U.S. Counterintelligence Effectiveness. Washington, D.C., May 3, 1994.

256.________. Presidential Decision Directive/National Security Council (PDD/NSC) 29, Security Policy Coordination. Washington, D.C., September 16, 1994.

257.________. Presidential Decision Directive (PDD) 39. U.S. Policy on Counterterrorism. Washington, D.C., June 21, 1995.

258.________. Presidential Decision Directive (PDD) 63. Protecting America's Critical Infrastructure. Washington, D.C., May 22, 1998.

259.________. Presidential Decision Directive/National Security Council (PDD/NSC) 29, Security Policy Coordination. Washington, D.C., September 16, 1994.

260.________. Presidential Review Directive (PRD) 27, Advance Telecommunications and Encryption. Washington, D.C., 1993.

261.________. Presidential Review Directive (PRD) 29. National Security Information. Washington, D.C., April 26, 1993.

262. "U.S. to Relax Restrictions on Encryption Technology," Wall Street Journal, New York, September 16, 1999.

263. Van Name, Mark L., and Bill Catchings. "Seamless Doesn't Always Mean Smooth." PC Week 14, no. 50 (December 1, 1997).

264. van Wyk, Ken. "(Long) Report on the Internet Worm: A Report on the Internet Worm by Bob Page." The Risks Digest: Forum on Risks to the Public in Computers and Related Systems 7, no. 76 (November 12 1988), http://catless.ncl.ac.uk/Risks/7.76.html.

265. Vibert, Robert. "Who's to Blame for This New-Found Love?" May 2000. http://www.vibert.ca/wholove.htm.

266. Wiener, Lauren Ruth. Digital Woes: Why We Should Not Depend on Software. Reading, MA: Addison-Wesley Publishing Company, 1993.

267. Williams, Martyn. "Hackers Penetrate Defense Department Computer Networks." Newsbytes, April 22, 1998. http://www.newsbytes.com.

268. Williams, Phil. "Transnational Criminal Organisations and International Security." Survival 36, no. 1 (Spring 1994).

269. Williamson, Mickey. "The Science of Software Development." CIO Magazine. April 15, 1996.

270. Williamson, Miryam. "Special Report: Software Reuse - Technology." CIO Magazine. March 1, 1997.

271. Zuckerman, M.J. “Asleep at the Switch? How the Government Failed to Stop the World’s Worst Internet Attack.” USA Today. March 9, 2000.