HOWARD UNIVERSITY

The Computer Security Enhancement Act and Presidential Decision Directive 63: Congressional and Presidential Attempts to Protect the Nation's Critical Infrastructures

A Dissertation
Submitted to the Faculty of the
Graduate School

of

HOWARD UNIVERSITY

in partial fulfillment of the
requirement for the
degree of

DOCTOR OF PHILOSOPHY

Department of Political Science

by

Vivian Elaine Luke-Vanzego

Washington, D.C.
May 2003

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

HOWARD UNIVERSITY

GRADUATE SCHOOL

DEPARTMENT OF POLITICAL SCIENCE

COMMITTEE APPROVAL FORM

~~Charles Harris, Ph.D.~~
Lorenzo Morris Ph.D.

Babalola Cole
Babalola Cole, Ph.D.

Morris Levitt, Ph.D.

Maurice Woodard, Ph.D.

Bamijoko Smith, Ph.D.
Assistant Professor
The American University
Kogod School of Business

Babalola Cole
Babalola Cole, Ph.D.
Dissertation Advisor

Candidate: Vivian Elaine Luke-Vanzego

Date of Defense: April 25, 2003

DEDICATION

In loving memory of Michelle A. Evans
(February 8, 1979 - March 16, 2000)

My dear Michelle

Taken from us
no warning, too soon
Only God knows why therefore we trust Him,
He who rules
You gave all that you had and expected nothing in return
The lessons you taught are many, so many to learn

To become a M.D. was your goal
You were an advocate for change
That was your role
You lived your life as Jesus lived
With love in your heart
Selflessly, you did

We call many men heroes who have contributed
Far less than you
But who are the real heroes,
Will we ever know their names, too?
Well you, Michelle, are one
And Raiven will know in time
That you made a difference in the world
and never asked for a dime

You made us all so proud you see
It's difficult to carry on
But when we see the brightest star and believe it is you
We remember to say 'to God be the glory'
For bringing us you

You touched many lives at home
Across the seas as well
So I dedicate this work to you
In celebration of your life,
my dear Michelle

ACKNOWLEDGEMENTS

With the passing of time we
have acquired knowledge,
understanding, and friendship.
With the help of many, we
have accomplished our goals
and are prepared to reach
tomorrow's challenges.
(Author Unknown)

In my quest to accomplish my goal I was blessed to have had the love and support of family and friends. Thank you for your prayers, support, and encouragement. I especially wish to thank and recognize those persons who in their own unique way made this dream a reality.

To my husband, Ray, while there were days when I doubted whether or not I would finish you were always there to encourage me to reach my goal. Often, it was your words that pushed me along and kept me focused. Thank you for your unwavering love and support.

To our daughter, Raiven, you are the reason I began this challenge, you are the reason I finished it. You kept me focused on my priorities -- family first. I pray mommy and daddy will continue to be positive role models in your life. You are my sunshine.

To my parents, Vincent and Elaine Luke, you laid the foundation upon which I stand – strong faith, love and support of family, and a thirst for knowledge. Every day I thank God for the examples you set and for blessing me with you.

To my in-laws, Raymond and Margaret Vanzego, the journey was long and often arduous but with your help, support, and encouragement I made it through. Thank you for helping to make my load a little lighter.

To my Dissertation Advisor, Dr. Babalola Cole, you were more than a professor and advisor along this journey -- you were my mentor, confidant, and friend. Due to your sincere dedication I finished the dissertation. You believed in my ability to succeed and guided me through it all. Thank you for your guidance, patience, and friendship.

Special thanks go to the members of my Committee, Drs. Charles Harris (Committee Chair), Morris Levitt (Professor Emeritus), Bamijoko Smith (External Reader – The American University), and Maurice Woodard, for their assistance, guidance, and encouragement. I pray my work has made each of you proud to have been a member of the Committee.

To Dr. Donn Davis, Director Graduate Studies Program - Department of Political Science, without your persistence and willingness to go that extra mile on my behalf -- on many occasions -- I would not have been able to maintain my committee and see my way through the process. Thank you for your efforts to fight the fight so that I may achieve my goal. All of the hard work you have done, your accessibility, reliability, and your commitment to students have not gone unnoticed.

To Dr. Lorenzo Morris, Interim Chair, Department of Political Science, your willingness to step in at the eleventh hour and serve as my Committee Chair cannot go unnoticed. Thank you, again, for the time you spent lobbying on my behalf to ensure that I graduated on time and as always for your continuous support over the years.

To my Colleagues, Drs. Pearl Ford, Joseph Green, and Eugene Laney, the end is finally here! It was a difficult road but we made it. We encouraged and supported one another through some of the most difficult periods in our lives. I pray we will continue to do so in the future. Go forth and make a difference in someone's life.

To the Potomac View Rug Rat Moms, Dr. Sandra Wills Hannon, Lt. Col.(Air Force) Lynn Hamilton-Jones, and Brenda Wise, thank you, thank you, thank you for the countless days when you lived up to the old African proverb "it takes a village to raise a child." Your love and support will always be appreciated. Each of you is a professional mom with demanding careers yet you always found the time to lend a hand and provide support and encouragement. You are all strong women, wonderful moms, and great friends.

ABSTRACT

The transition from the Industrial Age to the Information Age has brought technological advancements that have created vulnerabilities in our national information infrastructures and threats to our national security. While the technologies of the latter twentieth century have improved business and financial processes and the ability to communicate, they have also significantly contributed to a pervasive problem in our ability to secure the homeland. Further, although national security has, traditionally, been recognized as the responsibility of the federal government, the onus is now on the infrastructure's stakeholders to share the responsibility for developing and implementing security measures to ensure national security.

This dissertation seeks to study the relationship between the transition between the Ages, the technological advancements and ensuing vulnerabilities that accompanied the Information Age, and the roles of the legislative and executive branches of government to address these issues. Thus, where the politics of the last one hundred years focused on the needs of the Industrial Age, the politics of the Information Age must focus on information security, storage, protection, and information sharing.

A descriptive analysis of the decision-making processes that affected both the legislative and executive branches was utilized in this study. David Easton's Systems model and Malcolm Jewell and Samuel Patterson's Legislative Role Orientation model were used to closely examine and, where applicable, dissect the plethora of actors who comprise the legislative system. Those factors – both external and internal - that influence the Congress and the President, their respective committees and layers of bureaucracy, interest groups, private sector businesses, and public opinion were also analyzed.

The findings in the research reveal that the Information Age has necessitated a shift in the practices of the federal government. It has forced the legislative branch, to reconsider how issues of national security relative to critical infrastructures, i.e., water supply, electrical power grids, telecommunications networks, and financial services, will be safeguarded. Moreover, it has forced the executive branch to fill the gaps where the legislation was either inadequate or ineffective.

TABLE OF CONTENTS

Page

LIST OF TABLES

TABLE PAGE

LIST OF FIGURES

LIST OF ABBREVIATIONS

AOL: America On-line

APC: Association for Progressive Communication

BARC: Bhabha Atomic Research Center

CEO: Chief Executive Officer.

CERT: The Computer Emergency Response Team

CIA: Central Intelligence Agency

CIAO: Critical Infrastructure Assurance Office

CIO: Chief Information Officer

CIP: Critical Infrastructure Protection

COCA: Clearinghouse on Computer Accommodation

CPSR: Computer Professionals for Social Responsibility

CSPP: Computer Systems Policy Project

CSTB: Computer Science and Telecommunications Board

DARPA: Department of Defense Advanced Research Projects Agency

DES: Data encryption standard

DHS: Department of Homeland Security

DOD: Department of Defense

E-Commerce: Electronic Commerce

EEF: Electronic Frontier Foundation

ENAIC: Electronic Numerical Integrator and Computer

ERP: Enterprise Resource Planning

FAA: Federal Aviation Administration

FBI: Federal Bureau of Investigations

FDA: Food and Drug Administration

FEMA: Federal Emergency Management Agency

FIDNET: Federal Intrusion Detection Network

FOIA: Freedom of Information Act

GAO: General Accounting Office

GITS: Government Information Technology Services

GPRA: Government Performance and Results Act

HERF: High Energy Radio Frequency

HPCA: High Performance Computing Act of 1991

HPCP: High Performance Computing Program

IW: Information Warfare

INS: Immigration and Naturalization Service

ISACs: Information Sharing and Analysis Centers

ISSA: Information Systems Security Association

ITAA: Information Technology Association of America

LBL: Lawrence Berkley Laboratory.

LAN: Local Area Network

NASA: National Aeronautics and Space Administration

NC: Network Computer

NGO: Non-governmental organizations

NII: National Information Infrastructure

NIPC: National Infrastructure Protection Center

NIST: National Institute of Standards for Technology

NME: National Military Establishment

NPR: National Performance Review

NREN: National Research and Education Network

NSA: National Security Agency

NSC: National Security Council

OMB: Office of Management and Budget

PCCIP: President's Commission on Critical Infrastructure Protection

PDD 63: Presidential Decision Directive 63

PIN: Personal Identification Number

R&D: Research and Development

WANK: Worms Against Nuclear Killers

Y2K: Year 2000

Chapter I

INTRODUCTION

Statement of the Problem

Advancements in technology have placed our nation's security at risk and to a large extent have impacted our national government and national information infrastructures. In an attempt to address the effect of these advancements on our national government, the 105th Congress passed the Computer Security Enhancement Act of 1997. This Act amended the Computer Security Act of 1987, by giving the National Institute of Standards and Technology (NIST) the primary role of establishing guidelines for the protection of computer systems in the Federal Government. Although the 1987 Act and a limited version of the ensuing Computer Security Enhancement Act of 1997 authorized NIST to establish the much needed guidelines for federal computer systems, it did little to address and/or protect our nation's critical information infrastructures.

Shielding, preserving and assuring the continuity and viability of our nation's very important information systems has long been the policy of the United States. As conditions necessitate, however, Congress updates the law or laws in order to keep adhering to this course. Thus, and as a result of technological developments in the fields of information, information management, and communications of the "Information Age," the 105th Congress passed the Computer Security Enhancement Act of 1997. Unfortunately, however, the Act did not go far enough. In an attempt to address the shortcomings and inadequacies of this law, the Clinton Administration developed the

Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (PDD 63), dated May 22, 1998.

Arguably, prior to the passage of the 1997 Act and the ensuing PDD 63, efforts to protect our national information infrastructures were not comprehensively addressed by both the executive and legislative branches of government. Thus, where the politics of the last one hundred years centered on "Industrial Age" technology, the politics of the future will necessarily focus on "Information Age" concerns; specifically security, storage, protection, and the exchange of information. As a result, a new paradigm must be developed in order to fully and adequately address the current vulnerabilities as a result of technological advancements.

Statement of Purpose

When comparing the governmental structure of the United States to that of other industrial nations, one might be most intrigued by the unique nature of its three separate yet equal branches of power -- executive, legislative, and judiciary. The founding fathers of the American system of government purport this type of structural arrangement as a potential safeguard against one branch obtaining a dominant role in the government. This approach inherently created the concept of checks and balances within the American governmental structure as set forth in the United States Constitution. With the advancements in technology, however, this co-equal form of governance has been challenged on many fronts.

The Technological Age or Information Age has forced the legislative and executive branches, primarily, to reconsider how issues of information security and national security are addressed, and, how -- if possible -- these matters may be resolved if they both work in unison. One may argue that the advances in technology have exacerbated an existing yet long-standing conflict between these two branches of government. Further, while legal challenges have been raised before the third branch of government -- the U.S. Supreme Court -- they have tended to defer to the legislative branch and, thus have assumed a less than prominent posture on the matter.

Advances in computer technology, satellites, telecommunications, fiber optics, and networks, to name just a few, have permeated every aspect of daily life to such an extent that the fundamental means and methods of conducting government affairs and addressing issues of national security have undoubtedly -- yet necessarily -- changed. A logical consequence of this pervasive technology is the inevitable struggle, albeit positive and/or negative, between the president and the Congress over who shall lead the charge in protecting our national information infrastructures.

The purpose of this dissertation is to examine the Computer Security Enhancement Act of 1997 and the attempts made by the executive branch to address its shortcomings via the Clinton Administration's Policy On Critical Infrastructure Protection: Presidential Decision Directive 63 (PDD 63), dated May 22, 1998.[1]

In furtherance of the research, this dissertation will analyze the roles played by congressional committees, members of the Clinton Cabinet, and other key advisors to the

[1] This directive was established in part to address aspects of the Act which failed to codify laws to protect our national information infrastructures.

president in providing a knowledge base for the making of information policy -- which impacts our domestic and foreign policy decisions.

An additional goal of this study is to contribute to the presently inadequate literature on the effect that technology has had on our national information infrastructures and the steps we must take to improve the mechanisms in place to protect them. This becomes important especially when one realizes that "with few exceptions, policy makers and analysts are just beginning to discern how government and politics may ultimately be affected by the information revolution."[2]

This dissertation is organized into six chapters. The first one, as the introductory chapter, states the problem, purpose of the study, a review of related literature, theoretical framework, methodology, the significance of the study, and its limitations.

Chapter Two addresses the role of Congressional Committees in the passage of the Computer Security Enhancement Act of 1997. Specifically, these committees include the House Committee on Science and Subcommittee on Technology, and Senate Committee on Commerce, Science, and Transportation. The Senate and House committee hearings and debates were closely examined in order to illustrate their involvement and levels of consideration of the bill.

Chapter Three deals with the history of Executive Orders and their impact on legislative policies. An examination of the role of the Executive, i.e., the Clinton Administration, and its attempts to improve upon or expand the focus of the Computer Security Enhancement Act through PDD 63. Presidential messages and speeches (before

[2] David Ronfeldt, "Cyberocracy is Coming", *The Information Society Journal* 8, no. 4 (1992) : 243-296.

and after the issuance of the Directive), press releases and briefings, as well as the statements of government officials in Congressional hearings were perused in order to shed additional light on executive influence and interest in addressing the inadequacies of the Act.

Chapter Four analyzes threats to our national information security and national security in general since the PDD 63 edict was issued. This section addresses our on-going struggle with matters concerning information vulnerability and security, threats to our information integrity and stability, the real threat of information warfare, and the political context of information warfare and its consequences.

Chapter Five deals with the importance of forging a public-private partnership to reduce the vulnerabilities created by technological advancements. The formulation and cultivation of this partnership was provided as a recommendation in PDD 63. It was through the Directive that the Clinton Administration tried to encourage and coordinate the efforts of both the government and the private sector to make our critical infrastructure less vulnerable to attack.

Chapter Six provides conclusions and recommendations that are designed to address how attacks against our national information infrastructures may be thwarted and our national security protected.

Review of Literature

This section of the research will address the following relevant areas: (1) an overview of selected literature on the legislative process; (2) a review of the relevant literature pertaining to the constitutional authority of the executive in the issuance of presidential directives historically; (3) literature on specific events relative to threats to our national information infrastructures. For example, hacker activity, viruses and worms, and cyberterrorism; (4) literature on the methods used by the public and private sectors to address information vulnerabilities, public sector efforts to combat cyber attacks and threats to information integrity and security.

1. A Review of Related Literature on the American Legislative Process.

The American legislative process is a complex web of political activity which is arguably at the root of our political system. Although much has been written about the legislative process, the primary focus of the existing literature has been on programs and institutions that are impacted by the process. In this section the American legislative process will be examined from a different perspective, specifically, that which addresses the politics of the process, the internal and external factors which influence the process, and to a limited extent the roles of selected yet relevant participants in the process.

The existing literature on the legislative process is vast. However, one cannot reference the literature in this field without first noting the classics. The outstanding classical works of David Truman, *The Governmental Process: Political Interests and*

Public Opinion[3] and Arthur Bentley, *The Process of Government*[4] are two requisite classical references. David Truman dissects the role interest groups play in the political system, he examines their influence on the system, and the ramifications of their involvement in the system and the process. He argues that they are an integral part of American politics.

Further, Truman maintains that interest groups are an implicit part of the legislative process. They often impact the operational aspect of each branch of government -- legislative, executive, and judicial -- and their interrelationship in the political and legislative processes. Similarly, Arthur Bentley articulates the importance of the role of interest groups in American politics and argues that to study the political process one must examine the influence of interest groups and the integral importance of their contribution to the political system.

Another noteworthy writer who has stressed the importance of interest group activities in the legislative process is Alan Rosenthal, *The Third House: Lobbyists and Lobbying in the State.*[5] Rosenthal argues that interest group activity and their pervasive influence on the legislative process have created a virtual "*Third House*" in the legislature. Whereby, bills -- once endorsed or sanctioned by an interest group(s) – will either continue onward through the legislative process or dwindle to nothing.

[3] David Truman, *The Governmental Process: Political Interests and Public Opinion,* 1st ed. (New York: Alfred A. Knopf, Inc., 1951).

[4] Arthur Bentley, *The Process of Government* (Bloomington: The Principia Press, Inc., 1935).

[5] Alan Rosenthal, *The Third House: Lobbyists and Lobbying in the State* (Washington, DC: Congressional Quarterly Press, 1993).

Randall Ripley, in his work *Congress: Policy and Process,*[6] studies business processes and the organizational structure of Congress. He observed that Congress's decision making capability hinges on three sets of principles. First, members of Congress are elected representatives of the people. Second, there exists a powerful executive office. Third, the influence of a professional bureaucracy.[7]

In *Congressional Politics*[8], Christopher Deering examines how members of Congress in their legislative decision making role receive assistance and are influenced by power brokers both within and outside of the legislature. He reveals how members of Congress can assist the passage of bills by imposing their will and powerful influence on their colleagues. In addition, he discusses how members of Congress engage in tactics such as the careful drafting and scheduling of bills, their roles in coalition building, and through the identification of powerful groups outside the Congress. Deering also provides insights into the role of congressional committees in the legislative process.

When examining the funding appropriations procedures in the legislative process one is instantly drawn to the work of Richard Fenno, *The Power of the Purse.*[9] Fenno examines funding appropriations primarily through an introspective of the House Appropriations Committee. In his examination, the author pontificates that the House Appropriations Committee (and the Senate Appropriations Committee to a lesser degree) constitutes an identifiable and independent political system with internal parts existing in

[6] Randall P. Ripley, *Congress: Policy and Process* (New York: W.W. Norton and Company, 1988).

[7] Ibid.

[8] Christopher Deering, *Congressional Politics* (Illinois: The Dorsey Press, 1969).

[9] Richard Fenno, *The Power of the Purse* (Boston: Little Brown, 1966).

an external environment that over time becomes stable in its internal and external relationships.

He opposes the view that committees are virtually autonomous because the internal system of the House Appropriations Committee is comprised of and governed by what he terms an elaborate "esprit de corps." Additionally, its members – like all politicians – seek to increase and maximize their influence. Fenno defends his position that decision making patterns may be explained by highlighting two basic variables: (a) the degree of external support received – especially that which is received from the parent chamber; and (b) the degree of confidence developed by the Committee in the agency as a result of the committee-agency interaction.[10]

Another insightful book that examines the legislative process in America is Paul Light's *Forging Legislation.*[11] Through his exclusive examination of a single bill -- that which raised the Veterans Administration to a cabinet level agency, i.e., the Department of Veteran's Affairs -- Light argues that establishing public policy is the primary objective of the congressional agenda.

Forging Legislation is a case study on "how a bill becomes law." It details an eleven-step process commencing with agenda setting to the final passage. He states that coalition building activities are central to congressional policy making and that congressional staffers play an integral role in setting the agenda for a bill in addition to doing the bulk of the work in the conference committees.

[10] Ibid.

[11] Paul Light, *Forging Legislation* (New York: W.W. Norton and Company, 1992).

Although Light attempts to theorize the legislative process, he contributes a thoughtful typology of six senatorial decision making styles. Specifically, they are: (a) the rational actor; (b) the universal teacher who is in constant pursuit of the imperfect search for truth; (c) the business tycoon who plays the part of policy entrepreneur; (d) the medieval warrior who seeks to exercise raw political power in search of total victory; (e) the small town neighbor who trades favors and makes decisions based on a friendly give and take approach; and (f) the garbage collector who uses a bill to see other issues through that would have never passed on their own merits.

Michael Malbin's book, *Unelected Representative: Congressional Staff and the Future of Representative Government,*[12] provides an overview of the effects the increase in size, influence, and power of congressional staffs have on the legislative process. Malbin raises two very important questions. First, have the elected representatives of Congress delegated too much power to their staffs? Second, is the Congress better informed today than it was thirty to forty years ago?

Malbin argues that the size of congressional staffs has measurably increased over the years as Congress attempts to redefine its goals and meet the needs of its constituents. These newly defined goals include, but are not limited to, being less dependent on the executive branch and interest groups, being more vocal and visible on issues of national import, obtaining control of the ever expanding and growing workload, and ensuring that the media plays a more visible role in the political process.

[12] Michael Malbin, *Unelected Representative: Congressional Staff and the Future of Representative Government* (New York: Basic Books, 1980).

Further, Malbin maintains that members of Congress -- in order to be successful in the legislative making process -- need to ensure that they receive a continuous flow of information and requisite time to digest information received. In this light, however, it has been observed that large congressional staffs have at times been more of a detriment to the Congress because they have created serious managerial challenges in the distribution of information. Malbin further argues that to improve the accuracy of information does not necessarily result in a Congress capable of digesting and acting on it accordingly. Thus, it is a major function of the congressional staff to make it possible for the members to do so.

2. A Review of the Related Literature on the Role of the Executive Branch in the Development of Presidential Decision Directives.

This section provides a general overview of the President's use of executive directives. As a prerequisite, this section will discuss the sources of presidential authority in this area, the historical practices relative to its use, and a legal framework of analysis where applicable in order to complete the discussion.

In studying the writings of Baron de Montesquieu, the Founders of the United States Constitution and other political philosophers and writers of their time endeared a great gift to the people of the United States -- the inclusion of separation of power principles in the United States Constitution. Much debate, discussion, and careful explanation was given this subject in *The Federalist Papers*[13] and during the lengthy debates over its ratification.

The United States Constitution provides clear guidance on the president's scope of authority in issuing directives.[14] Additionally, Harold C. Relyea in a Congressional Research Service report titled *Presidential Directives: Background and Overview* provides an excellent historical perspective on the issuance of presidential directives in the United States, commencing with George Washington's directive to holdover officers of the Confederation government.

In his general order, Washington asked each of the holdover officers to prepare a report "to impress me with a full, precise, and distinct general idea of the affairs of the United States" for which they were individually responsible.[15] President Washington's directive may be viewed as having been proper, within his realm of authority -- according to the U.S. Constitution -- and the precursor of the executive order.[16]

The more explicit references or sources of presidential authority in this area may be found in the U.S. Constitution. Whereby -- barring congressional action -- the President

[13] Clinton Rossiter, ed., *The Federalist Papers* (New York: Penguin Group, 1961).

[14] U.S. Constitution, art. 2, sec. 2.

[15] Harold C. Relyea, "Presidential Directives: Background and Overview," Congressional Research Service, *CRS Report for Congress* no. 98-611 GOV, July 16, 1998, p. 1, citing from John C. Fitzpatrick, ed., *The Writings of George Washington*, 80. (Washington, D.C.: U.S. Government Printing Office, 1939) : 343-344.

[16] U.S. Constitution, art. 2, sec. 2, col. 1 ("The president...may require the opinion, in writing, of the principal officer in each of the executive departments, upon any subject relating to the duties of their respective office.")

may, for example, recommend a national holiday as he sees fit. [17] Historically, however, Congress has gone further than the President in passing laws issuing a particular government holiday and/or granting federal employees with paid leave.

Presidential proclamations or orders have historically had a legally binding effect as well. Authority for these decisions, however, is derived from either the Constitution or statutory delegations. Relyea gives relevant examples of statutory authority, for example, citing President Washington's proclamation during the Whiskey Rebellion.[18] William J. Olson and Alan Woll aid in this discussion by citing the "Christmas Proclamation" issued by President Andrew Johnson – where he pardoned "all and every person who directly or indirectly participated in the late insurrection or rebellion" related to the Civil War. [19]

The Supreme Court subsequently ruled in *Armstrong v. United States* that Johnson's proclamation was a "public act of which all courts of the United States are bound to take notice, and to which all courts are bound to give effect."[20] Olson and Woll argue that Johnson's Christmas Proclamation demonstrates the authority of the President to issue written directives without having to rely on expressed language of the Constitution granting him power to issue such directives. Thus, the Executive may utilize additional authority that is "implied" or "inherent" in the issuance of such orders.

[17] Relyea, *Presidential Directives*, 1. (George Washington's proclamation that urged the American people to recognize Thursday, November 26, 1789, as a national day of thanksgiving.)

[18] Ibid., 13.

[19] William J. Olson and Alan Woll, "Executive Orders and National Emergencies, Cato Institute, *Policy Analysis,* no. 358, (October 28, 1999) : 9.

[20] *Armstrong v. United States*, 80 U.S. 154, 156 (1871).

The research will refer to some cases[21] that have questioned, challenged, or argued against a President's use of directives. Calling into question the legitimacy relative to the uses of presidential directives may be found and best understood through the examination of the functions of the president as stated in the U.S. Constitution. Thus, the following presidential functions were utilized to establish a framework from which to examine the case law that questioned and/or challenged presidential directives in the past.

1. Commander-in-Chief[22]
2. Head of State[23]
3. Chief Law Enforcement Officer[24]
4. Head of the Executive Branch[25].

Arguably, when a president is exercising one of these functions, the scope of his power to issue written directives may be viewed as exceedingly broad.

[21] *Armstrong v. United States*, 80 U.S. 154, 156 (1871); *Myers v. United States*, 272 U.S. 52, 164 (1926); *Public Citizen v. Burke*, 843 F.2d 1473, 1477 (D.C. Cir. 1988); *Morrison v. Olson*, 487 U.S. 654 (1988); *I.N.S. v. Chadha*, 462 U.S. 919 (1983); *U.S. Chamber of Commerce v. Reich*, 74 F.3d 1322, 1332-1337 (D.C. Cir. 1996).

[22] U.S. Constitution, art. 2, sec. 2, col. 1.

[23] U.S. Constitution, art. 2, sec. 2, col. 2; sec. 3.

[24] U.S. Constitution, art. 2, sec. 3.

[25] U.S. Constitution, art. 2, sec. 2.

3. **A Review of the Literature on Threats to Our National Information Infrastructures and the Political Context of Information Warfare.**

With the advancements in technology and the subsequent explosion of information available to anyone with the means, the security of our nation has been placed at additional risk. This section will define the terms 'National Security'[26], 'National Information Infrastructures'[27], and 'Information Warfare'[28] in order to provide a framework from which to discuss the political context and impact of a compromise to our information infrastructures on our national security.

Our national information installations and facilities -- the physical and virtual nerve centers of our country comprise of financial networks, communications networks, government and defense networks, public utilities, and transportation centers -- are the modern equivalent of the engineering marvel of the Roman road networks developed in antiquity. The distinguishing characteristic of exception, however, is in the complex automation of today's infrastructures. This has resulted in additional risks to the security of our nation.

This "Third Wave,"[29] i.e., the Information Age, as defined by Alvin Toffler in his work of the same title, has created an environment where we have become familiar

[26] John J. Weltman, Michael Nacht, and George H. Quester. *Challenges to American National Security in the 1990's* (New York: Plenum Press, 1991), xi.

[27] Ronfeldt, *"Cyberocracy is Coming,"* 243-296.

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

[29] Alvin Toffler, *The Third Wave* (New York: William Morrow and Company, Inc., 1980).

with such terms as bytes, networks, hacker, denial of service, virus (in computer terms), etc. Those who purposefully set out to compromise the integrity of computer systems are arguably, the single worst threat to our automated information systems. Clifford Stoll illustrates this point in his book *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.*[30] Stoll takes us into the world of the computer hacker by tracking hacker activities. Stoll, an astronomer by trade, however not a computer security expert, at the Lawrence Berkeley Laboratory (LBL), discovered a German hacker using the university's computer to access other sensitive databases, i.e., military computers.

Furthermore, during the Gulf War we learned first hand of our inability to protect our computer systems as demonstrated by attacks on Department of Defense computer systems. A Congressional testimony confirmed that during the spring of 1991, computer hackers from the Netherlands penetrated numerous Department of Defense computer sites.[31] A Congressional testimony also indicated that the hackers "modified and copied military information"[32] and that many of the sites were warned of their vulnerabilities but failed to realize the implications or rectify the problems.

The aforementioned examples address unauthorized access and/or compromises to sensitive military information, thereby erecting a breach of security with serious national security implications. In addition, attacks that target information infrastructures with the intent of damaging information flows are of even greater concern because the denial of

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

[31] Congress, Senate, Committee on Governmental Affairs, Jack L. Brock, *Testimony in Hackers Penetrate D.O.D Computer Systems: Hearings before the Subcommittee on Government Information & Regulation,* 102nd Cong., 2nd sess., 20 November 1991.

[32] Ibid.

access to information transfers can have a negative impact on economic markets and bring about economic instability.

Bruce Sterling details the impact of interruptions of service in the telephone system where seventy million phone calls went uncompleted in New York City in 1990. During this period, it was believed that hackers were the cause of the interruption. It was later discovered that programming error was to blame for the failure.[33] The impact of the event was far reaching and bolstered a sense of urgency regarding the development of formal security measures for the phone networks.

In addition to telephone system crashes, Stephen Bowman shared a parallel concern for our nation's electrical systems. These "power grids", Bowman writes, are "divided into four electrical grids supplying Texas, the eastern states, the mid-western states and the northwestern states. They are all interconnected in Nebraska.[34] These grids may be penetrated due to poor security measures causing an adverse effect on the electrical systems of the country as they are "designed to anticipate no more than two disruptions concurrently".[35]

[33] Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (New York: Bantam Books, 1992), 1.

[34] Stephen Bowman, *When the Eagle Screams: America's Vulnerability to Terrorism* (New York: Carol Publishing Group, 1994), 124.

[35] Ibid., 124.

4. **Literature on Public and Private Sector Initiatives to Address Information Infrastructure Vulnerabilities.**

This section discusses the literature on public/private relationships and initiatives that have been forged in order to forestall attacks, such as insertions of viruses in strategic computers, interruption or denial of service attacks, or both; destruction of information and/or compromising the integrity of sensitive information; the concept of information warfare and the impact of this new type of military posturing to our information infrastructures -- that are in many aspects -- linked to private sector networks.

The Bush administration according to a *Federal Computer Week* article by on-line writer Diane Frank has called on the "information technology industry to assist in government efforts to strengthen the state of cybersecurity and is also urging vendors to ensure that what they sell is secure."[36] According to Frank, the Bush administration's cyberspace security advisor, Richard Clarke, reported that several government programs are in the development stages and have been tasked with increasing security within the agencies.[37]

Additionally, the National Science Foundation -- Office of Legislative and Public Affairs, announced in a May 15, 2000 press release a new partnership for the advancement of digital government with a national workshop located in Los Angeles,

[36] Diane Frank, "Clark presses industry on security," *Federal Computer Week*, 5 December 5 2001 [journal on-line]; available from http://www.fcw.com/fcw/articles/2001/1203/web-clarke-12-05-01.asp; Internet.

[37] Ibid.

California.[38] The digital government partnership brings industry researchers -- specifically, from federal, state, and local agencies -- in the field of computer science together to "improve the quality and scope of on-line government services".[39] This partnership will also attempt to address the plethora of problems that now exist as a result of our newly formed "digital government". An important focus of the partnership is to find "ways for the government and citizens to interact more effectively via the Internet."[40]

In recent years the Congress has been taking proactive steps to improve the lines of communication between government and industry. One example of this effort is the August 2001 House hearing where Representative Thomas M. Davis III (R-VA) proposed a "Digital Tech Corps" exchange program between government and industry. Representative Davis' Digital Tech Corps is designed to augment staffs that are under pressure to create technologically advanced government services (i.e., e-government) and better protect federal databases. His proposal won broad support at the house hearing and drew no objections from the head of the General Accounting Office, David M. Walker; Director of the Office of Personnel Management, Kay Coles James; or the head of the General Services Administration, Stephen Perry.[41]

[38] National Science Foundation, [press release on-line] (NSR PR 00-31, 15 May 2000); available from http://www.nsf.gov/odlpa/news/press/00pr0031.htm; Internet.

[39] Ibid.

[40] Ibid. (Quote: Yigal Aren, Conference Chair of the dg.o 2000 workshop and Co-Director – National Science Foundation's Digital Government Research Center.)

[41] Congress, House, Committee on Science and Technology, *Digital Tech Corps*: *Hearing before the Committee on Science and Technology*, 102nd Cong., 2nd sess., October 1991.

Theoretical Framework

This study employs the "Systems Model"[42] designed by David Easton and the "Legislative System Configuration Model"[43] created by Malcolm Jewell and Samuel Patterson for the theoretical framework. Additionally, the "Legislative Role Orientation Model" will also be utilized as a method to study the flow of influence targeting the legislative branch. Utilization of these models as the theoretical framework is noteworthy because it is through these models that our understanding of the political system, legislative process, and the relationship between the executive and legislative branches is enhanced.

Oran Young, in Systems of Political Science,[44] asserts that David Easton's "Systems Approach Model" is still considered a contemporary model and therefore is valid today. He describes it as the most inclusive model used by political scientists and one that is applicable and relevant in studying the nature of political systems.

David Easton's "Systems Approach Model" is selected because of its ability to provide an exhaustive examination of political systems versus viewing each of these systems in isolation. Further, this model enables the researcher to analyze the entire political system relative to the activities and inter/intra relationships between and amongst the respective subsystems. For example, the president and his advisors in the development of PDD 63, Congressional Committees relative to the hearings held that

[42] David Easton, *A Framework for Political Analysis,* 2nd ed. (Chicago: The Chicago University Press, 1979).

[43] Malcolm Jewell and Samuel Patterson, *The Legislative Process in the United States* (New York: Random House, 1977).

[44] Oran Young, *Systems of Political Science*

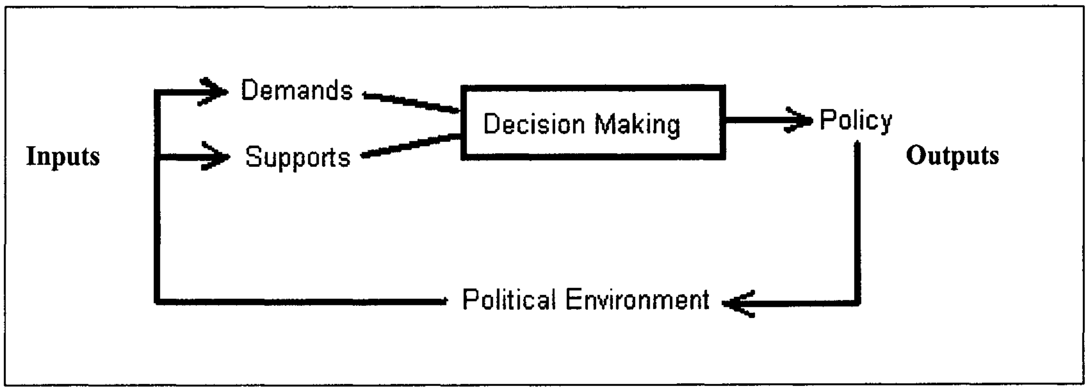
helped lay the foundation for the 1987 and 1997 Acts, the intelligence community and the roles they play in advising both the Congress and the president, members of the Cabinet, and interest groups -- namely industry and private sector groups appearing before and communicating with members of Congress -- to name just a few.

In understanding the critical role the environment plays in the Eastonian model one quickly learns of the connection between feedback and inputs and their relationship with political authorities. Thus, each subsystem plays a major role in the political process and is regarded as a key component of the model. Viewing this model as one of two conceptual frameworks will enable the reader to become familiar with and gain a thorough understanding of the American political system, the conflict between the branches in policy making, and the role technology plays in further exacerbating the tension that exists between the Congress and the President.

The Eastonian model espouses the view that a political system "will depend upon the capacity of the system to allocate values for the society and assure their acceptance."[45] Easton argues that a political system is comprised of the environment, its input, authoritative conversion, outputs, and feedback. These he suggests are the paramount components of the system. His comprehensive model of the political system shows a linkage of activities between the input and output components, with each component having a specific function. (See Figure 1) Easton argues that the environmental component is comprised of the "intra-societal" and "extra-societal"

[45] Easton, *A Framework for Political Analysis,* 96.

environments. The intra-societal environment is devised of four subsystems, i.e., the ecological system, personality system, biological system, and the social system.[46]



Source: From David Easton, *A Framework for Political Analysis*, 2nd ed. (Chicago: The Chicago University Press, 1965, 1979).

Figure 1. David Easton's Political Systems Model

The extra-societal environment includes the international political systems, the international social systems and the international ecological system. Both of these societal systems impact the input component of the "Systems Approach Model." Further, Easton argues that these environmental influences can have a "decisive effect on the way in which a political system operates."[47]

Inputs, according to Easton, are "the disturbances or influences", which occur in the environment and flow into the political system as demands or supports. They are "articulated statements, directed towards the authorities, proposing that some kind of authoritative allocation ought to be undertaken."[48] An example of this type of input, i.e., demands or supports, may be viewed in the form of congressional hearings. In the case

[46] Ibid., 110.

[47] Ibid., 104-105.

[48] Ibid., 120.

of the Computer Security Act of 1987 and the Computer Security Enhancement Act of 1997, the Committee on Science and Committee on Rules along with the Subcommittee on Government, Management, Information, and Technology, and the Subcommittee on Technology among others, held countless hearings on these two proposed pieces of legislation. Representatives from the private sector -- namely industry and academia -- provided testimony before Congress in an effort to influence the outcome of the legislation. Their "demands and supports" consequently affected the way the laws were crafted and the types of budgetary outlays that were eventually dedicated to the legislations, i.e., outputs.

These articulated statements may be viewed further as statements on a number of issues pertaining to, for instance, "social wants, preference, hope, expectation or desires." Easton argues that conflict is the result of the competition for resources that in turn are directed to the authorities. This dynamic of the political system then acts on these inputs in such a way as to convert the inputs into outputs. The final step is for the outputs to return to the system via the environment or in most cases return back into the system itself directly.[49]

Once inputs are processed and the decision allocation is made, inputs are changed to outputs. Easton perceives outputs to be:

1. Exemplified in the statutes of a legal system
2. Administrative decisions, actions, and decrees
3. Rules and other enunciated policies on the part of the political authority
4. The informal consensus of a clan council, and even favors, and

[49] Ibid., 122.

5. Benefits from authorities.[50]

According to Easton, the impact of inputs on authorities may be summarized in this manner. Outputs are the linkages between authority and the environment. Feedback links outputs to the environment. Thus, the advice, i.e., inputs, President Clinton received from his numerous advisors on national infrastructure vulnerabilities and threats helped him, in his authoritative role as Chief Executive, to develop and deliver PDD 63 to the "environment," i.e., federal agencies, private sector, and the public. Furthermore, the function of feedback is to supply information to the environment and generate new inputs to the decision-makers, i.e., authorities. Additionally, Easton suggests that any environmental influence affects both the input and the output components of the system. Thus, within a political system influences occurring result in outputs called "within put."[51]

This cyclical process is a function of demands, e.g., testimony provided to congressional committees by citizens, corporations, and senior government officials, and advice given to the President, flowing into the system from the environment in the form of inputs. Because this study examines the policy-making processes of the President and the Congress this model more than adequately illustrates the methodical nature of the decision making process. Inputs, however, may or may not translate into executive and/or legislative outputs. To define the nature of outputs for the purpose of this study is to refer to or employ the making of technology policy and the subsequent implementation

[50] Ibid., 126.

[51] Ibid., 114.

of those policies, legislation, Executive Orders, and international agreements, among others.

Easton's Systems Approach Model is pertinent to this study and the analysis utilized herein because it thoroughly examines the critical components of a political system, i.e., the environment, inputs, outputs, feedback, and authoritative conversion and the role each plays in the political system. Although the Eastonian model may be perceived as broad in scope it, nonetheless, provides a useful framework in which to examine the intricacies of the political system.

In order to narrow the scope or effectively apply a theoretical framework that would utilize the model on a national level, the "Legislative System Configuration" and the "Legislative Role Orientation" paradigms by Malcolm Jewell and Samuel Patterson will be utilized. These paradigms effectively analyze the legislative process and the interrelationship between the president and the Congress, and a host of other actors, in technology policy decision making.

The Legislative Role Orientation Model examines the various actors who filter in and out of the Legislative Configuration System, for example, senior industry executives, academics, business owners, presidential advisors, and many more. In this light, this model is similar in scope to Easton's Systems model. The authors employed a broad approach of Structural-Functional Systems analysis as their primary model of analysis. Decision-making, in the legislature, is believed better understood by examining the institution where the decision making is to occur, according to Jewell and Patterson. Further, they argue that the institution or place where the decision making is set to occur takes place within a legislative system that is part of a "social system in which individuals interact -- from within and without the legislature itself."[52]

The Jewell and Patterson model is significant to this research as a result of the use of concepts such as legislation, legislative system, and legislative process. The authors define a legislature as "the collection of individuals who are elected as members of the formal parliamentary bodies prescribed by National and State Constitutions."[53] Further, administrative agencies, lobbyists, constituents, the President, party leaders, and others play critical roles as advisors to and sources of information for legislative bodies.

A legislative system, Jewell and Patterson state, is comprised of "a number of individuals who interact with each other in a situation that may lead to the achievement of some goals or set of goals defined in terms of culturally structured and shared symbols."[54] Thus, the Legislative System - described by Jewell and Patterson - is a complex system where individuals and groups inside and outside the structure interact to affect change. They further contend that the "goals" and process of "interaction" that occur with a legislative system are auxiliary concepts when examining this type of system.

Additionally, Jewell and Patterson assert that where non-legislative members interact with members of the legislature, this is the point at which the former enters the legislative system.[55] Thus, when representatives of major corporations, for example,

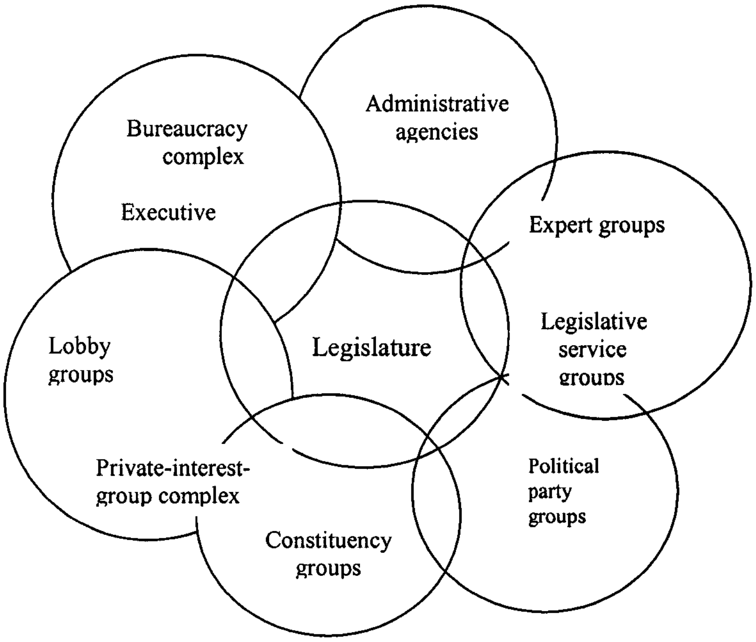
[52] Jewell and Patterson, *The Legislative Process in the United States*, 3.

[53] Ibid., 3.

[54] Ibid., 4.

[55] Ibid., 348.

appear before a congressional committee and provide testimony in favor or against a piece of proposed legislation, for example, it is at that point that they have entered into the legislative system as participants. The executive branch, constituent groups, and political parties, among others, comprise the legislative subsystem and the interaction within this subsystem is part of the framework of the decision-making process. Figure 2 below is a diagrammatic depiction of the Legislative Process system configuration.



Malcolm Jewell and Samuel Patterson, *The Legislative Process in the United States* (New York: Random House, 1977), p. 4.

Figure 2. The Legislative Process System

Jewell and Patterson's flow chart of how demands and expectations from the legislature are changed to influence the eventual output is illustrative of their efforts to expand the concept of the formal legislative system and process model. Thus, the legislature is viewed within the context of a legislative input-output scheme, where the input into the system are the demands made, expectations held, and the support and resources given by the executives, the bureaucracy, interest groups and others.[56] Conversely, the decisions derived by the legislature are the outputs. Decisions include actions taken on bills, resolutions, and policies, the formulation of goals and issues that may not become enacted into laws and services. The feedback loop completes the Jewell and Patterson's Legislative Role Orientation Model.[57]

An additional dynamic of the Legislative Role Orientation Model hinges on the concept of the existence of categories of legislative roles. Jewell and Patterson argue that each category differs in their orientation and function relative to their position at the state or national levels. Thus, the role orientation categories are inclusive of the following:

1. Party Role Orientation
2. Bureaucratic Role Orientation
3. Structural Role Orientation
4. Purposive Role Orientation
5. Representational Role Orientation
6. **Legislative Role Orientation**
7. Interest Group Orientation
8. Constituency Role Orientation
9. Others.

In an effort to further enhance the reader's understanding of each of these aforementioned categories, an analysis of each is provided. It is, however, the Legislative Role Orientation model that is operationalized primarily throughout this study. A detailed examination of the components of this model shows its likeness, however, in greater detail to David Easton's Systems Model.

[56] Ibid., 348.

[57] Ibid., 350.

Within the Party Role Orientation, Jewell and Patterson argue that, legislator's view themselves primarily as a group; wherein, their role is to support their policy preferences irrespective of how they view their particular party loyalties. In addition, legislators view themselves as independent entities and often cross party lines in order to vote with the other Party. Lastly, legislators regard themselves as delegates, representing their constituencies' interests irrespective of their party affiliation.[58]

Jewell and Patterson indicate that in the Bureaucratic Role Orientation category legislators assume the role of presidential spokesperson if they are executive-oriented. Conversely, when legislators are agency-oriented, they consider themselves to be the governmental spokesperson for a particular agency.[59]

Legislators, according to the Structural Role Orientation model, view their roles as relatively expansive. This includes seeing themselves as: (a) experts; (b) leaders; (c) committee members; and (d) friends who have interpersonal relations with fellow legislators and associates.[60]

Purposive Role Orientation reflects lawmakers as having one of five specific or purposive functions: (a) ritualists -- that is there is a fundamental routine-like dimension as part of their work on and with such committees as the Rules and Procedures committee; (b) tribune -- lawmakers regard themselves as advocating popular demands; (c) inventors -- where lawmakers view themselves as creating, formulating, and initiating public policy; (d) brokers -- in this light lawmakers are viewed as compromising,

[58] Ibid., 1.

[59] Ibid., 350.

[60] Ibid., 351.

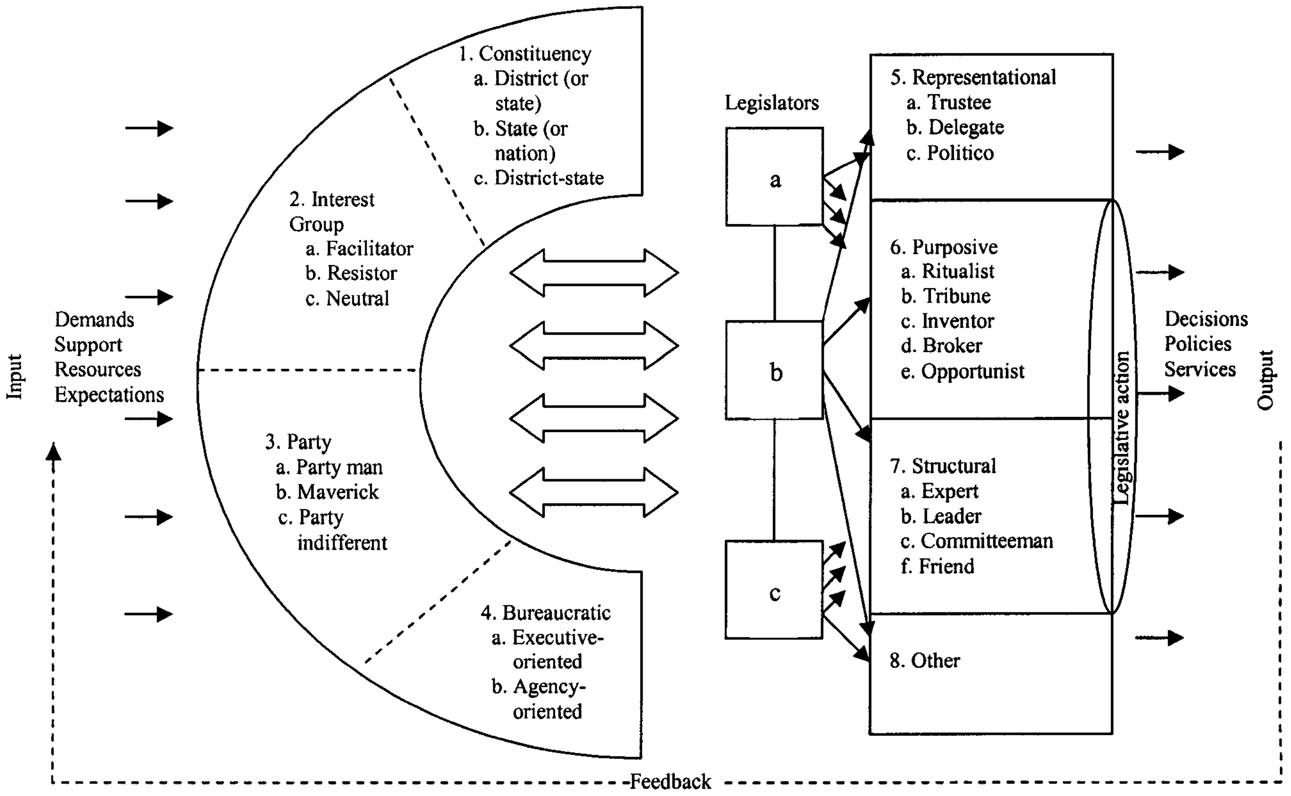
integrating, and coordinating legislation; or (e) opportunist -- where their legislative offices are used to play non-legislative roles.[61]

The Representational Role Orientation model dictates that legislators make decisions based on principle and on their individual consciences when they see themselves as trustee. However, when they view their role as delegates, their decision-making ability entails consultation with constituents and executing the directive of constituents although they may espouse differing points of view. Lastly, although legislators are politicians they may express themselves as both trustees and delegates given the circumstances.[62]

The Legislative Role Orientation model is typically used in highlighting the role of congressional committees and its leaders as well as the executive branch, its agencies, and the role interest groups play in Congress. This model in particular will be useful in depicting how committees receive information and the processes used to render decisions. It is within the utilization of this model that this study is based. The Legislative Role Orientation model is illustrated in Figure 3 below.

[61] Ibid.

[62] Ibid., 350.



Malcolm Jewell and Samuel Patterson, *The Legislative Process in the United States* (N.Y., New York: Random House, 1977), p. 349.

Figure 3. Legislative Role Orientation Model

The Interest Group Orientation model argues that legislators view themselves as: (a) facilitator – where they are considered congenial toward pressure groups whilst being aware of group activities; (b) their role may be viewed as relatively hostile toward interest groups; and (c) they are viewed as being neutral toward interest groups whereby they are neither favorable nor unfavorable toward them or their activities.

In the Constituency Role Orientation model, legislators regard themselves as one of the following: (a) "District Oriented," thereby favoring any legislation viewed as being beneficial to their districts; (b) "Nation Oriented," whereby legislators are concerned with that which affects and effects the entire nation; or (c) legislators who are a combination of both the District and Nation orientation and therefore look toward policies and programs with both a local and national eye and with the same amount of energy.

Lastly, the authors argue that the legislative system is comprised of a network of interrelated roles as depicted in Figure 3 above. Jewell and Patterson suggest that the players, i.e., the executive, legislators, administrative officials, constituents, and party leaders, among others, are all joined together by their involvement in policy formulation and implementation. This relationship, they argue, thereby forms a concentric network of offices, people, and roles and responsibilities.

The aforementioned Systems and Legislative Role Orientation models clearly relate to this study based on their capacity to illustrate the inter- and intra-relationships between and among various groups in the environment and within the legislative system. These models guide the researcher in the evaluation of inputs, i.e., testimonies, advice, lobbying efforts, etc., and the impacts they have on the outputs, i.e., legislation, decision directives, budgetary outlays, and much more. Furthermore, these models have been operationalized throughout this study as a framework for garnering an understanding and practical application of the political process relative to legislative development and passage of proposed bills, and the impacts inputs, feedback, and ultimately outputs have on the environment relative to public policy.

Hypothesis and Research Questions

In quantitative and qualitative research questions, objectives and hypotheses represent specific restatements of the purpose of the study. Further, they are tentative assumptions that may be made for the sake of the investigation. An hypothesis may be defined as "a proposition, condition, or principle which is assumed, perhaps without belief, in order to draw out its logical consequences and by this method to test its accord with facts which are known or may be determined. The role of hypotheses in scientific research is to suggest explanations for certain facts and guide in the investigation of others."[63]

This dissertation will examine the hypothesis that the transition from the Industrial Age to the Information Age, and subsequent technological advancements, have brought about national infrastructure vulnerabilities and threats to national security that require the development of a new paradigm to address the roles of the legislative and executive branches of government. Thus, from this thesis, this study will endeavor to address the following research questions:

1. Has the legislative branch adapted to the transition from the Industrial Age to the Information Age in its ability to develop sound technology policy?

2. Will public policy issues that are not adequately addressed by sound legislation precipitate executive level involvement in order to address the deficiencies?

3. Have technological advancements further exacerbated tensions between the legislative and executive branches of government?

[63] Claire Selltiz, Marie Jahoda, Morton Deutsch, and Stuart W. Cook, *Research Methods in Social Relations* (New York: Holt, Rinehart & Winston, 1951), 35.

4. Will poorly constructed legislation leave the nation's infrastructures at risk of attack?

5. Will infrastructure vulnerabilities brought about by technological advancements necessarily result in public-private information sharing?

Methodology

A descriptive analysis of the decision-making processes that affect both the legislative and executive branches will be utilized in this study. The Eastonian model and Jewell and Patterson models will be used to closely examine and, where applicable, dissect the plethora of actors who comprise the legislative system. Those factors – both external and internal - that influence the Congress and the President, their respective committees and layers of bureaucracy, interest groups, private sector businesses, and public opinion will be analyzed as well.

In an effort to thoroughly examine the activities of major players within the legislative and executive branches, this study will seek to effectively utilize both primary and secondary sources. Thus, primary sources will include congressional reports and records, government publications, congressional testimonies, and speeches. Secondary sources may be listed as pertinent and relevant books, journals, newspapers, and magazine reports.

The use and value of congressional publications cannot be overstated here. Thus, this study will fully utilize the record from Committee and Subcommittee Hearings and the Congressional Record. Examining committee hearings will permit the reader to observe first hand the type of information Congress -- via its designated committees --

receives and how that information is utilized in its decision making role. Further, this study will pay close attention to testimony and hearings conducted before House and Senate committees relative to information gathered in favor of and/or against proposed legislation for enhancing legislative policy on protecting federal computer systems.

An examination of the Congressional Records will provide vital information on House and Senate floor deliberations. Further, the views of key congressional legislators from both sides of the Congress will be extracted from the annals of the Congressional Record. Thus, this research will effectively make use of the subject index in order to determine and evaluate the relevant or pertinent deliberations including "extension of remarks".

An examination of the legislative system and a cursory look at the committee structure and process is important in this research because, as depicted in Jewell and Patterson's legislative models, Congress is at the very nucleus of the legislative system. Further, Christopher Deering -- in his book, Congressional Politics[64] -- states that although it is important and relevant to study the legislative system via Congress it is equally as important to study the complex nature of congressional committees. Committees, Deering contends, are the clearinghouses and vehicles through which legislators plot strategies for creating and passing bills, build coalitions, negotiate, compromise, and much more in order to achieve their goals and meet the needs and expectations of their constituents.

[64] Christopher Deering, *Congressional Politics* (Illinois: The Dorsey Press, 1969).

The Journals from which information is extracted show the role that technology has played and is playing in national security and in the protection of our nation's critical infrastructures. These periodicals include such publications as the Congressional Quarterly, Congressional Quarterly Almanac, Congressional Digest, Journal of Homeland Security, National Journal, Science and Technology. These journals also contain useful information relative to the daily activities of congressional committees and subcommittees in both the House and Senate. In addition, these publications also cover presidential actions and involvement, in particular, and the interrelationship between the branches.

The role of the executive branch as policy initiator and policy maker in the legislative process is equally as important to this study. Richard Neustadt in his seminal and highly respected book, Presidential Powers,[65] poignantly states that the executive possesses an enormous amount of power and influence, prestige, and reputation. These assets have been used to influence the legislative process and effect and implement policy changes where needed. The role of the President in shaping, formulating, and implementing technology policy is of critical importance to national security and critical infrastructure protection.

Furthermore, the President's relationship, i.e., influence, with the intelligence community is further exacerbated by his position of power, prestige, and reputation. A review of Presidential addresses, briefings, messages, and speeches regarding the

[65] Richard E. Neustadt, *Presidential Powers* (New York: John Wiley and Son, Inc., 1964).

intelligence community and its role in technology policymaking will serve to shed an even greater light on the role of the executive in this area.

Sources that will be utilized to obtain information and greater insights to presidential viewpoints and directives include: The Weekly Compilation of Presidential Documents and The Congressional Quarterly Report. The Weekly Compilation of Presidential Documents report contains a variety of messages that have been compiled from press briefings, weekly radio addresses, messages, speeches, and other executive correspondence. The Congressional Quarterly Report covers daily congressional activities as they occur.

The role of interest groups cannot be overlooked in this type of study due to the significant role they play in influencing the legislative process.[66] Therefore, the role of interest groups will be examined through the congressional testimony, position papers, scholarly essays and articles.

In addition to the variety of publications mentioned, this study will also peruse publications such as: The Wall Street Journal, The New York Times, The Washington Post, The National Law Journal, Foreign Affairs, and Media Affairs. They are selected because of their vast readership, editorials, and their relatively reliable sources of information. Further, these publications are viewed as reputable, read by members of an elite socio-economic stratum and, tend to reflect the philosophies of policy makers. In addition, they provide daily accounts, developments, and reactions to major policy issues.

[66] Bentley, *The Process of Government.*

The information retrieved from the aforementioned publications will be utilized as required by the study.

Limitations of the Study

This study has been organized to specifically examine the Computer Security Enhancement Act of 1997 and Presidential Decision Directive 63, in terms of their impact on our nation's security. The reader should be advised that this study contains no quantitative analysis as none was conducted during the course of the study. Additionally, this study is confined to the scope of the subject matter addressed herein and makes no effort to address matters that are outside of its scope.

Significance of the Study

This study is a comprehensive analysis of the Computer Security Enhancement Act of 1997 and Presidential Decision Directive 63. By design, the study examines the legislative and executive processes that led to the passage of the Act and the issuance of the Decision. It also examines the inadequacies of the Act and, where applicable, the Decision -- relative to their inability to adequately protect our national security via critical information infrastructures.

As a result, researchers and scholars alike may deduce that the body of this study contributes to the dearth of knowledge that currently exists in the area of political science and technology and specifically the role technology policies have played in the development of legislation with the express purpose of protecting our nation's critical infrastructures and national security as a whole.

Further, this study attempts to address the volumes of disparate literature that does exist in the area of political science and technology by consolidating much of the material into one source. The limited number of literature in this very specialized field -- where one examines the relationship of the advancements of technology on the political system -- warrants further research and thorough examination by political scientists. Thus, this study attempts to make an important contribution in this area.

Chapter II

THE AMERICAN LEGISLATIVE PROCESS AND THE MAKING OF THE COMPUTER SECURITY ENHANCEMENT ACT OF 1997

Historical Background

The history of U.S. technology policy making and its science and technology system may be viewed as an extension of the history of the nation. Beginning with the patent clause in the U.S. Constitution to the most recent scientific discoveries, technological applications, and federal research and development (R&D) programs, science and technology (S&T) have been an integral part of the nation's growth and development. As the colonies grew and developed, so did their scientific and technological innovations.[67] Further, as the nation evolved and advanced so did its science and technology system, achieving its present structure mainly during and immediately following World War II.

After that war the United States underwent a major restructuring of its S&T system from the defense-dominated war effort to what later evolved into the Cold War. There are several reasons for the emergence of this complex system, including:

1. The strength of the nation's defense-related R&D programs
2. The balance between defense and civilian R&D efforts

[67] U.S. Library of Congress. Congressional Research Service, *Federal Research and Developing Funding: A Concise History*, by Richard E. Rowberg, Report 95-1209 SPR (December 15, 1995), 11.

3. The federal role in basic and applied research and development

4. Congressional R&D policy making and legislation

5. Executive branch R&D policy making and management, and

6. Critical national S&T problems and opportunities.

In 1944, President Theodore Roosevelt asked Vannevar Bush, the then director of the Office of Scientific Research and Development, which was responsible for the U.S. wartime R&D effort, to prepare a report on how to exploit the nation's extensive S&T capabilities, consistent with national security secrecy restrictions, in the postwar years. The Bush report, *Science – The Endless Frontier*,[68] was submitted to President Harry S Truman in 1945.

To summarize, the Bush report -- a compilation of four committee reports[69] -- reasoned that, due to the significance of scientific progress in the United States, science was a proper concern for government. It reinforced its position by recalling the enormous contribution of science and technology to the war effort. The conclusion of the Bush report echoed, in part, the finding of a report of the National Resources Committee, that federal support of research was such an appropriate responsibility of the federal

[68] National Science Foundation, *Science – The Endless Frontier,* Vennevar Bush (Reprint, Washington: National Science Foundation, 1980) : 192 (page citation is to the reprint edition).

[69] Bush convened four committees, which submitted their reports to him, they were: the Medical Advisory Committee, the Committee on Science and the Public Welfare, the Committee on the Discovery and Development of Scientific Talent, and the Committee on Publication of Scientific Information.

government that, consequently, might assist the United States in getting out of the Great Depression.[70]

The report suggested that the government "should extend financial support to basic medical research in the medical schools and in universities" and fund "civilian-controlled" military research in support of that conducted by the Armed Services. It also recommended support for the funding of basic research in academia, i.e., in the field of applied research, improving the procedures for hiring and retaining federal scientific personnel, and providing tax and patent incentives to industry. Additionally, the report provided for "a reasonable number" of undergraduate scholarships and graduate fellowships to develop the nation's scientific talent, especially those currently in the Armed Services. Lastly, it recommended the declassification of secret scientific information as quickly as possible.[71]

It also recommended the establishment of a National Research Foundation, which was to be the central scientific agency within the federal government. While consensus was reached on this recommendation by 1945, the two major proponents of the idea -- Vennevar Bush and Senator Harley M. Kilgore of West Virginia -- differed on some important matters, such as whether the new organization should support basic research primarily (Bush's proposal) or R&D generally (as proposed by Senator Kilgore) in furtherance of societal goals.

[70] National Resources Committee, *Research – A National Resource*, 3 vols. (Washington, D.C.: GPO, 1935-41).

[71] Bush, *Science – The Endless Frontier*, op. cit., 5-8

Another significant issue concerned political control of the organization. President Truman levied executive authority by vetoing the first bill because it did not provide for presidential appointment of the director of the proposed Foundation. It wasn't until the 1950s before the aforementioned issues were resolved and the National Science Foundation (NSF) was officially established. While these matters were being debated, however, several other federal R&D agencies were also established – for example, the Atomic Energy Commission and the Office of Naval Research. The R&D responsibilities and capabilities of another agency, namely the National Institutes of Health, were increased. As a consequence, NSF did not become the government's central scientific agency as was originally intended.[72] Notwithstanding its history, the Bush report has played a significant part in the development of science and technology policy making in the United States. Further, the report has been viewed as guidance for federally-funded R&D programs because it established strong support for university-performed basic research, and other postwar technology policies.

While the Bush report laid the ground work for future legislative action, relevant to the development of science and technology policy, future congresses continued to keep their collective fingers poised on the societal pulse of the nation. With advancements in technology and the severe impacts these technologies were having on the missions of government -- for example, the security and privacy of sensitive information in Federal computer systems -- Congress had no choice but to address those matters which were beginning to directly effect and affect its mission by passing some laws. Examples of

[72] U.S. Library of Congress. Congressional Research Service. *Federal Support of Basic Research and the Establishment of the National Science Foundation and Other Research Agencies*, by William C. Boesman, Report 88-456 SPR, (June 28, 1988), 22.

such legislations are the Federal Property and Administrative Services Act of 1949[73], the Brooks Act of 1972[74], the Computer Security Act of 1987[75], the Information Technology Management Reform Act of 1996[76], and the Computer Security Enhancement Act of 1997.[77]

The Making of the Computer Security Enhancement Act of 1997

The evolution of technology policy in the United States is one that when examined closely is as complex as the technologies the policies are designed to protect. From the development of standards for technology to public key cryptography and the security of the data the technology is designed to collect, many government communities

[73] Public Law 81-152, 63 Stat. 377. The most notable aspect of this law is the establishment of the Federal Information Processing Standards (FIPS). These are standards promulgated by the U.S. Federal government – namely the National Institute of Standards and Technology (NIST) a division of the U.S. Department of Commerce - for use by all (non-military) U.S. government agencies and U.S. government contractors, for information technology. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

[74] Public Law 92-582. Also known as the Qualifications Based Selection (QBS) which was enacted on October 18, 1972, and amended the Federal Property and Administrative Services Act of 1949 (Public Law 81-152). It established the General Services Administration (GSA) as the central authority for the procurement process by which architects and engineers are selected for design contracts with federal design and construction agencies.

[75] Public Law 100-235.

[76] Public Law 104-106. Also known as the Clinger-Cohen Act of 1996. It abolished the Brooks Act and established the role of Chief Information Officers in the federal government and formed the interagency Chief Information Officers' Council. The intent of the Act was to improve government performance through the effective application of information technology.

[77] Also known as H.R. 1903.

have fought to obtain "direct control" over the systems and their accompanying standards.[78]

In 1972, when the development of public key cryptography was underway at Stanford University, the Bureau of Standards -- which at the time was also exploring developments in this area -- worked together with the academic community "in the development of appropriate commercial protection systems."[79] Additionally, the National Security Agency (NSA) participated in the development of public key cryptography by making their contributions to the development of the data encryption standard that is now utilized by both the public and private sectors.

During the 1980's, however, NSA and other intelligence agencies -- involved in an effort to secure sensitive government data -- found themselves using systems, e.g., cryptographic systems, for which they had no direct control; a luxury they had grown used to. While their "lobbying"[80] efforts failed, Congress heard the cries of many private

[78] Congress, House, Committee on Science, Whitfield Diffie. H.R. 1903 - The Computer Security Enhancement Act of 1997: Hearing before the Subcommittee on Technology, 105th Cong., 1st sess., Committee on Science, Subcommittee on Technology. June 19, 1997.

[79] Ibid.

[80] Ibid. NSA attempted to secure their position as overseer of a standardized secret cryptographic system via a plan they designed called the "Commercial COMSEC Endorsement Plan". This plan outlined the use of secret cryptographic systems protected in tamper resistant hardware. The result, "Type II" cryptography designed especially for the protection of unclassified yet sensitive government information and all commercial and other information. Additionally, during this period, there was a national security decision directive that would have on its face expanded the authority of DOD over security arrangements throughout the federal government. Collectively, had these two strategies succeeded, they would have effectively recaptured control over cryptography throughout the United States. Congress did not find this appropriate and moved to dismantle the plan via decisive legislation.

interests -- namely from the banking industry[81] -- and responded with the passage of the Computer Security Act of 1987.[82] The Act gave authority to the U.S. Department of Commerce and particularly to the newly renamed National Institute of Standards and Technology (NIST) to develop standards for computer security, network security, and communications security for civilian government communications. Specifically, in part, it also established “a computer standards program within the National Bureau of Standards”, that would “provide for government-wide computer security”, and also “...provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes."[83]

While the efforts of the congress were monumental -- considering the inter- intra-agency firestorm that erupted surrounding this issue -- the provisions of the Act required NIST to consult with NSA, consequently, giving NSA control over NIST’s actions. An examination of the Act reveals a fundamental flaw. Specifically, and by design, the legislation did not provide for the much required resources NIST would need in order to perform its duties. Thus, whereby the newly formed organization received congressional authority it did not receive the requisite resources necessary to do the work it had been enacted to do, independently. The unfortunate consequence of such nebulous legislation -- relative to funding appropriations for NIST -- was the development and promulgation

[81] Ibid. The banking community argued vehemently for a freer, much more openly developed technology.

[82] Public Law 100-235. The Computer Security Act of 1987, enacted January 8, 1988.

[83] Ibid.

by NSA of three federal information processing standards,[84] only one of which was generally accepted by industry, i.e., the digital signature standard. Having three standards caused confusion within the annals of industry and had a negative impact on the prescribed role and function of NIST. Hence, NSA's actions rendered NIST's purpose ineffective.

During the 1980's it became necessary for the development of a data encryption standard, due to the advancements in technology that severely affected the security and privacy of sensitive information in federal computer systems. The National Bureau of Standards received legislative authority and was assigned the responsibility for developing standards and guidelines for federal computer systems with the passage of the Computer Security Act of 1987, known as Public Law 100-235. This legislation was later found to be inadequate, resulting in the enactment of the Computer Security Enhancement Act of 1997 (also referred to as H.R. 1903), which strengthened the authority provided to NIST by the 1987 Act. It specifically provided funds to implement the type of practices and procedures which would ensure that the federal standards setting process remained open to the public -- via input and analysis -- as well as providing technical guidance and assistance to federal civilian agencies on how to protect the nation's electronic information.

The General Accounting Office (GAO) helped renew the emphasis on the security of federal civilian agency systems when they released a series of reports focusing on "high risks" in the federal government. This series of reports underscored information

[84] Ibid. The three federal information processing standards were: digital signature standard, the "secure has algorithm", and the Escrowed Encryption Standard or Clipper Chip.

safeguarding as a government-wide, high-risk issue in need of immediate yet swift attention by both the legislature and the executive branch. To summarize, these reports indicated -- on various levels -- that despite their sensitive and critical functions, federal systems and data were not being adequately protected.[85]

Further, between the period of 1993 and 1996, the GAO issued over 30 reports describing serious information security weaknesses at many of the major federal agencies. In a September 1996 GAO report the auditors reported that during the period of 1994 through 1996 serious information security control weaknesses were reported for 10 of the 15 largest federal agencies.[86] Moreover, for approximately half of these agencies, the weaknesses were repeatedly reported for five years or longer.[87]

With the publication of the GAO high risk reports and the ever present technological changes and advancements occurring during this period, the 105th Congress had no choice but to address these matters via constructive and steadfast legislation.

[85] Examples of these GAO reports include, *Customs Service Modernization: Strategic Information Management Must Be Improved for National Automation Program to Succeed.* GAO/AIMD-96-57, May 9, 1996; *Defense IRM: Critical Risks Facing New Materiel Management Strategy.* GAO/AIMD-96-109, September 6, 1996; *Information Management Reform: Effective Implementation Is Essential for Improving Federal Performance.* GAO/T-AIMD-96-132, July 17, 1996; *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks.* GAO/T-AIMD-96-92, May 22, 1996; *Information Technology Investment: Agencies Can Improve Performance, Reduce Costs, and Minimize Risks.* GAO/AIMD-96-64, September 30, 1996.

[86] The departments and agencies surveyed in the GAO study were: the Departments of Agriculture, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Justice, Labor, Transportation, Treasury, and Veterans Affairs, the General Services Administration, National Aeronautical and Space Administration, Social Security Administration, and Office of Personnel Management.

[87] General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (Washington, D.C.: GPO, 1996), GAO/AIMD-96-110, 24 September 1996.

Congressman James Sensenbrenner (R-WI) was the Chairman of the House Committee on Science and is credited with introducing H.R. 1903 – "to amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass."[88] The bill was later referred to the House Subcommittee on Technology chaired by Representative Constance "Connie" Morella (R-MD).

The House Subcommittee on Technology hosted many hearings in an effort to gather facts, obtain insights, and garner perspectives from interested groups on the issues plaguing the technology industry so as to ensure the production of a worthwhile yet viable piece of legislation. On February 11, 1997, the Subcommittee -- chaired by Representative Morella -- hosted a briefing on the subject of secure electronic communications.[89] They heard testimony from senior managers in the technology industry – specifically, Daniel Geer, Director of Engineering, Open Market, Inc., Cambridge, Massachusetts; Daniel Lynch, Chairman, CyberCash, Redwood City, California; and, Geoff Mulligan, Senior Staff Engineer, Security Products Group, SunSoft, Colorado Springs, Colorado. The subcommittee also heard testimony from members of the academy – i.e., Eugene Spafford, Associate Professor of Computer Sciences, Purdue University, West Lafayette, Indiana and Tsutomu Shimomura, Senior Fellow, San Diego Supercomputing Center, La Jolla, California. Daniel Farmer, an

[88] Congress, House, Congressman Sensenbrenner of WI speaking for the Computer Security Enhancement Act of 1997 to the Committee on Science, 105th Cong., 1st sess., *Congressional Record* 105 243.

[89] Ibid, 17.

independent computer security consultant, also provided testimony before the subcommittee.

An analysis of the testimonies heard at this briefing and at subsequent committee briefings revealed an emphasis on encouraging the Congress to establish sound yet fundamental laws that would permit and "produce the most attractive environment for the electronic world to develop."[90] Daniel Geer (Director of Engineering, Open Market, Inc.) emphasized in his testimony that the developments that were underway in the electronic world had not only begun but they were unstoppable. Therefore, he continued, there was an immediate need for the establishment of rules to ensure and govern this new technologically based environment in which we live. Geer indicated that it was imperative that Congress should provide rules that would not only be well understood but would enable the "game" to develop at its own pace prior to permitting substantial investments in these technologies to produce diverse and conflicting interests. Thus, a proactive congress would surely produce the most attractive environment for the electronic world to develop. Geer further stated that "there is really very little time remaining for Congress to itself choose whether to lead, follow or get out of the way. Where it is crucial that government lead is in setting the rules of the game." He cautioned Congress to "not let anyone make it more complex or argue that we need to go slow or that we first have to let foreign governments or domestic law enforcement catch up. By the time that happens, you will definitely be somewhere between follow and get out of the way."[91]

[90] Ibid., 17.

[91] Ibid., 17-18.

Daniel Lynch (Chairman, CyberCash) likened the pervasive nature of the Internet system to a biological element, where people added value, hopes, and ideas, then waited to see if other people liked them. He argued that while the Internet had considerably lowered the cost of the communication infrastructure, it had also increased the visibility of activity that had once been conducted over dedicated networks. In his testimony, Lynch recommended the elimination of the "old laws" that protected us against the "bad guys," in order to allow Internet business to grow. He indicated his vision of the Internet as an invaluable tool for business in the future and stressed that he did not want this to be lost to foreign markets.[92]

San Diego Supercomputing Center's Senior Fellow, Tsutomu Shimomura, provided examples of communications security problems and testified about the inherent risks that faced Internet users as a result of the evolved system. Tsutomu Shimomura indicated that the average Internet user does not realize the fact that much of his/her data is at risk. He attributed this to the fact that the technologies to better protect users did not exist and a full scale deployment of security technology to protect us from such risks had yet to occur. Daniel Farmer (Independent Security Consultant), like Tsutomu Shimomura, testified on the current state of Internet security. Basing his comments on the widespread security compromise that was caused by the Internet Morris Worm program, Farmer emphasized the need for a paradigm shift among those persons who use computers. This shift, he stressed, would range from a prevailing blindness relative to

[92] Ibid., 18.

information integrity and issues of computer security, to an acceptance of the fact that one must be proactive in the protection of both his physical and virtual property.[93]

Senior Staff Engineer, Geoff Mulligan (Security Products Group, SunSoft), outlined the three major types of security attacks (interception, intrusion, and denial of service)[94] during his testimony and provided a summary of the primary means of protection that existed (i.e., the firewall and the sandbox).[95] He emphasized to the subcommittee that many and varied opportunities existed to violate communication security. He further maintained that protection can only be ensured by "unconstrained" freedom to use any and all available security technologies.[96]

Eugene Spafford, Associate Professor of Computer Sciences at Purdue University, formulated the basis of his testimony on the lack of funding support from both the federal government and industry for education in the area of computer security. Spafford testified that of the 5,500 Ph.D.s granted in computer science and engineering, a scant 16 pertained to computer security. Furthermore, of that number, only 50% were given to U.S. nationals. He respectfully urged the Congress to develop legislation that would provide graduate fellowships that promoted the study of computer security and

[93] Ibid., 18-19.

[94] Mr. Mulligan defined the three major types of security attacks as follows: interception – where one attempts to gain valuable information by monitoring communications; intrusion – a break-in to change or steal information; and, denial of service – interaction that serves to restrict the access to one's own information.

[95] The firewall is a perimeter defense that restricts entry access to a network, yet allows unlimited freedom once inside. The sandbox is an application containment that restricts certain executions from being performed by a user.

[96] Ibid., 18-19.

that would entice graduates to remain in academia upon completion of their degree programs.[97]

While the foregoing persons appearing before the subcommittee agreed that securing the internet from hackers, intrusion, and denial of service attacks should be a primary focus of new and pending legislation, no one testified to the importance of protecting and maintaining the citizen's right to privacy. The development of this type of legislation -- while difficult and complex -- would have without question treaded on an individual's right to privacy.[98] This observation and or link, however, was neither addressed nor broached by members of the subcommittee or those who testified above. As the issue of information security became more predominant in the minds of legislators, business owners, corporations, and citizens, this type of discussion and attempts to address the issue of privacy head on became more prevalent as evidenced by subsequent subcommittee hearings and future legislation.[99]

While much of the testimonies provided to the subcommittee came from representatives of industry and academia in the initial stages, the Honorable Gary Bachula, Acting Under Secretary for Technology, Technology Administration, U.S.

[97] Ibid., 19.

[98] See, William Raspberry's Washington Post article in which he addresses the conflict between protecting the homeland and protecting our rights to privacy. William Raspberry, "Embracing Big Brother," *The Washington Post,* 25 November 2002, sec. A15.

[99] See, for example, the E-Government Act of 2002 (S. 803, 107th Congress, sponsored by Sen. Joseph Lieberman) where a provision of the Act (Section 208) focused on strengthening privacy protections by requiring privacy impact assessments for new systems. This provision calls for assessments any time personal information is collected on 10 or more people. The assessments must address what information is to be collected and why, how it will be used and secured, with whom it will be shared, and requires notice of how consent is to be obtained from individuals.

Department of Commerce, was able to weigh in on the discussion as an invitee at a June 19, 1997 legislative hearing. Mr. Bachula's testimony provided a different perspective – specifically, one that addressed the interests of one of the 15 government agencies. He described a future that would be driven by the electronic capabilities of technology and a technologically informed consumer. This new world, he stated, would require a "reliable, secure and trustworthy environment... We need to have access to public information but also assurance that the wrong people will not have access to classified or private information."[100] This was not an expressed concern of those persons appearing before the subcommittee from industry. Mr. Bachula, in addressing the sections of the bill and speaking on behalf of the Administration, expressed strong support for portions of the bill that augmented NIST's role in assisting the establishment of non-federal public key management infrastructures. He also supported those portions that provided for guidance and assistance to federal agencies. He expressed outright support for Section 5 of the bill and the intent of Sections 6 and 8 were also supported. However, he recommended that the language dealing with these two sections needed improvement.

Dr. Whitfield Diffie, Distinguished Engineer, Sun Microsystems of Mountain View, California, provided testimony based on the historical development of the government's role in computer security. He spoke highly of the intent of the Computer Security Act of 1987. After tracing the development of the relationship between the National Security Agency (NSA) and NIST, Dr. Diffie expressed his satisfaction with the law. He indicated that the provision of the 1987 Act which called for NIST to consult

[100] Congress, House, Committee on Science, *Computer Security Enhancement Act of 1997*: Hearing before the Committee on Science, 105 Cong., 1st sess., *Congressional Record*, 19.

with NSA was later modified by an inter-agency Memorandum of Understanding (MOU). According to him, that law caused the separation of authority and funding whereby NIST maintained the authority for carrying out the intent of the Act while NSA acquired the budget to get the work done. He highlighted the problems caused by the NIST/NSA relationship and argued that NIST required autonomy thereby eliminating the inherent problems. He strongly supported the proposed 1997 Act, stating it would bring back the spirit of the Computer Security Act of 1987.[101]

Despite the foregoing, nearly all of the provisions of the 1997 Act were agreed to -- in whole or in part -- by those persons appearing before the subcommittee. Section 7 of the bill, which proposed to make NIST the department responsible for conducting evaluations and assessing the strength of foreign encryption technologies, received the greatest criticism accompanied by recommendations for improvements and/or change. This department provides guidance to the Department of Commerce in granting export licenses for domestic encryption products. The Acting Under Secretary for Technology, Gary Bachula, articulated the administration's opposition to this section as did Stephen T. Walker, President and CEO, Trusted Information Systems, Inc. of Glenwood, Maryland.

Both men argued strongly against this section because, as Mr. Walker indicated, "no one in government or industry has been able to perform effectively at this point"[102] an evaluation of this sort. While the provision remained in the enacted legislation, it raised concerns relative to NIST's ability to satisfy the requirement based on the following observations:

[101] Ibid., 20.

[102] Ibid., 21.

1. Maintaining existing public-private relationships

2. An unwillingness to effectively share information between the sectors, and

3. An uncertainty as to how the data compiled, evaluated, and reported would be effectively and efficiently utilized.

James Bidzos, President and CEO, RSA Data Security of Redwood City, California, expressed his disagreement with Mr. Walker's contentions regarding NIST's involvement in the evaluation of encryption technologies. He stated that the provisions of Section 7 were not only doable but definitely needed. He went on to praise those portions of the bill's provisions that attempted to increase the role of the private sector in establishing computer security of civilian government agencies. He argued that while implementation of the 1987 Act missed the opportunity for NIST to work closely with industry, "we have an opportunity now to correct it. And, I think that's what [H.R.] 1903 does." In concluding his remarks, Mr. Bidzos found no fundamental shortcomings with the bill, and strongly supported its contents and timing.[103]

Marc Rotenberg, Esq., Director, Electronic Privacy Information Center, Washington, DC, utilized his time before the subcommittee to provide an appraisal of the bill. Citing the merits of the 1987 Act, he indicated his support of the bill as powerful and timely legislation -- that furthers the intent of its predecessor. In addition, he stated, this bill would eliminate the inefficacy induced by NIST's MOU with NSA for consultation on computer security matters under the Act. Rotenberg went on to express the pivotal role the Computer System Security and Privacy Advisory Board (CSSPAB) had played in providing public input into the decision-making process since the passage

[103] Ibid.

of the Computer Security Act of 1987. He emphasized the importance of building on the success of the Board and ensuring that it continued to have the resources necessary to evaluate important concerns about computer security and privacy. In addition to having played a critical role since the passage of the 1987 Act, Rotenberg made clear that the Board continued to provide the critical link between the public user community and the agency.

As his testimony pertained to Section 7 of the bill, Rotenberg was extremely supportive. He stated that the proposed legislation recognized that the United States was not grappling with the issues of data security and privacy in a vacuum. In addition, he noted that advanced knowledge of foreign encryption technologies would enable the Secretary of Commerce to analyze export restrictions while possessing a firm understanding of the availability of strong foreign encryption products. He also expressed his hopes that having an awareness of technologies outside the United States might influence decision-makers to adopt a policy on encryption that would help U.S. computer hardware and software manufacturers to become competitive in the global market place. Rothenberg was encouraged by the bill's framework in that he felt it would ensure a responsive, open decision-making process that would promote technical standards compatible with the interests of civilian agencies and the commercial sector.

Mr. Rotenberg, in his closing remarks, complimented the National Research Council's (NRC) efforts in reviewing cryptography policy in a 1996 report titled 1996 Cryptography's Role in Securing the Information Society. Further, he suggested that the proposed study (Section 12 of the bill) be expanded to include "new techniques to promote privacy and security on-line, techniques to promote anonymous or pseudoanonymous commerce, and communications that are now being explored in other countries." Rotenberg expressed the importance of the NRC to look at privacy enhancing technologies that may enable the growth of electronic commerce on the Internet and strengthen public confidence in Internet communication. While similar work had been completed in other countries, the United States, Rotenberg pointed out, had yet to look closely at the significant opportunities that such technologies provided. He added that a report produced by the NRC which outlined the basic research and policy issues accompanied by some preliminary recommendations would prove useful.[104]

In addition to the live testimony heard above, the subcommittee also received written testimony submitted by the Chair of the Computer System Security and Privacy Advisory Board (CSSPAB), Willis Ware. In his written testimony, Ware recalled reviewing the 1987 Act ten years after its enactment. The CSSPAB heard presentations from a variety of government and private sector representatives who criticized the Act's implementation versus its structure and phraseology. For example, Ware stated that NIST does not provide federal civilian agencies the support they needed to ensure computer security. He suggested that NIST should focus on providing "general system-level security advice and overall assistance to civil agencies," not just technical assistance in implementing standards and guidelines. In June 1997, Ware stated, CSSPAB adopted two resolutions. The first resolution called for NIST to increase its assistance to civilian federal agencies. The second recommended that NIST should develop a repository for data from civilian agencies on computer security and privacy violations. As is the case

[104] Ibid., 21-22.

for all written testimonies submitted to a congressional committee, Mr. Ware's comments were placed on record and his comments were taken into consideration by the members.

Based on the aforementioned testimonies, the most divisive section of the proposed bill was Section 7. In providing a rationale for maintaining the context of Section 7 of the Act, the sub-committee's notes on this section stated the following:

> NIST currently assesses domestic products in its mission to set appropriate federal standards and to assist civilian federal agencies in the area of computer security. By directing NIST to develop standard procedures and tests that can be used by commercial encryption providers whose products are the subject of export restrictions to evaluate the strength of foreign encryption, the bill will allow the Administration and Congress to make informed decisions on criteria for exporting U.S. encryption products.
>
> The Committee believes that providing accurate and verifiable information on the availability of strong security products will also assist U.S. companies to remain competitive in the international market.[105]

As the legislation is examined further, one may surmise that the committee unwittingly created a cleavage in the legislation. The fundamental absence of carefully worded legislation pertaining to methods, mechanisms, and approaches to addressing potential cyber interruptions, manipulations, or corruption of critical infrastructure functions is a clear indication of a Congress that did not consider all areas where technological advancements would have a negative impact on the nations critical systems and networks. Fortunately, however, these matters would be later addressed by the executive branch via Presidential Decision Directive 63 (PDD 63).

[105] Congress, House, Committee on Science, *Computer Security Enhancement Act of 1997*: Hearing before the Committee on Science, 105 Cong., 1st sess., *Congressional Record*, 32.

A careful review of the Congressional Record revealed that the House Committee on Science found the following:

1. The National Institute of Standards and Technology has responsibility for developing standards and guidelines needed to ensure the cost-effective security and privacy of sensitive information in the federal computer systems.

2. The Federal Government has an important role in ensuring the protection of sensitive, but unclassified, information controlled by federal agencies.

3. Technology that is based on the application of cryptography exists and can be readily provided by private sector companies to ensure the confidentiality, authenticity, and integrity of information associated with public and private activities.

4. The development and use of encryption technologies should be driven by market forces rather than by Government imposed requirements.

5. Federal policy for control of the export of encryption technologies should be determined in light of the public availability of comparable encryption technologies outside of the United States in order to avoid harming the competitiveness of United States computer hardware and software companies.[106]

The Committee also indicated the following as the purposes of the Act:

1. Reinforce the role of the National Institute of Standards and Technology in ensuring the security of unclassified information in federal computer systems;

2. Promote technology solutions based on private sector offerings to protect the security of federal computer systems; and

3. Provide the assessment of capabilities of information security products incorporating cryptography that are generally available outside the United States.[107]

[106] Ibid., Section 2, Findings and Purposes.

[107] Ibid.

As the bill began gaining recognition and attention, it became imperative for the White House to become active. The Office of Management and Budget (OMB) quickly expressed its disagreement with Section 7 of the bill. It thereby added more weight to the opposition already stated by Acting Under Secretary for Technology, Gary Bachula, and Stephen T. Walker, President and CEO of Trusted Information Systems, Inc., in their testimonies before Congress. While OMB articulated their appreciation for the support this Act was expected to provide -- via reinforcement of the role of the Commerce Department's NIST office, i.e., the promotion of "strong computer practices" -- it strongly opposed passage of the Act unless it was amended to delete Section 7.[108] The Office of Management and Budget argued, "Section 7 would require NIST to evaluate the foreign availability and strength of encryption technologies subject to U.S. export controls. The regulations that implement U.S. export control policy already provide a mechanism for assessing availability and strength of foreign encryption products."[109] The administration articulated its sensitivity to this provision of the legislation because it was setting the stage for placing "NIST, a non-regulatory agency, in the position of second guessing the existing export control process."[110]

In addition to expressing their dissatisfaction with Section 7 of the 1997 Act, OMB also recommended the deletion of four additional provisions of the Act – specifically, Section 6 (which required NIST to obtain written recommendations from the

[108] Office of Management and Budget, *(House) H.R. 1903 – Computer Security Enhancement Act* (Sensenbrenner (R) Wisconsin and 29 Others) 15 September 1997; available from http://www.whitehouse.gov/omb/legislative/sap/105-1/hr1903-h.html; Internet.

[109] Ibid.

[110] Ibid.

Computer System Security and Privacy Advisory Board (CSSPAB) prior to the submission of proposed standards and guidelines for Federal computer security to the Secretary of Commerce); Section 8 (which prohibits NIST from adopting standards or carrying out activities or policies for the establishment of encryption requirements for use in non-Federal computer systems); Sections 13(a) and 14 (which directed the Under Secretary of Commerce for Technology to promote the establishment of a national standards-based infrastructure to support commercial and private uses of encryption, and to establish a national policy panel for digital signatures).[111]

Although the committee attempted to draft legislation that would address the vast and extenuating needs of the federal government, the results proved to have a limiting effect in ensuring the protection of the nation's critical information infrastructures. The federal government's steadfast move into the technology age and the vulnerabilities of critical systems that accompanied these advancements were not adequately addressed by the legislature. Further, the most efficient approach to ensuring the successful protection of these systems would necessarily require the active involvement of the private sector -- a relationship that could not be coerced or mandated, but one that would have to be collectively genuine in its creation, function, and implementation.

The committee attempted to bring the private sector into the fold via Section 13 of the Act titled *Promotion of National Information Security*. This section required "the Under Secretary of Commerce for Technology to actively promote the use of technologies that will enhance the security of federal communications networks and

[111] Ibid.

information in electronic form; to establish a clearinghouse of information available to the public on information security threats; and to promote development of the standards-based infrastructure that will enable the more widespread use of encryption technologies for confidentiality and authentication."[112]

Thus, while the committee intended for this section to encourage the formulation of a relationship between the public and private sectors based on information sharing and infrastructure protection, the relationship congress envisioned never fully materialized. The Committee's rationale appears below, in part, as cited in the *Committee Report*:

> Through the requirements of section 13, the Committee intends to designate a central government focus for increasing public awareness of the need for improving the security of communications networks and the information accessed through such networks.
>
> The Committee intends that the Technology Administration actively promote the development of a national, standards-based infrastructure to support the uses of encryption technologies for confidentiality and authentication by working closely with the private sector and by assisting and supporting the development of standards through a private-sector oriented, consensus-based process.[113]

A closer reading of the Act partially explains why this relationship was never adequately formed. H.R. 1903 contained no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act of 1995 (UMRA) and would not affect the budgets of state, local, or tribal governments.[114]

[112] Congress, House, Committee on Science, *Computer Security Enhancement Act of 1997, Congressional Record*: 34.

[113] Ibid., 35.

[114] Ibid., 40.

The bill authorized the appropriation of $3.2 million to NIST to: (1) enable the Computer System Security and Privacy Advisory Board (CSSPAB) administered by NIST to conduct public forums to identify emerging issues related to computer security; (2) contract for a study by the National Research Council on computer security issues; and (3) award computer security fellowships.[115] The Congressional Budget Office (CBO) estimated that implementing other provisions of the bill would require expenditures of an additional $33 million over a four year period (1998-2002). NIST received an appropriation of $582 million for Fiscal Year 1997, and its 1997 outlays were approximately $640 million.

The estimated budgetary impact of H.R. 1903 is shown in Table 1 below.[116]

Table 1. Changes in Spending Subject to Appropriation

By fiscal year, in millions of dollars

	1998	1999	2000	2001	2002
Estimated Authorization Level	9	8	7	6	6
Estimated Outlays	7	8	7	7	6

Many technological changes and advancements had occurred between the passage of the 1987 and 1997 Acts which were addressed to one degree or another in the 1997

[115] Ibid., 41.

[116] Ibid.

Act; for example, the proliferation of networked systems, the Internet, and web access. The 1997 Act also provided for increases in security, for example, the widespread use of strong encryption, for federal civilian agencies that based their procurement decisions for computer security hardware and software on the standards set by NIST.

Further, H.R. 1903 promoted the use of commercially available products and encouraged an open exchange of information between the private sector and NIST. However, this dialogue quickly grew into a unilateral exchange and only seemed to occur when the private sector queried NIST.

Although the 1997 Act addressed many of the technological changes and advancements of the period, it was unable to address the protection and security of critical information infrastructures that have a direct impact on our national security needs. The legislation did not attempt to develop a national cyber security strategy for the nation or address the matter of protecting the crucial information infrastructures from a national, i.e., public-private, perspective. While the legislation encouraged the formulation of public-private sector relationship it limited the interaction to the development of standards and, where applicable, information sharing.

As a result, the Computer Security Enhancement Act of 1997 -- while it addressed the voids that were prevalent in the Computer Security Act of 1987 -- was inadequate in addressing the vulnerabilities in our national security that were brought about by technological advancements. The onus would now be on the executive branch of government to effect the requisite changes in public policy in order to remove the weaknesses which were now readily apparent in our critical information infrastructures and national computer systems and networks.

The Clinton Administration realized the troublesome inadequacies that pervaded the 1997 Act, the enormous speed at which technological advancements were being made, and the impact these advancements were having on the nation's critical systems and networks. In a proactive attempt to fill the gaps left behind by the Act and the dearth of legislation that existed in this area, President Clinton issued the 1998 *Policy on Critical Infrastructure Protection: Presidential Decision Directive 63.* This presidential decision directive, we will see in Chapter 3, played a significant role in re-shaping technology policy going into the 21st Century, i.e., the Information Age. Furthermore, it forced the Congress to make the requisite adjustments in the way they formulated technologically based legislation, i.e., computer related, information focused, technologically driven laws.

Chapter III

THE ROLE OF THE EXECUTIVE IN THE DEVELOPMENT OF EXECUTIVE ORDERS AND PRESIDENTIAL DECISION DIRECTIVES

As this great nation began to develop and formulate the foundations of the laws under which we live, U.S. Presidents established and implemented a variety of presidential or executive directives. The most common of these are executive orders and presidential proclamations. At the core of these edicts, presidential directives are written instructions or declarations issued by the Executive. They are official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government. The President, therefore, is not limited solely to oral instructions and declarations but, as has become the practice for every president, the use of the written directive has become one of many vehicles used to run this most coveted office.

The text of executive orders appears in the daily Federal Register, as each Executive order is signed by the President and received by the Office of the Federal Register. In addition, the text of Executive orders beginning with Executive Order 7316 of March 13, 1936, also appears in the sequential editions of Title 3 of the Code of Federal Regulations (CFR).

The Origins of Executive Orders and Presidential Directives

Three months after George Washington was sworn in as the first President of the United States -- June 8, 1789 -- he instructed officers of the newly formed government to prepare a report "to impress me with a full, precise, and distinct general idea of the affairs of the United States" for which each were responsible.[117] While there is no constitutional or statutory definition of the terms "executive order," "proclamation," or any other form of presidential directive and, no record of the use of the term "executive order" specifically until 1862, Washington's directive is considered the precursor of the executive order as we know it today.

Several months later, Congress formally requested President Washington to "recommend to the people of the United States a day of public thanksgiving."[118] The president of the newly formed United States responded to Congress' request with a proclamation to the people of the United States to recognize Thursday, November 26, 1789, as the day of thanksgiving.[119] Proclamations have been issued by Heads of State commemorating victorious battles and national holidays for centuries. Thus, there was no reason for Congress or the President to conclude that the Constitution removed this ceremonial function from the President as the Head of State. Historically, Congress has gone farther than the President and passed laws establishing federal holidays and granting paid leave to federal employees, for example, but the President is free in the absence of congressional action to recommend such actions at his discretion.

As the country's Chief Diplomat, Presidents have used executive orders to direct and or influence foreign policy since the very first administration of George Washington. It was he who issued a "Neutrality Proclamation" in 1793 stating that the United States

[117] Relyea, *Presidential Directives,* 1.

[118] Congress, *Annals of Congress*, vol. 1, (25 September 1789): 88, 914-915.

[119] Relyea, *Presidential Directives,* 1.

would be “friendly and impartial toward the belligerent powers” of Britain and France. With the issuance of this proclamation, Washington justified his power based on the “law of nations.” Arguably, however, Washington’s justification would have been viewed as more solidly built had he made his argument based on the constitutional powers vested in the President over foreign affairs.

While Washington conferred with and received the concurrence of Secretary of State Thomas Jefferson and Secretary of the Treasury Alexander Hamilton, he did not seek congressional debate on the “Neutrality Proclamation” before issuing it. Many, including James Madison, were openly critical of Washington’s proclamation, stating that it surpassed the level of executive authority vested in the executive and was an outright infringement on congressional authority.

At Washington’s request, Congress later approved his course of action by passing the Neutrality Act of 1794, thereby giving the President the power to prosecute violators of the proclamation. This early example is illustrative of the circumstances under which the President and Congress may have overlapping responsibilities. As a result, the scope of the President's power to act unilaterally is sometimes unclear.

Types of Presidential Directives

There are two fundamental categories in which the two functional types of presidential directives fall. These represent the form and function of the types of directives issued in 1789 by President George Washington. The first category includes documents -- with written instructions from the President (whose audience is primarily executive branch officials) on his expectations of how they are to carry out their duties. Generally speaking, most executive orders fall into this category. The second class addresses a broad group of people, i.e., government officials, the general public, or even foreign governments. In this category the President includes written statements that communicate a presidential decision or declaration. Most presidential proclamations and directives may be identified within this category.

The distinction between executive orders and presidential proclamations is not always clear, especially upon the examination of early presidencies. While in contemporary administrations the calling forth of the militia is customarily achieved by executive order,[120] President Abraham Lincoln, for example, summarily directed much of the early part of the Civil War by presidential proclamation, including a call for the militia. While he may be credited with the issuance of the first formally designated executive order in 1862, he, later that year, ordered federal officials not to return captured former slaves to the states in rebellion in his "Emancipation Proclamation."[121] Lincoln's Emancipation Proclamation ordered the "Executive Government of the United States, including the military and naval authorities thereof, [to] recognize and maintain the freedom of those persons set free by the presidential proclamation."[122]

[120] For example, E.O. No. 13120 (1999) – ordering reserve units into active duty in Yugoslavia. See also, E.O. No. 13119 (1999) – designating Yugoslavia and Albania as war zones.

[121] See the Emancipation Proclamation, September 22, 1862 (original), and January 1, 1863 (final).

[122] Ibid.

Legal Authority: Constitutional and Statutory

Although President Washington's Thanksgiving Proclamation was the first of its kind, other proclamations or orders communicate presidential decisions that have a legally binding effect. Authority for these directives must come from either the Constitution or statutory delegations.

Presumably, the first presidential proclamation occurred on August 7, 1794, when then President George Washington, while calling forth the militia, issued a proclamation ordering those participating in the Whiskey Rebellion to disperse. This official announcement was made pursuant to statutory authority delegated to the President.[123] The statute required the President to first issue a warning to all citizens to disperse and return to their homes, as well as providing that he could call forth the militia to deal with any individual who ignored this command.[124] In this light, the Whiskey Rebellion Proclamation may have been the first directive issued pursuant to legislative authority.

Similarly, President Andrew Johnson issued the "Christmas Proclamation" on December 25, 1868, pardoning "all and every person who directly or indirectly participated in the late insurrection or rebellion" related to the Civil War.[125] Clearly, this proclamation was rooted in his constitutional pardon power.[126] In a subsequent Supreme Court decision, the Court ruled that the proclamation was "a public act of which all courts

[123] Relyea, *Presidential Directives*, 13.

[124] See 1 Stat. 264-265.

[125] Olson and Woll, *"Executive Orders and National Emergencies,"* 9.

[126] U.S. Constitution, art. 2, sec. 2, cl.1 ("The President...shall have power to grant reprieves and pardons for offenses against the United States, except in cases of impeachment.")

of the United States are bound to take notice, and to which all courts are bound to give effect."[127]

The "Christmas Proclamation" demonstrated that the authority of the Executive to issue written directives is not solely limited to that which is expressly outlined in the Constitution. It clearly implies that presidents possess additional authority to issue directives where that is the reasonable implication of the power granted, i.e., implied authority. Conversely, the President also possesses an inherent authority if it is inherent in the nature of the power conferred. For example, the orders -- i.e., oral and written commands -- the President issues as the Commander-In-Chief of the Armed Services necessarily implies that these are duties that are inherent in the nature of the responsibility of a military commander.

The U.S. Constitution expressly outlines the functions of the President relative to his authority to issue directives in the exercise of his constitutional and statutorily delegated powers. Article II, Sections 2 and 3 of the U.S. Constitution provides the President the following guidance in the issuance of Presidential Directives:

As Commander-In-Chief the President's power is limited by other constitutional powers granted to Congress, such as the power to declare war, raise and support the armed forces, make rules (i.e., laws) for the regulation of the armed forces, and provide for calling forth the militia of several states. However, the President's power as military

[127] *Armstrong v. United States.*

commander is still very broad with respect to the armed forces at his disposal, including some situations in which Congress has not acted to declare war.[128]

As Head of State the President is solely responsible for carrying out foreign policy, which includes the main power to recognize foreign governments, receive foreign ambassadors, and negotiate treaties. Congress may enact laws affecting foreign policy, and two-thirds of the Senate must ratify any treaty before it becomes binding law, but Congress must still leave the execution of foreign policy and diplomatic relations to the President.[129]

As Chief Law Enforcement Officer the President has the sole constitutional obligation to "take care that the laws be faithfully executed,"[130] and this grants him broad discretion over federal law enforcement decisions. He has not only the power, but also the responsibility to see that the Constitution and laws are interpreted correctly.[131] In addition, the President has absolute prosecutorial discretion in declining to bring criminal indictments.

As Head of the Executive Branch the Framers debated and rejected the creation of a plural executive. They selected a "unitary executive" and determined that he alone

[128] U.S. Constitution, art. 2, sec. 2, cl. 1

[129] U.S. Constitution, art. 2, sec. 2, cl. 2, and sec. 3.

[130] U.S. Constitution, art. 2, sec. 3.

[131] *Myers v. United States*, 272 U.S. 52, 164 (1926); *Public Citizen v. Burke*, 843 F.2d 1473, 1477 (D.C. Cir. 1988) ("[T]he incumbent President, by virtue of Article II's command that he take care that the laws be faithfully executed, quite legitimately guides his subordinates' interpretation of statutes."). See, Geoffrey P. Miller, *The Unitary Executive in a Unified Theory of Constitutional Law: The Problem of Interpretation*, 15 Cardozo L. Rev. 201 (1993).

would be vested with "[t]he executive power" of Article II. After much debate, the Framers also determined that the President would nominate and appoint (with the Senate's consent in some cases) all officers in the executive branch. With very few exceptions, all appointed officials who work in the executive branch serve at the will and pleasure of the President, even if Congress has specified a term of years for a particular office.[132]

The scope of the President's power to issue written directives is significantly broad when the President is lawfully exercising one of the aforementioned functions. In short, the president has enormous latitude in issuing and/or executing any written directives, orders, guidelines (such as prosecutorial guidelines or nondiscriminatory enforcement policies), communiqués, dispatches, or other instructions he deems appropriate and/or necessary.

The President may also issue directives in the exercise of his statutorily delegated authority. Congress, however, may specify through law that the statutory power may be exercised only in a particular way. There are limits, however, to the lengths Congress can go in attempting to micromanage the President's statutorily delegated power.[133] For example, Congress can grant the President (or his Attorney General) the authority to

[132] See *Myers v. United States*, 272 U.S. 52 (1926) for a detailed discussion of the President's power to fire executive branch officers at will. See also *Morrison v. Olson*, 487 U.S. 654 (1988).

[133] See, Congress, House, *Committee on Rules*: Testimony of Principal Deputy Assistant Attorney General, U.S. Department of Justice, 1992-1993, Douglas R. Cox, before the Subcommittee on the Legislative and Budget Process, Committee on Rules, 106th Cong., 2nd sess., 27 October, 1999, for an insightful discussion of what Congress can and cannot do to limit the President's executive order powers.

deport certain illegal aliens, but it cannot attempt to retain a veto over the final decision as it tried to do in the Immigration and Nationality Act.[134] Thus, the Executive has significant latitude to use written directives when he is lawfully exercising one of his constitutional or statutorily delegated powers.

Legal Analysis

During the early months of the Civil War, President Abraham Lincoln used presidential directives to support the war effort. He presented Congress with the decision to either adopt his practices as legislation or to cut off support for the Union army. On April 15, 1861, after being in office only two months, Lincoln activated troops via presidential proclamation with the intent to defeat the Southern rebellion and for Congress to convene on July 4th. Additionally, he issued proclamations to procure warships and to increase the size of the military. In both cases, the proclamations provided for payment to be advanced from the Treasury without congressional approval. Arguably, Lincoln's actions may be construed as unconstitutional; but facing wartime contingencies, Congress reluctantly agreed and the matters were never challenged in court.

While in office, President Franklin Roosevelt greatly expanded the use of executive orders as well. His exercise of presidential might may be explained in part due to an effort to respond to the growth of government and partly in response to the demands

[134] *I.N.S v. Chadha*, 462 U.S. 919 (1983). In this case, the Court held that Congress's attempt to retain a veto over the statutory discretion of the executive branch violated the constitutional separation of powers.

placed on him during World War II as Commander-In-Chief. Unfortunately, FDR also showed a tendency to abuse his executive order authority and claim powers that were not conferred on him in the Constitution or by statute.[135]

In like fashion, President Harry S Truman followed this pattern of governing by executive order. Much to his credit, however, some of his orders had significant impact in addressing some of the social issues of the period (e.g., the integration of the armed forces.)[136] While others were to his shame, such as the attempted seizure of the steel industry during the Korean conflict.[137]

A true understanding of when a President's executive order is or is not considered valid was developed in a Supreme Court opinion in the "Steel Seizure Case" striking down Truman's executive order.[138] Justice Robert Jackson's famous framework of analysis surrounding this case, in part, follows:

> The President's authority (to act or issue an executive order) is at its apex when his action is based on an express grant of power in the Constitution, in a statute, or both. His action is the most questionable when there is no grant of constitutional authority to him (expressed or inherent) and his action is contrary to a statute or provision of the Constitution.

While the above framework of analysis may be useful as a point of departure, the discussion still requires a substantive knowledge of the relevant statutory law and a

[135] An example is Executive Order (E.O.) No. 9066 which authorized the military internment of many Japanese-Americans during World War II. The executive order was upheld by the Supreme Court based in part on the discretion the Court gave to the Commander-In-Chief.

[136] E.O. No 9981.

[137] E.O. 10340.

[138] *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952).

President's and Congress's constitutional powers. Thus, a review of the substantive law shows why President Truman's desegregation of the armed forces was proper notwithstanding Congress's constitutional authority regarding the military. Congress has the power to create or abolish the military forces, and it has the power to "make Rules for the Government and Regulation" of the military,[139] including the Uniform Code of Military Justice.

Congress' constitutional power permits it to establish standards for the induction of soldiers, including height, weight, and age restrictions. When Congress has acted pursuant to its constitutional authority and its act does not violate any other provision of the Constitution, its rules govern who shall serve in the military, what their pay and retirement age shall be, and more.

Conversely, Truman's executive order authorizing the desegregation of the armed forces did not interfere with any congressional power over induction or any military rules of conduct. President Truman exercised his authority as Commander-In-Chief to lawfully assign individual soldiers in his command to units that he deemed appropriate. Moreover, he also had a constitutional duty to stop government racial discrimination.[140]

Thus, even if Congress wanted to override the desegregation order, it possessed no authority to tell the President how to detail or utilize the soldiers already in his command. This example demonstrates that an application of the legal framework

[139] U.S. Constitution, art. 1, sec. 8, cls. 12-15.

[140] While the Fourteenth Amendment's equal protection clause prohibits only state discrimination, the Supreme Court has determined that this constitutional command applies to the federal government as well.

requires that careful attention must be paid to the underlying constitutional and statutory powers of each branch.

There may be close cases in which the validity of the executive order is uncertain, such as when a claim of inherent constitutional authority is arguable and where Congress has been silent or its will is unclear. Nevertheless, Presidents since Harry S Truman were generally more careful to stay within their constitutional and statutory grants of authority -- relative to the issuance of executive orders -- at least until the administrations of Presidents Richard Nixon and William Jefferson Clinton.

Presidential Proclamations and Executive Orders: An Accounting

Since the administration of George Washington in 1789, more than 7,000 presidential proclamations have been issued. The numbering schema currently in use, however, was not utilized until the early 20th century. Thus, prior to the early 20th century, presidential proclamations were not numbered sequentially and consequently have been assigned numbers retroactively. Newer proclamations, however, are assigned a numerical identifier immediately upon issuance.

Historically, a significant number of modern proclamations may be categorized as ceremonial or hortatory – for example the designation of the Thanksgiving holiday. In more recent historical periods, however, there were two primary exceptions where presidential announcements were more than simply ceremonial, they are: emergency declarations and the land regulations under the Antiquities Act of 1906. An examination of presidential emergency declarations will be discussed later in this chapter.

Initially -- as it pertained to executive orders -- a systematic process for collecting and recording these documents did not exist. Through the eighteenth and nineteenth centuries, each federal agency, i.e., department, kept its own files of orders, and presidential documents. Over a period of time these documents found their way to a variety of places, including the Library of Congress, the National Archives, and individual collections of presidential papers.

In 1905 the State Department created a repository for the collection of executive orders and asked executive branch agencies to submit their individual collections.[141] Two years later, the Department organized this collection of executive orders chronologically, and assigned numbers to each beginning with the earliest one in its files (specifically, the order issued by President Lincoln in October 1862, establishing military courts in Louisiana[142]) and ordering each successive order sequentially. Orders issued since then were assigned new numbers in this series, which is now known as the "numbered series." To this day, executive orders are numbered according to their placement in this sequence.

Admittedly, the numbering system was confusing since officials often discovered old order series well after they had been issued. In these cases the practice was to assign

[141] Clifford L. Lord, "Presidential Executive Orders" *WPA Historical Records Survey* 1, comp. (New York: Archives Publishing Co., 1944): 1.

[142] Ibid.

fractional numbers or letters to orders that could not otherwise be squeezed into the series in the proper sequence. Yet even this record is far from complete, because many orders were issued but not transmitted to the State Department.[143] The original compilation of unnumbered orders contained only 1,500 out of an estimated total between 15,000 and 50,000. There was virtually no difference at all in substance, coverage, or significance between the numbered and the unnumbered series; the sole distinction is that orders that were transmitted to the State Department by 1907 received a number, and those that agencies failed to send over were not numbered. As of December 1999, the numbered series stood at 13,144. There are as many as 40,000 executive orders and proclamations that are excluded from this count.[144]

As the size of the federal government and scope of regulatory authority grew, the inadequacy of the State Department's record–keeping system became glaringly clear. In an effort to address this problem President Hoover, in 1929, issued an executive order (E.O. 5220) requiring all orders to be transmitted to the State Department, but compliance was a significant problem, and the process did not provide anything approaching universal access.[145] As the number of orders began to mushroom, during the first two years of Franklin Roosevelt's presidency, the system collapsed. The American Bar

[143] James Hart, *The Ordinance Making Powers of the President of the United States* (Baltimore: Johns Hopkins University Press, 1925), 318.

[144] Congress, *Presidential Executive Orders and Proclamations*, CIS *Index* (Washington, D.C.): x Clifford L. Lord, ed., "List and Index of Presidential Executive Orders", Unnumbered Series, *New Jersey Historical Records Survey Project* (Newark, N.J.: Historical Records Survey, Works Progress Administration, 1943), v.

[145] CIS *Index, Presidential Executive Orders and Proclamations*, ix.

Association, in a report titled *Report of the Special Committee on Administrative Law*, stated that the problem was that:

> the practice of filing executive orders with the Department of State is not uniformly or regularly followed...Some orders are retained or buried in the files of the government departments, some are confidential and are not published and the practice as to printing and publication of orders, is not uniform. Some orders are made known and available rather promptly after their approval; the publication of others may be delayed a month or more, with consequent confusion in numbering. The comparatively large number of recent orders which incorporate provisions purporting to impose criminal penalties by way of fine and imprisonment for violation is without numerical precedent in the history of the government. [146]

While President Abraham Lincoln is recognized as the father of the executive order, having issued the very first order in 1862, over 13,000 executive orders have been issued since his administration. Figure 4 illustrates the number of executive orders issued by presidents since the Lincoln administration. While the chart is not exhaustive, (i.e., depicting the executive orders issued by all American presidents to date), its purpose is to compare - via graphical illustration - the number of executive orders issued by past and post 20th century presidents. It is clear that early to middle 20th century presidents far exceeded their presidential counterparts of the latter 20th century in the issuance of presidential executive orders.

[146] American Bar Association, *Report of the Special Committee on Administrative Law* (Chicago: American Bar Association, 1934), 214. Cited in Erwin N. Griswold, "Government in Ignorance of the Law," *Harvard Law Review* 43 (1934): 199.

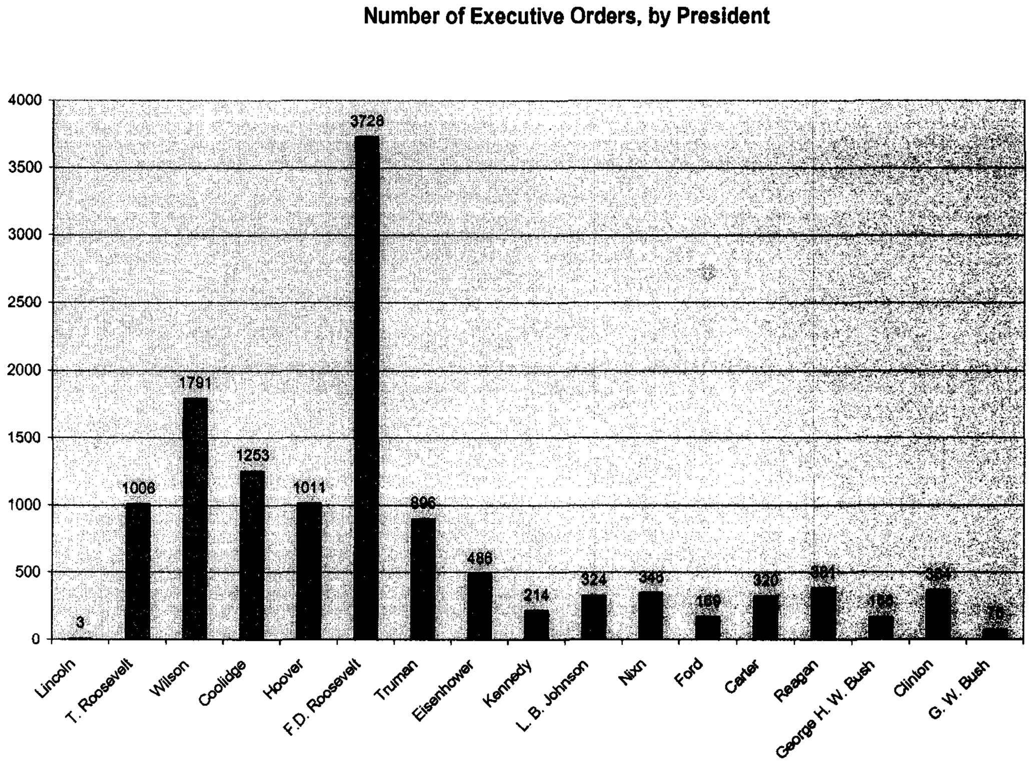


Figure 4. Number of Executive Orders, by President

An explanation may be provided for what appears to be a surge of executive orders during certain periods in American history. One must, however, exercise caution when attempting to draw comparisons of executive orders produced by presidents from different periods perhaps even in the same century. For example, a wartime period is likely to produce a high volume of mobilization orders that are not required in other periods. Thus, during the Second World War, Franklin D. Roosevelt's primary presidential role was that of Commander-In-Chief. As a result of this wartime environment, FDR issued significant numbers of executive orders – specifically, 3,728 during his entire administration (the most of any president past or present).

In addition, the President's National Security Council did not come into existence until 1947. Thus, a majority of the more specialized directives -- that organization's are now responsible for drafting -- were not developed until more recent presidential administrations.

Classifying Executive Orders

In an effort to better understand the nature of executive orders, Kenneth R. Mayer in his book *With the Stroke of a Pen: Executive Orders and Presidential Power*[147] developed a classification guide based on the subject matter of the executive orders. If an order addressed multiple issues or crossed policy lines, Mayer placed these presidential documents into categories that best described the order's primary focus. Thus,

Civil Service: Orders dealing with civil service appointments, retirement exemptions, administration of federal personnel, salary, holidays, and so on. Also included in this category are personnel loyalty orders and any orders dealing specifically with Foreign Service management or personnel.

Public lands: Orders that withdrew land for public use, restored public lands, revoked previous land orders, or that established or altered the boundaries of public lands, migratory waterfowl refuges, or airspace reservations.

War and emergency powers: Orders that created or abolished wartime agencies, addressed the exercise of special wartime administrative functions, took possession or

[147] Kenneth R. Mayer, *With the Stroke of a Pen: Executive Orders and Presidential Power*, (Princeton, N.J.: Princeton University Press, 2001), 80.

control of private economic entities, or established emergency preparedness procedures for federal agencies.

Foreign affairs: Orders dealing with export controls, foreign economic policy, foreign trade, foreign aid, foreign affairs and diplomatic relations generally, establishment of international or treaty-based organizations, management of territories (Philippines, Puerto Rico, the Canal Zone), and immigration.

Defense and military policy: Orders dealing with military personnel, classified information, organization of the intelligence community, administration and reservation of military lands and reservations, defense policy generally.

Executive branch administration: Orders creating boards, commissions, or interagency councils; orders that delegated presidential power or transferred powers from one agency to another, established civilian awards, administered tax policy (including inspection of tax returns), affected the organization of the Executive Office of the President, administered customs, law enforcement, and commemorative orders; contracting.

Labor policy: Orders creating emergency boards and boards of inquiry to investigate labor disputes and orders managing federal government labor policy.

Domestic policy: Orders that dealt with domestic policy generally, including energy, the environment, civil rights, the economy, and education.

Table 2 depicts the distribution of executive orders in a random sample of 1,028 by subject area over a period of time. Overall, from 1936 to 1999, more than 60 percent of the orders dealt with general executive branch administration, the civil service, or public lands. Most of the remaining orders covered the president's foreign affairs and war powers, with a small percentage dealing with domestic and labor policy issues. So, while presidents have used their positions as Chief Executive to impact the affairs of the nation -- albeit positively or negatively via the use of the executive order -- some experts have viewed these acts as abuses and as a violation of the authority vested in the Office of the President.[148]

Table 2. Executive Order Subject Categories by Decade, 1936-1999.

Sample of 1,028

	1936-1939	1940s	1950s	1960s	1970s	1980s	1990s
Civil service	30.5%	21.8%	13.8%	11.9%	22.0%	13.1%	12.0%
Public lands	46.1	18.4	10.5	5.0	2.5	1.0	0.0
War/emergency powers	0.0	19.3	3.3	4.0	1.7	1.0	0.0
Foreign affairs	9.6	7.6	9.9	11.9	10.2	20.2	22.7
Defense/military policy	2.4	12.7	27.6	10.9	6.8	6.1	11.9
Executive branch admin.	10.8	13.6	28.3	36.6	44.9	41.4	36.6
Labor policy	0.0	4.4	5.9	13.9	3.4	10.1	5.3
Domestic policy	0.6	2.2	0.7	5.9	8.5	7.1	9.3
Number of orders in sample	167	316	152	101	118	99	75
Number of administrations	1	2	2	4	3	3	2
Significant orders	1	50	14	14	26	23	21
Percentage	0.6%	15.8%	9.2%	13.9%	22.0%	23.2%	28.0%

Reprinted from Kenneth R. Mayer, *With the Stroke of a Pen: Executive Orders and Presidential Powers* (Princeton, N.J.: Princeton University Press, 2001), p. 82.

[148] Phillip Shaw Paludan, *The Presidency of Abraham Lincoln* (Lawrence: University Press of Kansas, 1994). See also, Forrest McDonald, *The American Presidency: An Intellectual History* (Lawrence: University Press of Kansas, 1994); Joel L. Fleishman and Arthur H. Aufses, "Law and Orders: The Problem of Presidential Legislation," *Law and Contemporary Problems* 40 (1976).

Thwarting Presidential Abuses of Executive Orders

Some scholars have argued that a president's use of executive orders and presidential proclamations stretches his executive authority beyond that of those powers vested in him as the executive and as set forth in the U.S. Constitution. Further, the executive in his use of the executive order, the argument goes, has crossed the line into law making and as a result has violated the constitution. A powerful and poignant example of this type of abuse of the executive prerogative are the actions taken by President Lincoln in 1861 after the outbreak of the Civil War; prior to Congress' convening in July of that year.

President Lincoln ordered a blockade of ports in the South, suspended habeas corpus, increased the size of the army and navy, expended government funds without congressional appropriation, censored mail, and imposed restrictions on foreign travel,[149] though "he had no authority to do these things."[150] Lincoln explained and defended his actions as being legal and that they were required due to the significant danger the Union army faced. Lincoln's actions have long been viewed as "unconstitutional and extralegal",[151] but the federal courts were powerless to enjoin him to comply.

In an attempt to squelch the abuse of the executive in this area, arguments have been presented before Congress to limit the abilities of the executive relative to the issue

[149] Mayer, *With the Stroke of a Pen,* 52.

[150] Paludan, *The Presidency of Abraham Lincoln*, 71.

[151] McDonald, *The American Presidency*, 398-399. Although the federal judiciary in several cases did view these acts as unconstitutional, they were powerless to intercede when Lincoln refused to accept the rulings.

of executive orders. More contemporary examples of such efforts were reflected during the Nixon and Clinton administrations, respectively.

During the administration of President Richard Nixon, Congress attempted to provide a check on the Executive branch's use of the executive order. In 1972 Congress created a special Senate committee -- the Special Committee on the Termination of the National Emergency -- to study the problem of presidential usurpation through declarations of national emergency.[152] During this period, Nixon used his executive position to institute the use of emergency powers to prosecute the Vietnam War; acts that were viewed by Congress as abusive of the executive power.

In order to nullify -- albeit in a less than direct manner -- Nixon's presidential directives, the special committee focused on the states of national emergency that framed many of the most aggressive executive usurpations of power. Two years after its creation a newly re-chartered committee was formed and renamed the Special Committee on National Emergencies and Delegated Emergency Powers. This committee recommended legislation to regulate presidential declarations of national emergencies as well as congressional oversight of such emergencies.[153] The legislation passed unanimously and became known as the National Emergencies Act.[154] It was signed by President Gerald Ford on September 4, 1976.

Two years later -- on September 14, 1978 -- the National Emergencies Act effectively terminated "[a]ll powers and authorities possessed by the President, any other

[152] Congress, Senate, Committee on Government Operations, *National Emergencies Act*: Hearing before the Committee on Government Operations, 3-9.

[153] Ibid., 6

[154] 50 U.S.C. sec. 1601-51.

officer or employee of the Federal Government, or any executive agency ... as a result of the existence of any declaration of national emergency in effect on September 14, 1976."[155] Moreover, the Act stipulated that the president had to declare a national emergency to congress and publish the declaration in the *Federal Register* prior to exercising this extraordinary power. Further, thereafter, the Act cited several provisions relative to the termination of national emergencies -- specifically, either by a joint resolution of Congress or by presidential proclamation.[156]

After the passage of the Act, Congress began focusing on a World War I piece of legislation titled Trading with the Enemy Act (TWEA) originally passed on October 6, 1917.[157] This Act was used by President Roosevelt to close the banks and seize private holdings of gold. In 1977, however, Congress amended TWEA to explicitly state that it may only be applied after a formal declaration of war has been issued by Congress. Shortly after amending TWEA, Congress passed the International Emergency Economic Powers Act (IEEPA);[158] its purpose was to effectively limit the emergency powers of the president when the nation was not at war.

Congress' efforts -- illustrated by the amendments and passages of these acts -- were focused on drawing clear lines of delineation of a check on executive power and on curbing any future abuses by presidents as seen during the Watergate era. Their efforts, however, proved to be futile, because since the passage of the IEEPA there has been an exponential increase in the number of declared national emergencies. For example,

[155] Ibid., sec. 1601.

[156] Ibid., sec. 1622.

[157] 50 app. U.S.C. sec. 5(b)

[158] 50 U.S.C. sec. 1701-6.

during President Clinton's terms in office he used his executive order power to generate multiple concurrent states of national emergency.[159] Some of these declarations, however, as history attests were not at all frivolous in purpose or in scope.

While there is no clear objective standard which defines what constitutes a national emergency, the events of September 11, 2001, proved there are certain circumstances, groups and/or a combination of both that do in fact pose a significant risk to our national security while others, e.g., UNITA, are likely to pose little or no threat.

The president's ability to institute these types of public policy initiatives may at times appear to be an abuse of his power and position while at other times his efforts may be viewed as futuristic and provocative, thereby, assisting the legislature in their quest to develop good sound public laws and policies. The executive's role in this instance, however, is one of policy agent or collaborator, i.e., attempting to fill the void left by the laws created by congress.[160] President Clinton's Presidential Decision Directive 63 is a tangible example of this type of executive involvement.

[159] One example is Clinton's national emergency declarations which enabled him to prevent U.S. residents from providing "humanitarian aid" to a variety of groups his pundits argued he disfavored. For example, UNITA (anti-communist participants in the Angolan civil war who had received support during the Reagan administration). E.O. 12865 (September 26, 1993). As well as certain groups identified as Middle Eastern terrorists – E.O. 12947 (January 23, 1995) -- and Colombian drug traffickers – E.O. 12978 (October 21, 1995).

[160] Fleishman and Aufses, "*Law and Orders: The Problem of Presidential Legislation*," 5.

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63

The 1997 Computer Security Enhancement Act did little to effectively address matters pertaining to critical infrastructure protection and our national security. While the Act served many purposes it fell short of addressing the challenges brought about as a result of the advancements in technology. The *Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* was a gallant attempt at filling the voids left behind by the 1997 Act.

While presidential memoranda and directives typically address issues that are temporary or are used to instruct agency officials to take a specified action in accordance with established regulatory or departmental processes, PDD 63 took the form of an executive order due to its high level of substance and direct presidential involvement. This directive, like an executive order, may be categorized as "presidential legislation"[161] or "executive lawmaking"[162] due to the scope through which it provided President Clinton the ability to make general policy with broad applicability that may be likened to public law.

Presidential Decision Directive 63 built upon the recommendations of the Clinton administration's Commission on Critical Infrastructure Protection. This presidential Commission issued a report in October 1997 which called for a national effort to ensure the security of the nation's vulnerable and interconnected infrastructures. Specifically, these critical infrastructures are those physical and cyber-based systems essential to the

[161] Ibid., 5.

[162] Edwards S. Corwin, *The President: Office and Powers* (New York: New York University Press, 1948), 440n.

basic operations of the economy and government.[163] Thus, they include, but are not limited to, telecommunications, banking and finance, energy, water systems, public and private transportation, emergency services, and important government services.[164]

Many of the nation's critical infrastructures, historically, were systems that were physically and logically independent and had very little interdependence. Due to the advancements in technology and the requirements for performance improvements and efficiency, these infrastructures became increasingly automated and interconnected. The consequence of these technological advancements and the interlinking of these infrastructures was the evolution of new vulnerabilities relative to equipment failures, human error, weather, and other natural causes, physical and cyber attacks.

Addressing the vulnerabilities became the focus of PDD 63 and President Clinton's efforts -- via the policy -- to develop swift, flexible, and evolutionary approaches and methods. The Directive included and encouraged the participation of both the public and private sectors in order to protect both domestic and international security and ward against domestic and international terrorism.

The Clinton presidency was very proactive in this effort. PDD 63 was a culmination of interagency efforts to evaluate those recommendations set forth by the Commission that produced a functional and innovative framework for critical infrastructure protection. Further, although numerous efforts have been made by the Congress to impose some type of legislative framework to direct the formulation of

[163] The White House, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998 (Washington, D.C.).

[164] Ibid., 1.

government information policy historically, they have had little impact on defense and national security information policy formulation, as it continues to remain the exclusive domain of the executive branch. Here we see Clinton's policy directive not only setting a goal of establishing a reliable, interconnected, and secure information system infrastructure by the year 2003, but also setting the stage for significantly increasing security of government systems by the year 2000.

This was to be effectuated by establishing and implementing several significant and requisite elements:

1. Establish a national center to warn of and respond to attacks
2. Develop and ensure a capability to protect critical infrastructures from intentional acts by 2003
3. Address the cyber and physical infrastructure vulnerabilities of the Federal government by requiring each department and agency to work to reduce its exposure to new threats
4. Require the Federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained
5. Seek the voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships
6. Protect privacy rights and seek to utilize market forces. The policy directive was meant to strengthen and protect the nation's economic power, not to stifle it.
7. Seek full participation and input from the Congress.[165]

PDD 63 was the first of many presidential decision directives and other forms of executive involvement to address national security from the perspective of critical information infrastructure security. The intent of President Clinton in issuing this

[165] Ibid.

directive was "to assure the continuity and viability of critical infrastructures"[166] and to "take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[167]

Additionally, PDD 63 made every effort to incorporate the needs, input, assistance, and efforts of the private sector. The order explicitly cited the need for the development of "a public-private partnership to reduce vulnerability."[168] With the understanding that "the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government,"[169] the Clinton administration attempted to invite and to some degree enjoin members of both the private and public sectors to be "genuine, mutual and cooperative"[170] in the fight to reduce the vulnerabilities to critical infrastructures brought about by technological advancements.

Further, the president assumed a less than traditional political party position when he proclaimed that "the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector." This recommendation was without a doubt quite favorable with private sector owners and operators.

[166] The White House, *The Clinton Administration's Policy on Critical Infrastructure Protection.*

[167] Ibid.

[168] Ibid., 2 (Title of Section IV: A Public-Private Partnership to Reduce Vulnerability)

[169] Ibid.

[170] Ibid.

For each of the major sectors of the economy vulnerable to an infrastructure attack, the president recommended the Federal Government to appoint a senior officer from a designated Lead Agency. This individual would act as the Sector Liaison Official to work with the private sector. Additionally, the Sector Liaison Officials -- after working with private sector entities in their infrastructure sector -- would identify a Sector Coordinator or private sector counterpart to represent their sector. Ultimately, these two individuals and the departments and corporations they represent will contribute to a sectoral National Infrastructure Assurance Plan by:

1. assessing the vulnerabilities of the sector to cyber or physical attacks;
2. recommending a plan to eliminate significant vulnerabilities;
3. proposing a system for identifying and preventing attempted major attacks;
4. developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.[171]

In an effort to provide formal guidance to the proposed implementers of PDD 63 and being mindful of the important role the Congress would be required to play in order to assure success, President Clinton outlined a set of ten guidelines in Section V of the directive. In summary, the guidelines stated the following:

1. Consult with and seek input from the Congress on approaches and programs to meet the objectives of the directive.
2. The protection of the nation's critical infrastructures is a shared responsibility between owners, operators, and the government. The

[171] Ibid.

Federal Government shall encourage international cooperation to help manage this global problem.

3. Frequent assessments of the nation's critical infrastructures' reliability, vulnerability and threat environment shall be made in order to ensure that the protective measures and responses taken are robustly adaptive.
4. Federal regulations will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people.
5. The full authorities, capabilities, and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be made available as appropriate in order to achieve and maintain critical infrastructure protection.
6. Privacy rights must be protected and consumers and operators must have confidence that information will be handled accurately, confidentially, and reliably.
7. The Federal Government shall encourage the introduction of increasingly capable methods of infrastructure protection.
8. The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and distribute the results of its endeavors to the private sector.
9. A focus on preventative measures and threat and crisis management is required. It is preferred that voluntary participation by owners and operators in a national infrastructure protection system occurs.
10. Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure program. All critical infrastructure protection plans and procedures must take into consideration the needs, activities, and responsibilities of this population, i.e., state and local governments and first responders.

Presidential Decision Directive 63 was in effect a Critical Infrastructure Protection Management Plan. It was fully equipped with purpose, scope, guidelines, organization and structure, tasking, resource allocation, and a comprehensive implementation schedule. It was, and continues to be, a framework from which owners, operators, and government entities applied their funding resources and human capital to the never ending quest for full and complete critical infrastructure protection.

PDD 63 -- which required the full support of the federal government and an inducement for the voluntary involvement of the private sector -- set the stage for addressing vulnerabilities in our national security and the well being of our nation brought about by global technological advancements. Further, the development and implementation of this "executive legislation" was proactive, futuristic, sound, and well grounded given the numerous and varied threats and attempts at thwarting, penetrating, and/or attacking some of our most critical infrastructures.

Information corruption and cyber attacks on our highly sensitive infrastructures, especially our cyber systems, have become the modern age and contemporary form of war. PDD 63 was this country's first attempt at creating the conditions that would make it possible to win that type of war.

It is against this backdrop that we move on to examine the viable threats, attempted attacks on our national information infrastructures, and the political context of information warfare.

Chapter IV

THREATS TO OUR NATIONAL INFORMATION INFRASTRUCTURES AND THE POLITICAL CONTEXT OF INFORMATION WARFARE.

The Information Revolution

What is the Information Age? In the years that concluded the twentieth century and the beginning of the twenty-first century, many pundits, writers, and analysts began to answer the question. They characterized this period based on the widespread proliferation of emerging information and communication technologies. These technologies have the capability to provide mankind not only with the opportunity to overcome the barriers imposed on communications by time, distance, and location, but to also minimize the limits and constraints inherent in human capacities to process information and make decisions. Advocates of the concept of the Information Age maintain that we have embarked on a journey in which information and communications will become the dominant forces in defining and shaping human actions, interactions, activities, and institutions.

We all sense that the changes surrounding us are not mere trends but the workings of large, unruly forces: the globalization of market, the spread of information technology and computer networks; the dismantling of hierarchy, the structure that has essentially organized work since the mid-nineteenth century. Growing up around these is a new Information-Age economy, whose fundamental sources of wealth are knowledge and communication rather than natural resources and physical labor.

Throughout history, man has needed to communicate and to exchange information. The need for this type of exchange is rooted in a variety of reasons, for example, to sound alarms, to establish a sense of community, to deliver information and news, and much more. In many ways our civilization is based on this intrinsic yet explicit need to communicate and exchange information. Notably, these needs and abilities have always been challenged by such variables as language, distance, time, and/or location.

In an effort to minimize or reduce the challenges caused by distance, time, and location mankind employed a variety of techniques. From the earliest messenger pigeons used by King Solomon to deliver messages as early as approximately 1000 B.C.[172] to the drums, torches, flags, pictographs on papyrus, and the writing on clay and stone tablets, man has continued to improve the mechanisms through which he communicates. While advances in information and communication technologies progressed, albeit slowly, man continues to make the strides needed to overcome the challenges posed by distance, time, and location.

From the mid-nineteenth to the mid-twentieth centuries, several technological advancements -- namely the telegraph, telephone, and radio -- were made in order to enhance man's ability to communicate more expeditiously and extensively. Arguably, this began what may be called the first of two "information revolutions".[173] The first one

[172] Eric A. Havelock and Jackson P. Hershbell, *Communication Arts in the Ancient World* (New York, NY: Hastings House, 1978).

[173] This terminology has been used by leaders of the United States to describe the transition to a knowledge-based economy. Former Vice President Al Gore argued that "we are in the midst of an Information Revolution." Remarks at the Federal-State-Local

commenced in the mid-nineteenth century and lasted for approximately 100 years. The first revolution primarily enhanced communications. Thus, during this period the telegraph, telephone, and radio changed the way we communicate as well as send, receive, and utilize information.[174] Not only did these technologies help transform mankind's ability to communicate, it also transformed the way we lived. Further, in industrial societies, these technological advancements changed the ways in which people related to one another and altered the ways in which businesses, governments, military and foreign policy entities conducted their affairs.

As World War I came to an end, the technologies of the first modern information revolution had, undeniably, had a significant impact on the way people lived and worked. It impacted the way businesses and governments conducted their affairs and, the way wars were fought and peace was pursued. With the ability to communicate less inhibited by the forces of distance, time, and location, people became more aware of that which was happening near and far than they had in the past. With such significant changes afoot, people were able to factor this knowledge into the decisions they made, thereby, changing their perspectives on local, national, and international affairs and the roles they played in them.

Telecommunications Summit, [Online]. (January 9, 1994); available from http//www.whitehouse.gov; Internet. Former President William Jefferson Clinton often spoke of the Information Age. During his presidency he created various working groups and committees, for example the National Telecommunications and Information Administration and the Information Infrastructure Task Force, to develop the foundations for a National Information Infrastructure.

[174] Daniel R. Headrick, *The Invisible Weapon: Telecommunications and International Politics 1851-1945* (New York, NY: Oxford University Press, 1991).

The second modern information revolution began during the mid-twentieth century and extended through the 1980s. During this period, technological developments and advances in television, early generation computers, and satellites helped to link the world together in ways that had never been seen before. These technologies like those of the first information revolution, transformed mankind's ability to communicate, changed the way people interacted and communicated, and altered the way we conducted business, government, and our relationships abroad.

By the end of World War II, the average person had made the connection that information and communication technologies had turned the world into a much smaller place and, arguably, a better one. With television at the helm, early generation commuters, and satellites, the second modern information revolution significantly reduced the impact of distance, time, and location on one's ability to communicate just as much, if not more than the technologies of the first information revolution. This revolution also had enormous impacts on the workplace, economic affairs, culture and society, military affairs, and international relations. The technological advancements of the second information revolution significantly enriched the communications experience.

The technologies of the second information revolution helped accelerate trends towards regionalization and globalization of business as more companies -- during the 1970s and 1980s -- gained access to less costly global communications capabilities. Further, advanced information and communication technologies enabled many firms to broaden their scope and customer base by becoming multinational on either a regional or global basis and hence, the expansion of the multinational corporation (MNC).

The technological advancements of the second information revolution may also be attributed to the role that non-governmental organizations (NGOs) play in international affairs. Many of these organizations have scattered memberships and have consequently become increasingly more active, better coordinated, and significantly more influential as advanced information and communication technologies have become more widely available. Additionally, these technologies have led to the formation of networks among certain NGOs. For example, the Association for Progressive Communication (APC) links approximately 20,000 NGOs and individual members in 95 countries via electronic mail and facsimiles. The APCs membership includes some of the world's most prominent NGOs and related organizations such as Amnesty International, Greenpeace, the Sierra Club, many labor unions, and a host of peace organizations.[175]

As history reminds us somel nation-states did not participate in the second information revolution. Throughout the 1970s and 1980s, the Soviet economy fell further behind the most advanced and technologically sophisticated industrialized democracies of the West and the Far East. One fundamental reason for this economic downturn was the U.S.S.R's unwillingness to participate fully in the second information revolution. Consequently, they were unable to compete against societies with knowledge–based technologies that were integrated into market driven economies. Although former Russian President, Mikhail Gorbachev, recognized this and instituted a set of reforms in the U.S.S.R to address these and other problems,[176] his reforms had unintended consequences. For example, while Gorbachev's reforms were intended to decentralize

[175] Howard H. Frederick, *Global Communication and International Relations* (Belmont, CA: Wadsworth Publishing Company, 1993), 97.

[176] Mikhail Gorbachev, *Perestroika* (New York, NY: Harper & Row, 1987).

the economic decision making process leading to improved production, they instead increased confusion and economic uncertainty. The result was that Soviet production saw a marked decline. Further, where his reforms were designed to encourage popular support for communism by bringing more people into the political decision-making process, they instead led more Soviet citizens to question the system and eventually reject it. While his intentions were to give more Soviet citizens a stake in the system, they instead led to the growth of nationalism and the eventual dissolution of the Soviet Union. The end result, U.S. and Western development of advanced information and communications technologies -- coupled with a closed Russian society and the centralized organizational structure of the Soviet economy -- played a major role in ending the Cold War. Moreover, the Soviet economy proved unable to widely adapt to the changing world surrounding it in the form of the emerging information and communication technologies.

As we embarked on the decade of the 1990s, more information technologies were developed and employed. Some may argue that we are now in a third modern information revolution; one whose focus is on "knowledge" since it encompasses advances in information technologies that significantly alter politics, economics, society, and culture. The notable differences in these revolutions are our increased ability to access, distribute, and store incredibly large quantities of information in very little time. For example, it is now possible to send an entire encyclopedia across the country in approximately two seconds. Access to extremely large quantities of information through electronic communications is a realizable goal any where one has access to a standard phone line or cellular cell. Thus, with this increase in interconnectivity and information resources, the labor force of Alvin Toffler's *Third Wave*[177] nation becomes knowledge-based. Further, as Peter Drucker writes:

> The basic economic resource – "the means of production," to use the economist's term – is no longer capital, nor natural resources, nor labor. It is and will be knowledge. The central wealth making activities will be neither the allocation of capital to productive uses, not labor – the two poles of nineteenth and twentieth century economic theory, whether classical, Marxist, Keynesian, or neo-classical. Value is now created by productivity and innovation, both applications of knowledge to work. The leading social groups of the knowledge society will be knowledge workers and knowledge executives who know how to allocate knowledge to productive use, just as the capitalists knew how to allocate capital to productive use... Yet, unlike the employees under Capitalism, they will own both the means of production and the tools of production.[178]

Daniel Bell shares Drucker's view. He argues that "the crucial point about a post-industrial society is that knowledge and information become the strategic and transforming resources of the society, just as capital and labor have been the strategic and transforming resources of the industrial society."[179]

The key financial institutions of knowledge-based societies also become information-based. Most of the financial transactions within the United States no longer involve the physical transfer of capital or physical representations of money such as gold or currency, but rather the transfer of information. To illustrate, when money is loaned between institutions no physical transfer of funds takes place. Instead, the informational representation of money is exchanged. Information now represents money and "finance

[177] Alvin Toffler, *The Third Wave* (New York, William Morrow and Company, Inc., 1980).

[178] Peter Drucker, *Post-Capitalist Society* (New York: Harper Business, 1993), 8.

[179] David Ronfeldt, "*Cyberocracy is Coming*," 243-296.

no longer has anything to do with money, but with information."[180] Thus, where industrial societies were concerned with the physical protection of capital and providing safe routes for the transport of resources, information societies must be concerned with protecting information and the transfer of that information. Further to this point, where once the destruction of bridges was a threat to the national security of an industrial society, today the destruction of information networks -- especially, those involved with financial transactions -- is the threat.

This is the most significant yet fundamental nature of the conflict that pervades the Information Age. Where the politics of the last one hundred years centered on Industrial Age technology, the politics of the future will be based on Information Age concerns with an orientation towards the storage, protection, and exchange of information in the public and private sectors. Our focus has necessarily shifted toward the establishment of an infrastructure that will be able to support the technological advancements of the Information Age while protecting our national interests.

The National Information Infrastructure

Telecommunications and secured information are of vital importance to the public welfare, national security, and competitiveness of the United States. Rapid advancements in technology in the telecommunications industry and information technology field made it necessary for the United States to establish, monitor, and maintain effective national

[180] Ibid.

and international policies and programs capable of capitalizing on these continued advancements.

Considering the vital role of the information and communication infrastructure, and realizing that telecommunications and information policies had not kept pace with the latest developments in telecommunication and computer technology, the U.S. government determined that there was a need for accelerated deployment of a National Information Infrastructure (NII). The fundamental yet primary objective of this initiative was to facilitate development of a national policy that would encourage competition and the rapid deployment of new technologies. Further, this was expected to provide a regulatory environment in which the private sector would be encouraged to make the investments necessary to build the national information network that the country would require for competing successfully in the future.[181]

The NII may be loosely defined as the physical and virtual backbone of an information society and includes, at a minimum, all of the following:

1. Financial networks: Used for the transfer of information between financial institutions.
2. Private corporate and institutional networks: Used for the exchange of information between international components of the same organization.
3. Public fee accessed networks: Telephone networks and other privately provided communications networks.
4. Cooperative networks: Used to link educational and research facilities for mutual benefit, as is the case with the Internet.
5. Subscription networks: Fee based access to enclosed virtual communities as is the case with America On-line (AOL). Also, increasingly connected to cooperative networks to create large national networks for the exchange of information.

[181] U.S. President, *Technology for America's Economic Growth: A New Direction* (Washington, D.C.: 1993), William J. Clinton, 1993.

6. Government and defense networks: Used for government and defense communications.
7. Department of Defense networks used for Command, Control, Communications, and Intelligence (also known as C3I).
8. Computer reliant public utilities: Power plants, water and sewage, transportation vehicles and traffic systems.
9. Computer reliant technology: Environment and security control in large buildings, chip reliant cars, and a plethora of other conveniences.[182]

The concept of a national data superhighway was first thrust onto the national stage by then U.S. Senator Al Gore (D-TN) in an initial draft of the High Performance Computing Act (HPCA) of 1991 (S. 272).[183] The Gore legislation outlined a plan to link the nation's supercomputing research centers together in a network of high-performance computing. The notion of building a data superhighway to stimulate the U.S. economy was expounded in the Democratic presidential campaign and later became a key component of the Clinton Administration's economic reconstruction policy.[184]

While the U.S. government is generally recognized as having been the initiator of the NII, the private sector may also be credited with playing an active role in this process.

[182] Ronfeldt, "*Cyberocracy is Coming*," 243-296.

[183] Michael Moeller, "Technology: Data Superhighway," *Communications International*, 20, no. 7, (July 1993): 16, 20.

[184] Clifford Stoll, *Silicon Snake Oil: Second Thoughts on the Information Highway* (New York: Doubleday - Dell Publishing, Inc., 1995). Stoll, in contrast to the Clinton Administration, argues "The Internet provides a vast amount of data. But there's a wide gulf between data and information. There's a long distance from information to knowledge. The Internet is a poor place for commerce ... it's missing one critical ingredient. Hint: digital cash won't solve this problem!"

In the early part of 1993, the CEOs of thirteen major U.S. computer companies[185] lobbied for legislation that would extend the government's existing high-performance computing and communications program, the National Research and Education Network, beyond that of government and university laboratories, into offices and homes across the country. These CEOs, who are also members of the Computer Systems Policy Project (CSPP),[186] proposed building a National Information Infrastructure -- a broadband digital network. They also recommended that the government should develop a public information program for the NII and make government data more accessible to the public.[187]

In an effort to improve the HPCA, Congressman Rick Boucher (D-VA) submitted a proposal to the House of Representatives in April 1993 to amend the 1991 HPCA. The result was the High Performance Computing and High Speed Networking Applications Act of 1993[188] which proposed that all schools, libraries, and local government offices should be connected to the Internet. Additionally, it provided for the set up of purely local networks to link various institutions, all of which will be using the information

[185] The thirteen companies were: Apple, AT&T, Compaq, Control Data Systems, Cray Research, Data General, Digital Equipment, Hewlett-Packard, IBM, Silicon Graphics, Sun Micro Systems, Tandem, and Unisys.

[186] CSPP is a leading information technology advocacy organization comprised exclusively of CEOs that develop and advocate public policy positions on trade and technology policy issues. Founded in 1989, CSPP is currently comprised of eight CEOs: Michael Dell, Chair CSPP (Dell Computer), Carly Fiorina (Hewlett-Packard), Christopher B. Galvin (Motorola), Lars Nyberg (NCR Corporation), Lawrence A. Weinbach (Unisys), Joseph M. Tucci (EMC Corporation), Craig R. Barrett (Intel Corporation), and Samuel J. Palmisano (IBM).

[187] Gary H. Anthes, "Industry CEOs Push National Digital Net," *Computerworld*, 27, no.3, (January 18, 1993): 25.

[188] H. R. 1757. This Act is also referred to as the National Information Infrastructure Act of 1993.

superhighway.[189] The Boucher legislation recognized the significance of the High Performance Computing Program (HPCP) and National Research and Education Network (NREN) established by Congress in 1991 and recommended that their scope be widened to include fields other than defense and research. Thus, the new fields would include education, libraries, government dissemination of information, and health care.

The 1993 Act also recommended a coordinated, interagency undertaking to identify and promote applications of the High-Performance Computing Program which was to provide large economic and social benefits to the entire country. Such benefits, as anticipated by the Act, would include new tools for teaching, the creation of digital libraries of electronic information, the development of standards and protocols for making the scores of government information readily accessible by electronic means, and the upgrading of computer systems to improve the delivery of health care.

As a result of the above, Vice President Al Gore and then Secretary of Commerce Ron Brown announced the Clinton Administration's National Information Infrastructure initiative in the fall of 1993. The administration indicated that the growing convergence of telecommunications, information technology, and the entertainment industry called for a revamping of the NII which is also referred to as the Information Superhighway, InfoBahn, or the IWay. Much of the Information Superhighway already existed in the national communications web comprised of fiber-optic strands, coaxial cables, RF, satellites, and copper wire. Notwithstanding this existing infrastructure, both the Congress and the Clinton Administration determined that better policy, organization, and an unencumbered support of the requisite players and stakeholders were needed. As it

[189] Moeller, "Technology: Data Superhighway," 16, 20.

pertained to technology, specifically, however, a need existed for improved access, encryption, protocols, and bandwidth.[190]

In an effort to improve many of the technology related needs noted above and to determine the nature, scope, and breadth of the vulnerabilities and threats to the nation's critical infrastructures -- specifically that of cyber threats -- President Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1996.[191] The Commission was tasked with developing a report for submission to the President on: the vulnerabilities and threats to the nation's critical infrastructures; recommend a comprehensive national policy and implementation plan for protecting critical infrastructures; determine legal and policy issues raised by proposals to increase protections; and, propose statutory and regulatory changes necessary to effect the recommendations.

The Commission presented its report to President Clinton in October 1997. It stated that there was no immediate crisis threatening the nation's infrastructures. The Commission did, however, advise that urgent action should be taken to address the vulnerabilities that were identified in the report. Specifically the PCCIP recommended, generally, that greater effort was required on the part of the private sector and the government relative to the development of greater cooperation and communication between the sectors. Because most of the nation's critical infrastructures are owned and operated by the private sector, it was the Commission's position that the government's

[190] Curtis Chan, "Broadcasters and the IWay," *Broadcast Engineering*, 36, no. 12, (December 1994): 28-32.

[191] President, Executive Order, "Critical Infrastructure Protection," Executive Order 13010 *Federal Register* 16, no. 138. (17 July 1996): 3747-3750.

primary function be in the collection and dissemination of the latest information. Moreover, the government would be expected to collect and spread widely information on intrusion techniques, threat analysis, and ways to defend against hackers -- in addition to and aside from protecting its own infrastructures.[192]

The Commission also proposed an approach for addressing these vulnerabilities:

1. Facilitate greater cooperation and communication between the private sector and appropriate government agencies by: setting a top level policy-making office in the White House; establishing a council that includes corporate executives, state and local government officials, and cabinet secretaries; and setting up information clearinghouses;
2. Develop a real-time capability of attack warning;
3. Establish and promote a comprehensive awareness and education program;
4. Streamline and clarify elements of the legal structure to support assurance measures (including clearing jurisdictional barriers to pursuing hackers electronically); and,
5. Expand research and development in technologies and techniques, especially technologies that allow for greater detection of intrusions.[193]

The Commission's rationale was based on the rapid growth of an increasingly computer-literate population; thereby, implying the existence of a larger pool of potential computer hackers among computer users. Additionally, the Commission reasoned that the inherent vulnerabilities of common protocols in computer networks, the easy availability of hacker "tools" (which are available on many websites throughout the internet), and that the basic tools of the hacker, i.e., computers, modems, and telephone lines, are the same essential technologies used by the general population. This made

[192] President, Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C.: Government Printing Office, October 1997.)

[193] Ibid.

clear to the Commission that there existed a clear threat and vulnerability to our critical infrastructures. Presidential Decision Directive 63 was released in May 1998, upon completion of an intensive interagency review which was conducted in order to garner an understanding of how the government should respond to these issues.

As noted in Chapter 3 of this study, the Clinton Administration along with the Congress realized the significance of the role the private sector has played in the development, maintenance, and use of the nation's critical infrastructures. The practical result of this realization was the passage of legislation, i.e., the Computer Security Enhancement Act of 1997, and the issuance of an executive order, i.e., PDD 63.

As technologies continue to advance and become increasingly more complex our entrée into and presence in the Information Age is solidified. It is our responsibility to now ensure we take all the requisite precautions and steps to protect ourselves, our resources, and our information from the clear and present danger of computer malfeasance such as computer worms, viruses, hackers, threats, and attacks.

Computer Worms, Viruses, and Hackers

During the Clinton presidency, every effort was made to keep an ever present eye on activities involving computer systems that were having an adverse effect on targeted systems. In addition, during the first Clinton administration there appeared an increase in computer viruses and worms[194] as they began appearing more frequently and with

[194] Computer viruses and worms are forms of malicious code used by computer hackers to spread protest messages and are designed to inflict significant damage on target

damaging effects.[195]

The first notable example of a protest use of a computer worm occurred on October 16, 1989, at the U.S. National Aeronautics and Space Administration (NASA) SPAN network. Scientists logging into computers at NASA's Goddard Space Flight Center in Greenbelt, Maryland, were greeted with a banner emblazoned with "Worms Against Nuclear Killers (WANK)". At the time of the WANK attack, antinuclear protestors were attempting to stop the launch of the shuttle that carried the Galileo probe on its initial leg to Jupiter. Galileo's 32,500 pound booster system was fueled with radioactive plutonium. John McMahon, protocol manager with NASA's SPAN office, approximated that the WANK worm attack cost the space agency upwards of a half million dollars in wasted time and resources. More importantly, however, the attack did not succeed in its intended effect of stopping the Galileo launch. Unfortunately, however, the source of the attack was never identified, but some evidence suggested that it might have been the work of Australian hackers.[196]

During the 1990s, threats to computer systems used to propagate political messages that in some cases caused serious damage were being levied both at home and abroad. The media are replete with stories of hackers gaining access to websites and replacing some of the content with their own. Frequently, the messages contained political messages, as when a group of Portuguese hackers modified the sites of forty

computer systems. The code is designed to infect computers and propagate over computer networks.

[195] The distinct difference between the two is that a computer worm is an autonomous piece of software that spreads on its own, whereas a computer virus attaches itself to other files and code segments and spreads through those elements, usually in response to action taken by users, e.g., opening an e-mail attachment.

[196] Ted Bridis, "Hackers Become an Increasing Threat," *Associated Press*, 7 July 1999.

Indonesian servers in September 1998 to display the slogan “Free East Timor” in large black letters. The New York Times reported the hackers also added links to websites describing Indonesian human rights abuses in the former Portuguese Colony.[197]

One year later, Jose Ramos Horta, the Sydney, Australia-based Nobel Laureate representing the East Timor independence movement outside Indonesia, warned that a global network of hackers planned to bring Indonesia to a standstill if Jakarta sabotaged the ballot on the future of East Timor. Horta told the Sydney Morning Herald that more than 100 hackers, mostly teenagers in Europe and the United States, had been preparing the attack.[198] As illustrated by the activities of the Portuguese hackers above, hacker activity and the negative impacts they were causing many domestic and international computer systems became the concern of many individuals and governments alike. News and media agencies have been the most prolific sources for documenting hacker activity and, in many cases, the political impacts of their work.

In February 1999, the London Sunday Telegraph reported that an Israeli teen had become a national hero after he claimed to have wiped out an Iraqi government website. The youth, 14 year old Nir Zigdon, was reported to have said the site “contained lies about the United States, Britain, and Israel, and many horrible statements against Jews.”[199] He further stated, “I figured that if Israel is afraid of assassinating Saddam Hussein, at least I can try to destroy his site. With the help of some special software I

[197] Amy Harmon, “Hacktivists of all Persuasions Take Their Struggle to the Web,” *The New York Times*, 31 October 31 1999.

[198] Lindsay Murdoch, “Computer Chaos Threat to Jakarta,” *Sydney Morning Herald*, 18 August 1999, 9.

[199] Tom Gross, “Israeli Claims to Have Hacked Saddam Off the Net,” *London Sunday Telegraph*, 7 February 1999.

tracked down the site's server to one of the Gulf States."[200] Once the teen accessed the Iraqi website, the Israeli "hacktivist"[201] then sent a computer virus in an e-mail attachment to the site. "In the e-mail message, I claimed I was a Palestinian admirer of Saddam who had produced a virus capable of wiping out Israeli websites," Zigdon said. "That persuaded them to open the message and click on the designated file. Within hours the site had been destroyed. Shortly afterwards I received an e-mail from the site manager, Fayiz, that told me to 'go to hell'."[202]

In June 1998, a group of international hackers calling themselves "Milworm" hacked their way into the website of India's Bhabha Atomic Research Center (BARC) and put up a spoofed web page showing a mushroom cloud and the text "If a nuclear war does start, you will be the first to scream...." The hackers were protesting India's nuclear weapons tests, although they admitted to doing it mostly for thrills. They also indicated that they also downloaded several thousand pages of e-mail and research documents, including messages between India's nuclear scientists and Israeli government officials, and had erased data on two of BARC's servers. The six hackers, whose ages ranged from 15 to 18, hailed from the United States, England, the Netherlands, and New Zealand.[203]

[200] Ibid.

[201] A hacktivist is defined as a person with computer knowledge and skill who converges hacking with activism; where "hacking" is used here to refer to operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software (i.e., "hacking tools"). Hacktivism may include electronic civil disobedience, which brings methods of civil disobedience to cyberspace.

[202] Gross, *Israeli Claims to Have Hacked Saddam Off the Net.*

[203] James Glave, "Crackers: We Stole Nuke Data," *Wired News*, 3 June 1998; Janelle Carter, "Hackers Hit U.S. Military Computers", *Associated Press*, Washington, 6 June 1998; "Hackers Now Setting Their Sights on Pakistan," *Newsbytes*, 5 June 1998.

These types of destructive activities played a significant role in President Clinton's decision to establish the President's Commission on Critical Infrastructure Protection (PCCIP) and the ensuing Presidential Decision Directive 63. These steps helped to address some of the weaknesses inherent in the Computer Security Enhancement Act of 1997.

Military Breaches

Perhaps the best publicized account of a hacker breaking into U.S. military computer systems occurred in 1986 when Cliff Stoll at the Lawrence Berkley Laboratory (LBL)[204] discovered a German hacker using the university's computer to access sensitive databases. Stoll's curiosity was sparked when he found a seventy-five cent error in the LBL accounting system that tracks system usage and then bills the correct party. By exploring the accounting software for the error, Stoll found that a user named Hunter had used seventy-five cents worth of computing time in the last month. He also discovered that Hunter did not have a valid billing address, so he had not been properly charged. Through a lot of work and research, Stoll discovered that Hunter was in fact an intruder, i.e., a hacker using LBL's system to access other systems. Typically, once a discovery such as this was made, the user would have been shut out of the system but, Stoll (an astronomer) not a computer security expert, decided to track the hacker's activities.[205]

[204] The Lawrence Berkley National Laboratory is located on the campus of the University of California at Berkley and operated by the university for the U.S. Department of Energy.

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

When Stoll first reported his discovery of the German hacker, no one in authority believed him. Those in charge of maintaining these sensitive systems were not aware of the hacker's activity, nor did they believe that a hacker had entered their system. Stoll experienced even greater difficulty when he reported his findings to members of the law enforcement community. Although he was able to prove that this was indeed a crime worthy of having the hacker's call traced, his attempts at convincing law enforcement agencies were nearly futile. The German hacker's criminal activities included a break into many military computer installations including the Redstone Missile Command in Alabama, the Jet Propulsion Laboratory in Pasadena, and the Anniston Army Depot. In many of these cases, the hacker successfully gained full access to computer systems and conducted searches for keywords such as stealth, nuclear, White Sands, and SDI.[206] When the files were found the hacker copied them onto his home computer.

The search for the German hacker lasted for nearly a year. The criminal activity was eventually traced to a West German citizen named Markus Hess, a member of a group called the German Chaos Computer Club. He used the pseudonym Pengo and was regarded as one of the best hackers in the Hanover area. His criminal activities, however,

Hacker." *Communications of the ACM,* May 1988. This is an academic paper highlighting the techniques used by Markus Hess to break into the computers.

[206] Katie Hafner and John Markoff, *Cyberpunk: Outlaws & Hackers on the Computer Frontier* (New York: Simon & Schuster, 1991), 172. See also, Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information* (Cambridge: Cambridge University Press, 2001) who makes the argument that the intelligence community is in need of reshaping its intelligence processes from the ground up as we delve further into the Information Age. James L. Tyson, *Target America: The Influence of Communist Propaganda on U.S. Media* (Chicago: Regnery Gateway, 1981).

came to a very abrupt end on February 15, 1990, when he and two of his colleagues were convicted of espionage for selling secrets to the KGB.[207]

The cases mentioned above may be viewed as explicit examples of threats to U.S. national security, especially in the context of the Cold War period. The German Hacker Spy case illustrates how any twenty year old German drug addict can accomplish the work of a sophisticated military spy from an apartment in West Germany. The vast computer networks and less than adequate security of U.S. computer systems give these types of computer savvy criminals the means to gain access to sensitive military information and an opportunity to compromise our national security and national interests.

The inability of the United States to protect its computer systems became glaringly apparent and demonstrated by the attacks on the Department of Defense computer systems during the Persian Gulf War in 1991. Testimony before the Senate Subcommittee on Government Information and Regulation confirmed that during April and May 1991, computer hackers from the Netherlands penetrated thirty-four Department of Defense computer sites.[208] The report states:

[207] Peter J. Denning, *Computers Under Attack: Intruders, Worms, & Viruses* (New York: ACM Press, 1991), 183.

[208] Congress, Senate, Committee on Governmental Affairs, *Hackers Penetrate DoD Computer Systems*: Jack L. Brock, testimony before the Subcommittee on government Information and Regulation, Committee on Governmental Affairs, November 20, 1991. See also, Government Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (Washington, D.C.: 1996) (May 22, 1996) GAO/AIMD-96-84. This is 1996 GAO Report reviewed the extent to which Department of Defense (DOD) computer systems are attacked. The report focused on: (1) potential for further damage to DOD computer systems; and (2) challenges DOD faces in securing sensitive information on its computer systems. In its report GAO found that: (1) DOD

> At many of the sites, the hackers had access to unclassified, sensitive information on such topics as (1) military personnel -- personnel performance reports, travel information, and personal reductions; (2) logistics – descriptions of the type and quantity of equipment being moved; and (3) weapons system development data. Although the information is unclassified, it can be highly sensitive, particularly during times of international conflict. For example, information from at least one system, which was successfully penetrated at several sites, directly supported Operation Desert Storm/Shield. In addition, according to one DOD official personnel information can be used to target employees who may be willing to sell classified information.[209]

The report further indicated that the hackers exploited known security holes to gain access to a majority of these systems. It observed that the Unites States government was aware of them yet it did nothing to close them. The hackers, continued the report, "modified and copied military information," and that many of the sites were warned of their vulnerability but failed to realize the implications. The report concluded with a warning of things to come: "Without the proper resources and attention, these weaknesses will continue to exist and be exploited, thus undermining the integrity and confidentiality of government information."[210]

relies on a complex information infrastructure to design weapons, identify and track enemy targets, pay soldiers, mobilize reservists, and manage supplies; (2) use of the Internet to enhance communication and information sharing has increased DOD exposure to attack, since the Internet provides unauthorized users a means to access DOD systems; (3) while the DOD information available on the Internet is unclassified, it is sensitive and must be restricted; (4) only about 1 in 500 attacks is detected and reported, but the Defense Information Systems Agency (DISA) estimates that DOD is attacked about 250,000 times per year; (5) attackers have stolen, modified, and destroyed data and software, disabled protection systems to allow future unauthorized access, and shut down entire systems and networks to preclude authorized use; (6) security breaches pose a serious risk to national security because terrorists or U.S. adversaries could disrupt the national information infrastructure; (7) security breaches cost DOD hundreds of millions of dollars annually; and (8) DOD needs to increase the resources devoted to computer security, update the policies that govern computer security, and increase security training for system and network administrators.

[209] Ibid., Brock, *Testimony in Hackers Penetrate DoD Computer Systems.*

[210] Ibid.

While the Dutch hackers are one of the premier hacking groups in the world and universally respected for their capabilities, they apparently hacked into the DOD systems for educational purposes only. Their attacks were blatant and open. However, had the Dutch hackers been acting with malicious intent, or under the sponsorship of another nation state, one can only imagine the damage that could have been inflicted on Allied operations in the Gulf War.

The military breaches detailed above demonstrate specific instances where sensitive military information was accessed, erecting a significant breach of security with serious national security implications. Although these cases were dangerous, they caused very little damage to the flow of information. Attacks that target infrastructures with the intent to damage information flows are of equal, if not greater, concern for both the private and public sectors.

Threats to Critical Infrastructures

In an information-based or knowledge-based economy, computers and networks are critical to and instrumental in day-to-day operations of companies, organizations, and government. As a result, denying access -- accidental or deliberate[211] -- to information

[211] The denial of access to information transfers may have accidental or deliberate origins. Generally, accidental causes are natural (e.g., a lightening surge that destroys a power supply in a network that causes part of the network to fail) or human but non-deliberate (e.g., an accidental programming error that causes a computer to crash under

transfers can create economic instability and impact critical functions such as managing and operating nuclear power plants, dams, the electric power grid, the air traffic control system, and the financial infrastructure.

An example of an accidental failure occurred on January 15, 1990, when seventy million phone calls in the New York City metropolitan area went uncompleted.[212] In Queens, New York two teenage hackers speculated as to whether they were to blame for the outage.[213] The phone company was uncertain whether hackers might be at fault as well. In fact, several hackers were -- at the time -- being closely monitored for illegally accessing, altering and using various phone switches. As it turned out, a programming error was to blame for the failure. This accidental outage, however, inflicted a sense of urgency and uncertainty regarding the security of the phone networks.

While crashes, since the 1990 outage, have been uncommon, the telephone switching stations -- which are scattered throughout cities in the United States -- are squeezed into a number of unprotected locations.[214] Steven Bowman states:

certain circumstances, or the unintended cutting of a communications cable during excavation). Deliberate causes are the result of conscious human involvement. This type of involvement is typically viewed as an "attack" due to the malicious nature of the activity. Further, a primary challenge in responding to an information system attack is in the identification of the attacker and distinguishing whether or not the motive is mischief, terrorism, or an attack on the nation. See, National Research Council Report titled "Cybersecurity Today and Tomorrow: Pay Now or Pay Later," *Computer Science and Telecommunications Board* (Washington, DC: National Academy Press, 2002), 3.

[212] Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (New York: Bantam Books, 1992), 1.

[213] Joshua Quittner and Michelle Slatalla, *Masters of Deception: The Gang that Ruled Cyberspace* (New York: Harper Collins, 1995), 6-21.

[214] Steven Bowman, *When the Eagle Screams: America's Vulnerability to Terrorism* (New York: Carol Publishing Group, 1994), 155.

> In 1992, a failed AT&T switching station in New York put both Wall Street and the New York Stock Exchange out of business for an entire day, with an estimated loss of billions of dollars in trading value. The failure resulted in 4.5 million blocked domestic long distance calls, nearly 500,000 interrupted international calls, and the loss of 80 percent of the Federal Aviation Administration's circuits. A similar failure on November 5, 1991, in Boston resulted in a 60 percent loss of calls in that area.[215]

The security of the telephone networks is still questionable today. We rely heavily on telephone communications to conduct business transactions; however, there is an inherent vulnerability of this service being denied, manipulated to divert calls to competitors, or that may increase the capacity of eavesdropping. In what has been called the "Hacker Wars", competing hacker groups throughout the United States, during the 1990s, used these techniques on a regular basis. Not only did they manipulate phone switches, but they also gained access to numerous private computer networks and military sites.

Though many of the losses were minimal, it was only due to the fact that phone system crashes had been isolated and uncoordinated. Should someone decide to target several large phone networks at once, the results would be more than an inconvenience. It would likely have devastating effects on the economic stability and prosperity of many businesses. If the denial of service is maintained for extended periods of time, many businesses, government agencies, and even some military installations would be paralyzed and their ability to communicate and ensure the critical transfer of information and data would be significantly affected.[216]

[215] Ibid.

[216] See, General Accounting Office Report – *Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks,* by Joel C. Willemssen, Managing Director Information Technology Issues (September 26, 2001) GAO-01-1168T.

Isolated incidents of electronic communications, computer, and power failures have significant costs associated with them and would undoubtedly levy enormous inconveniences for businesses, government, and the average personal computer user, but they are not a threat to the national security of this country. While accidents, as defined above, happen we are not prepared to deal with an internal or external attack on our entire information infrastructure, nor are we prepared to deal with the domestic and international political consequences that such vulnerabilities create.

It has been said that with as little as one million dollars and less than twenty well trained men and women, the infrastructure of the United States can be totally paralyzed.[217] Never before has the development of new technology created such vulnerabilities to national security at such low costs to the attacker. As Ivan Bloch has stated, the "future of war [would be] not fighting, but famine, not the slaying of men but the bankruptcy of nations and the break-up of the whole social organization."[218] Our steadfast emersion into the Information Age has made this vision prophetic. As it relates to the matter of national security, information networks have created a host of vulnerabilities that have subsequently been exposed. Furthermore, this exposure has consequently invited the potential for exploitation by any nation or group. Such advancements in technology have forced us to consider the ways in which we go about protecting and securing the information that has become so readily available via computer networks.

[217] Robert Steele, "War and Peace in the Age of Information," Superintendent's Guest Lecture, *Naval Post Graduate School*, 17 August 1993.

[218] As cited in, Robert Jervis, *The Meaning of the Nuclear Revolution* (Ithaca: Cornell University Press, 1989), 10.

Protecting our Critical Infrastructures: Cyber Security

The national security posture of the United States is becoming increasingly dependent on U.S. and international infrastructures. These are highly interdependent, particularly because of the interwoven nature of the information components and because of their reliance on the national information infrastructure. The information infrastructure depends, in turn, upon such component structures as electrical power, telecommunications systems, and the Internet.

Protecting our basic installations and facilities against physical and electronic attacks and ensuring their availability will be complicated because our computer systems are at risk. As we continue the transition into the Information Age and onward into the "Knowledge Age" we become increasingly more dependent on computers. These systems control the delivery of power, communications, aviation, and financial services. They store vital and sensitive information of all types, for example, medical records, business plans, criminal records, military plans and procedures, and much more. While we utilize them in every aspect of daily life and, on many levels have forged a trust, they are extremely vulnerable to the effects of poor design, insufficient quality control and processes, accidents, and quite possibly sabotage. Without question, the computer literate thief can steal more with a computer than with a gun. Moreover, terrorists may be able to do more with a keyboard and a mouse than with a bomb.

To date the types of disruption encountered has been relatively minimal in scope. Yes, there have been thefts of money and information, e.g., identification fraud. Computer failures have disrupted communication and financial systems. However, to date there has been no successful systematic attempt to subvert any of our nation's critical computing systems. Our luck, however, may soon run out. We have been fortunate not to have been the victims of malicious people who are both capable and motivated to do harm to us. We cannot, however, assume they do not exist.

In order to be prudent we must make every effort to build computer systems that are secure and trustworthy. While these efforts have been made in both the public and private sectors -- in the form of legislation and security systems respectively -- much more work needs to be done in order to fully and adequately protect and secure the nation's critical computer systems.[219]

Quoting from a report produced by the Computer Science and Telecommunications Board (CSTB), "...[T]he degree to which a computer system and the information it holds can be protected and preserved..., which is referred to here as computer security, is a broad concept; security can be compromised by bad system design, imperfect implementation, weak administration of procedures, or through accidents, which can facilitate attacks. Of course, if we are to trust our systems, they must survive accidents as well as attacks. Security supports overall trustworthiness, and vice versa."[220]

[219] *See also,* Bara Vaida, "Clarke Presses Private Sector to Protect Against Cyber Attacks," *Government Executive Magazine* (February 14, 2002).

[220] Computer Science and Telecommunications Board (CSTB), "Computers at Risk: Safe Computing in the Information Age" *National Research Council* (Washington, D.C.: National Academy Press, 1991), 7. *See also*, the Center for Security Policy website at www.centerforsecuritypolicy.org for additional information regarding security policies. As well as, Center for Secure Information Systems; available from http:// www.isse.gmu.edu; Internet.

The Computer Science and Telecommunications Board (CSTB) defined security as the "protection against unwanted disclosure, modification, or destruction of data in a system and also to the safeguarding of systems themselves. Security, safety, and reliability together are elements of system trustworthiness – which inspires the trust that a system will do what it is expected to do."[221] Further, the CSTB stated that the organizations and people that use computers described their trust in systems and information security needs as having the following three major requirements:

> Confidentiality: controlling who gets to read information;
>
> Integrity: assuring that information and programs are changed only in a specified and authorized manner; and,
>
> Availability: assuring that authorized users have continued access to information and resources.[222]

When applied to various applications these three requirements may be emphasized differently. For example, the primary concern in national defense systems may be ensuring the confidentiality of classified information, whereas the transferring of funds may require strong integrity controls. Further, applications that are connected to external systems may have requirements that will differ from those with applications without such interconnection. Thus, the specific requirements and controls for information security may vary relative to the association of the application(s).[223]

The framework within which an organization strives to meet its needs for information security is codified as security policy. A security policy is a concise

[221] Ibid., 2.

[222] Ibid., 49.

[223] Ibid., 49.

statement, by those responsible for a system (e.g., senior management) of information values, protection responsibilities, and organizational commitment. One can implement that policy by taking specific actions guided by management control principles and utilizing specific security standards, procedures, and mechanisms.[224]

Conversely, the selection of standards, procedures, and mechanisms should be guided by policy in order to be most effective. Further, to be considered useful, a security policy must not only state the security need (e.g., for confidentiality – that data shall be disclosed only to authorized individuals), but also address the range of circumstances under which that need must be met accompanied by the associated operating standards. Without this second part, a security policy may be considered so general as to be rendered useless. For example, not until recently did most security policies require that security needs be met in the face of a virus attack. This view existed due in large part because that form of attack was uncommon and not widely understood. Today, viruses have escalated from an abstract hypothetical consideration to a commonplace threat. Thus, it has become a requisite to rethink such policies with regard to methods of distribution and acquisition of software.[225]

The field of computer security has its very own language and mode of thought, which focus on the processes of attack and on preventing, detecting, and recovering from attacks. In practice, similar thinking is accorded to the possibility of accidents that, like attacks, could result in disclosure, modification, or the destruction of information or systems or a delay in system use. Security is traditionally discussed in terms of

[224] Ibid., 50.

[225] Ibid., 49.

vulnerabilities, threats, and countermeasures or safeguard.[226] Threats and countermeasures interact in intricate and often counterintuitive ways: a threat leads to a countermeasure, and a countermeasure spawns a new threat. New means of attack are devised, and the result is a more sophisticated threat.

Security developers cannot afford to wait until a threat is manifested through a successful attack because it is at that point that significant damage can be done before an effective countermeasure can be developed and deployed. Consequently, countermeasure engineering is more often than not based on speculation and educated guess work. Further, while effort, time, and valuable resources may be expended in countering attacks that have yet to be attempted, there still exists a need to speculate and to budget resources. Moreover, when countermeasure planning occurs the planners and policymakers must understand what it is that should be protected, and why.[227] This type of understanding will undoubtedly determine the choice of a comprehensive protection strategy and effective countermeasures. The evolution of countermeasures is certainly a dynamic process. The field of computer security requires ongoing attention and

[226] Ibid., 13. Vulnerability is defined by the CSTB as "an aspect of some system that leaves it open to attack." Threat is "a hostile party with the potential to exploit that vulnerability and cause damage." Countermeasure (or safeguard) "an added step or improved design that eliminates the vulnerability and renders the threat impotent."

[227] Reuters, "Experts: Cybersecurity Plan Offers Tips, Not Rules" *USA Today,* 16 September 2002; available from http:// www.usatoday.com/tech/news/techpolicy/2002-09-16-cyber-plan_x.htm; Internet. See also, Mark Schoeff, "Cybersecurity: Current Challenges Larger than National Strategy Response" *Center for Strategic and International Studies* (September 18, 2002).

planning, because yesterday's safeguards may not be effective tomorrow, or even today.[228]

Ensuring a clear and comprehensive understanding of the vulnerabilities, threats, and our approaches to countermeasures -- in order to protect our critical infrastructures and ultimately our national security -- will become the focus of the future in the Information Age. They will also determine how and in what context we address domestic and/or international conflicts relative to national security and the concepts of information warfare and cyber warfare.

National Security in the Information Age

The threat of another terrorist attack within our borders and against U.S. citizens and U.S. interests around the world has become the most significant national security issue to face this country since the tragic events of September 11, 2001. Realizing that an attack on our national critical infrastructures could cripple this nation and render it relatively defenseless has become of significant importance to members of the legislature and the executive branch alike. Much attention has focused on how an attack of our critical information infrastructures would ultimately affect our national security.

The concept of "national security" and its relationship to the electronic digital computer are similar in that they were both products of World War II. The Electronic Numerical Integrator and Computer (ENAIC), produced at the University of

[228] Ibid., 13-15.

Pennsylvania in 1946, was the world's first digital electronic computer.[229] One year later, the National Security Act authorized the creation of the Central Intelligence Agency (CIA), the National Security Council (NSC) and the organization of the separate military forces under the National Military Establishment (NME).[230] The relationship between national security and computers may be viewed as symbiotic. During a period of thirty or more years, the chief U.S. government agencies responsible for national security implementation and oversight were also the primary sponsors of computer research and foremost customers of the computer industry. By the end of the Cold War, the process of integrating advanced computers into weapons and command systems sped up instead of declining.

In more recent years, the relationship between national security and computer technology has flourished – resulting in the development of modern arsenals, "battle management", and communications that are the products of technology and dependent on technological advancements. With regard to military systems, the future appears to be in the hands of "smart" weapons. These are comprised of complex systems of command and control, telecommunications, satellites, electronic surveillance, and split-second information processing.[231] Table 3 is a sample listing of the U.S. smart missiles fleet.

[229] Gary Chapman, "National Security and the Internet," *The 21st Century Project* LBJ School of Public Affairs (University Station University of Texas, July 1998).

[230] As a result of amendments made to the 1947 Act, the NME was changed and named the Department of Defense (DOD) in 1949.

[231] Ibid., Chapman, *National Security and the Internet.* See also, Richard P. Hallion, "Precision Guided Munitions and the New Era of Warfare," *Air Power Studies Centre* Working Paper no. 53; Fred Kaplan, "U.S. Bombs Not Much 'Smarter" *Boston Globe* (20 February1998): sec. A01; Jim Randle, "New US Weapons," *Voice of America,* 13 February 1998; Gene I. Rochlin, *Trapped in the Net: The Unanticipated Consequences*

Table 3. U.S. Smart Missiles Fleet

Missiles														
		range km	**CEP m**	**quantity current & *planned***	**IOC**	**A-10**	**B-52**	**B-1B**	**B-2**	**F-15**	**F-16**	**F-117**	**F-14**	**F-18**
AGM-62	Walleye				1967									x
AGM-65	Maverick	27	1	**~40,000**	1972	x				x	x			x
AGM-84	Harpoon / SLAM	100		**~6,000**	1977		x							x
AGM-86C	CALCM	1,100		**+300**	1991		x							
AGM-88	HARM	50		**~19,000**	1984						x			x
AGM-123	Skipper	25			1985									x
AGM-130		30		**500**	1994					x				
AGM-136	TACIT RAINBOW	430		0	XXX		x	x	x	x	x			x
AGM-137	TSSAM	100		0	XXX		x	x	x	x	x	x		x
AGM-142	HAVE NAP	80		**130**	1992		x							
AGM-154	JSOW	75		*~24,000*	1998		x	x	x	x	x	x	x	x
AGM-158	JASSM	100		*+2,400*	2001		x	x	x	x	x	x		x
BGM-109	Tomahawk	1,100		**2,000**	1983									
	LOCAAS					x	x	x	x	x	x	x		x
	FRSW						x	x	x	x	x	x		x
	ARRMD	1100			2010		x	x	x	x	x	x		x
	HyStrike / Fast Hawk	1300			2010		x	x	x	x	x	x		x
Guided Bombs														
Laser Guided Bombs		**range km**	**CEP m**	**quantity current & *planned***	**IOC**	**A-10**	**B-52**	**B-1B**	**B-2**	**F-15**	**F-16**	**F-117**	**F-14**	**F-18**
GBU-10	Paveway II 2000lb	15	8	**11,000**	1976	x				x	x	x	x	x
GBU-12	Paveway II 500lb	15	8	**32,000**	1976	x				x	x	x	x	x
GBU-16	Paveway II 1000lb	15	8		1976	x				x	x	x	x	x
GBU-24	Paveway III 2000lb	20	8	**13,000**	1983	x				x	x		x	x
GBU-27	HAVE VOID	20	8	**3,200**	1987							x		
GBU-28	"bunker buster"	10	8	**300**	1991					x				
GPS Guided Bombs														
GBU-15	GPS-mod	10	3	*~1,500*	1999					x				
GBU-24 E/B	Paveway III 2000lb	20	8		2000	x				x	x		x	x
GBU-28 E/B	"bunker buster"	10	8	**350**	2002					x				
GBU-29	JDAM 250lb	10	13	*87,000*	1997		x	x	x	x	x	x	x	x
GBU-30	JDAM 500lb						x	x	x	x	x	x	x	x

Source: GlobalSecurity.org; available from http:// www.globalsecurity.org/military/systems/munitions/smart.htm; Internet. Copyright 2000-2003.

of Computerization (Princeton University Press, 1997) specifically, Chapter 8 titled, Smart Weapons, Smart Soldiers.

While the nation's overwhelming superiority in information technologies will, undoubtedly, ground its superpower status in the future, it will also, likely, pose a significant threat to national security.

Our transition into the Information Age has created a series of dangerous threats and circumstances to American national security. Technological innovations provide vulnerabilities with different sets of incentives, consequences, and political dilemmas than have previously been encountered by nation-states. Thus, where the destruction of bridges or railroads posed a threat to the security of an industrialized nation, the destruction of information networks, especially those involved with financial transactions, poses an even greater threat to the national security of information societies. Consequently, information warfare endangers not only the ability to respond to physical threats, but economic prosperity as well. Historically, a nation's ability to remain prosperous has been inexplicably linked to physical threats. In the Information Age this is no longer the case. Further, economic prosperity can now be completely destroyed without the infliction of any physical damage.[232]

If national security is defined as "no more than the total of the individual's perceived sense of security"[233] -- at its simplest level -- or that it entails the "range of physical threats that might arise for the nation and the force structures, doctrines and military policies mobilized to meet those threats...[234] then information warfare can be categorized as a national security threat. Further, "those internal and external factors –

[232] Bowman, *When the Eagle Screams*, 155.

[233] John Peterson, as cited by Steele in, "War and Peace in the Age of Information."

[234] John J. Weltman, Michael Nacht, and George H. Quester, *Challenges to American National Security in the 1990's* (New York, Plenum Press, 1991), xi.

such as economic or technological change – that might arise and whose direct or indirect effect would be to diminish or to enhance the nation's capacity to meet physical threats"[235] have become of significant national concern.

Given the vulnerabilities facing military information networks and the military's reliance on private sector communications paths for roughly ninety-five percent of its communications,[236] information warfare can impede the military's ability to respond to conventional and non-conventional threats. The military's reliance on computer technology for digital mapping and intelligence also creates a vulnerability to our conventional military forces. To illustrate, it took two months to meet the digital mapping requirements to use Tomahawk missiles in the Gulf War.[237] Had the threat been immediate, the United States would not have been able to effectively utilize its smart weapons capabilities and collateral damage would have been significantly higher than was encountered.

As the transition into the Information Age is solidified, nations now face the clear and present danger of having their information infrastructures destroyed, altered, or incapacitated by new and emerging offensive technologies. This potent mixture of technological threats, vulnerabilities, and unprecedented tactics is often identified as Information Warfare (IW). While the topic of IW has been debated within military, defense, and intelligence circles, significantly far less work has been contributed to the

[235] Ibid.

[236] Steele, "The Military Perspective on Information Warfare", 5.; *See also*, Bill Gertz, "Electronic Crime Threatens Integrity of Long Distance Phone System," *The Washington Times*, 24 October 1994, sec. A3; "Services Gear Up for Information War," *Defense Daily* 184, no. 48 (September 8, 1994): 377.

[237] Steele, *War and Peace in the Age of Information.*"

field of political science in an effort to examine security issues related to information technology.[238]

Information Warfare / Cyber Warfare

What is Information Warfare? Robert Steele argues that it is

> about applied intellect – it is about harnessing intellect and protecting intellect, and it is above all about providing the commander – including the civil commander in the role of political, economic, or cultural leader – with survivable, reliable, decision-support through war and operations other than war, on the home front as well as on the traditional front line – and to do it so largely with 'out of control' civil resources.[239]

To put it simply, information warfare endangers not only our ability to respond to physical threats, but our economic prosperity, as well. Its ultimate goal is the destruction of information, reducing information flows, reducing the reliability of content, and denying access to services. Information warfare is waged against industries (big and small), political spheres of influence, global economic forces and, may even be waged against entire countries. It is the use of technology against technology. It is about secrets and the theft of secrets, turning information against its owners, and denying an enemy the ability to use both its technology and its information.[240]

[238] Eugene B. Skolnikoff, *The Elusive Transformation: Science Technology and the Evolution of International Politics* (New Jersey: Princeton University Press, 1993).

[239] Steele, "The Military Perspective on Information Warfare: Apocalypse Now." Keynote address at the Second International Conference on Information Warfare: Chaos on the Electronic Superhighway, Montreal, 19 January 1995.

[240] Winn Schwartau, "Something Other Than War", *Cyberwar 2.0* (AFCEA International Press: Fairfax, 1998).

Historically, science has always been applied to war. As scientific capacities increased, so did the weapons societies used in warfare. Agrarian society saw the development of the crossbow. Industrialized nations developed the machine gun, tanks, and bombers. Further, as the field of physics matured, nuclear fission was used to deal devastating effects from the highest altitudes. Today, computer-guided electronics allow even more damage to be dealt from the comfort of an underground bunker thousands of miles away. As we steadfastly move into the Information Age and make our mark, it is only natural that our weapons will follow and be reflective of the age. Thus, as projected by William S. Cohen, the former Secretary of Defense, "the more reliant we become upon computers and information systems, the more vulnerable we become to cyber-terrorists who will conceive unlimited ways to cripple our infrastructure, our power grids, our banking systems, our financial markets, our space based communications systems."

Not only is information warfare an entirely new paradigm for waging war, it must also be adopted as a supplement to traditional and conventional means of warfare, if successful campaigns are to be waged and effective defenses are to be established. Information warfare can span the spectrum from psychological attacks to traditional intelligence gathering practices. As a result, we must narrow the scope of the discussion further from information warfare (IW) to cyber warfare (CW). This form of warfare is significantly different from the aforementioned forms of warfare, i.e., conventional and nuclear, and, may be considered what makes IW distinctly new and challenging to national security.

Although damaging physical security may be the ultimate objective, it is accomplished solely by means of using computers and networks to degrade or destroy information. (This, however, excludes conventional or nuclear attacks to achieve "IW" ends.) For example, bombing NSA or CIA headquarters with the intent of disrupting the flow of information to decision makers would not be considered a "cyber" attack, although it may be viewed as information warfare. While the differences may be subtle, conceptually they revolve around a change in the means and space of conflict.

As we examine the concept of information warfare, its damaging effects, and its targets one cannot help but wonder why in this post Cold War world would any actor choose to wage information warfare against an adversary. There are several political and strategic reasons for state-sponsored information warfare. The cost of such an attack is low, it is timely and not specifically reliant on a particular location; it provides little or no warning, there would be minimal human life costs, and very importantly, may be waged in complete anonymity. Each of these attractions will be examined in order to provide a clear understanding of how information warfare is politically and strategically advantageous to states.

Limited Costs

Information warfare is a fairly inexpensive form of warfare with a significantly high return on investment. With less than one million dollars and less than twenty well-trained persons, significant harm and damage could be perpetuated on the infrastructure of the United States.[241] These costs are cheap when compared to the costs of waging

[241] Steele, *War and Peace in the Age of Information.*

conventional warfare.[242] This type of offensive warfare, i.e., the inexpensive information warfare, undoubtedly is very attractive to developing countries and offers them comparable capability to inflict damage on information infrastructures just as damaging as attacks carried out by industrialized countries. One defining feature of the post-Cold War era has been that the single, large threat of the Soviet Union has been replaced by a greater number of lesser threats. Further, the declining cost of information technology promises that many of these new threats will take the form of IW.

Timely and Specific to any Location

Information warfare can be waged from any location and at the push of a button or the click of a mouse. There is no fail-safe early warning system for information warfare and as a result this creates extremely heightened levels of anxiety, mistrust, and fear. Unlike in cases where conventional weapons are used, no radar can pick up a long distance telephone call from overseas; however, that particular call has the potential to cause more monetary damage than a dozen planes carrying conventional missiles. The example of the first World Trade Center bombing in February 1993 is illustrative. The damage to the flow of information was estimated at over one billion dollars[243] at that time and that disruption proved to be more costly than the structural damage inflicted on the building.

Information networks, telephone lines, or simple floppy disks can import viruses into the United States and go undetected by U.S. Customs Inspectors because they do not

[242] Schwartau, *Information Warfare: Chaos on the Electronic Superhighway.*

[243] Bowman, *When the Eagle Screams*, 7.

attract attention. Although a well-planned information warfare attack may take several years to orchestrate, it can occur instantaneously. Further, to uncover plans for such an attack would involve a great deal of investigation and intelligence. Most of the actors would be invisible, both to the victim and to each other. Due to the connectivity now offered by the Internet, most of the preparatory work for lower levels of information warfare and much of the actual attack can be completed outside the traditional territorial boundaries of the victim nation.

Anonymity

One of the most engaging features of waging an information warfare attack on an adversary is the ability to conduct the attack anonymously. Not only can a state's national security be breached, but there may be no one to hold readily accountable for the attack. This makes information warfare a very attractive mechanism for covert operators. Political dilemmas may arise in the victim state when citizens demand retribution and the government has no specific target. The result could be political instability as citizens focus blame on the government for allowing this situation to occur. It might even instigate the collapse of an unstable political system should the anonymous attack be prolonged and systematic. In addition, targets can be strategically selected to generate the maximum amount of chaos and insecurity possible.

An example of how critical national infrastructures can be threatened anonymously from abroad is the intrusion that occurred into the computers controlling part of the California power grid in 2001. Although the attack was traced back to a computer in China, security experts handling the case admitted that due to the ability to route and re-route attacks, it was difficult to discern the point of origin for many attacks.[244] Re-routing attacks involves compromising a set of computers in various geographic locations. With each compromised system, the attacker gains a level of anonymity because defenders must trace through an additional location. Such tracing legally requires consent, and that consent can be difficult to obtain for political reasons.

Loss of Human Life - Minimal

Another attractive feature of information warfare is its ability to be waged with minimal loss of human life inflicted within the target nation. This makes information warfare techniques politically attractive since there are no established global taboos associated with waging war against machines. There are three reasons why states might restrain from using certain weapons or means of warfare, according to Jeffrey Legro: (1) countries may pursue restraint because popular opinion vilifies certain weapons; (2) because leaders calculate that escalation would damage their domestic and international political support; or, (3) because states fear retaliatory attacks.[245] Thus, information warfare may be applied to this framework because this type of warfare causes low levels of human casualties and structural damage. Further, there is little reason to believe that popular opinion will vilify it. In fact, populations will not even know information warfare has been waged against them until it is too late (and few will understand the

[244] Dan Morain, "Hackers Victimize Cal-ISO." *Los Angeles Times Online*; available from http://www.latimes.com/news/state/20010609/t00047994.html; Internet.

[245] Jeffrey W. Legro, "Military Culture and Inadvertent Escalation in World War II," *International Security*18, no.4 (Spring 1994): 108.

methods used in the attack). Therefore, it is highly unlikely that information warfare will be considered an inhuman way to pursue diplomacy by other means.

In addition, there is little reason to believe that by using information warfare the aggressor country will be politically damaged. This type of warfare assures that the anonymity of the aggressor may well be identified only if it wishes to be. When information warfare is waged by one nation against another without anonymity, the political outcomes would likely resemble those of traditional warfare. Strategic alliances could be formed and some states could choose to remain neutral, though it is highly unlikely that neutral states will be able to avoid the global economic aftershocks of high intensity global information warfare.

Legro uses three examples, in his essay, to demonstrate that military culture is a strong factor determining when alternative or taboo forms of warfare will be used. Since information warfare is a relatively new concept, it is doubtful that it has been fully adopted by the military culture. Recent trends, however, indicate that it is an area that is getting a great deal of attention and increased funding in an age of increasing growing military budgets. This reveals that the military culture perceives information warfare as a reasonable and arguably preferable form of warfare. Each branch of the United States Armed Services has publicly admitted to concentrating on information warfare concerns.[246]

Despite collective interests and hopeful cooperation, information attacks will continue to be a viable national security concern. Unfortunately, a state's ability to

[246] Paul Mann, "Dialing for 'Info War'," *Aviation Week and Space Technology* 142, no. 4 (January 23, 1995): 31.

control these types of attacks is currently very limited. By increasing security, gathering intelligence regarding any plans that might be in consideration, and pursuing a credible policy of deterrence, we can better ensure that the threat of information warfare is contained to isolated incidents from which the United States can recover. Unfortunately, the environment under which we operate can make no such assertions.

Addressing the Threat / Defending Against an Attack

Prior to dealing with the threat posed by information warfare, a state must acknowledge that it exists. It is wrong to assume that security through obscurity will work indefinitely. Offensive information weapons can be developed using open source material and assembled using readily available electronic components. In fact, some offensive information warfare weapons, namely a HERF gun,[247] have been assembled completely by accident.[248]

The existence of offensive information warfare capabilities, coupled with the United States' heavy reliance on information technologies, has introduced a new threat to our national security. Information warfare, most likely in the form of terrorism, is probable because the costs, both politically and economically, are lower than the benefits

[247] HERF stands for High Energy Radio Frequency. HERF guns are able to shoot a high power radio signal at an electronic target and put it out of function. The damage can be moderate (e.g., that a system shuts down, but can be restarted) or severe (e.g., the system hardware has been physically damaged). Simply put, HERF guns are nothing but radio transmitters.

[248] Winn Schwartau, "Class II Information Warfare: Corporate Espionage and Sabotage." Presentation at the Second International Conference on Information Warfare. Montreal PQ, January 18, 1995.

derived. If an autonomous nation or political group wishes to inflict damage, chaos, and fear on American society with minimal costs, then its most rational option is to use offensive information warfare capabilities.

If this threat is acknowledged, the response options available to the United States increase. Specifically, actions to decrease the impact of an information warfare attack can be undertaken in advance to minimize the damage incurred. Political scientist James Wyllie argues that:

> Deterrence demands that an adversary be made completely aware of the value of the issue in dispute to the deterrer, and the willingness to collect a price should the rival not be dissuaded from its unwelcome course of action.[249]

Acknowledging the threat acts as a deterrent for several reasons. First, it increases the number of responses available to the United States because the issue has been addressed at a political level. Our capabilities to deal with such an attack are increased because we are prepared for it. Second, it motivates the military and private industry to deal with this problem and create viable security solutions that minimize the vulnerability of the United States' critical information infrastructure. Third, it gives the United States a political catalyst to deal with this issue on a global level and to enter into treaties and agreements to protect the global information infrastructure.

The concept for defending against information warfare is clear. In the information age as in the nuclear age, *deterrence* is the first line of defense. This

[249] James H. Wyllie, "The Deterrence Condition," In Carey, Roger & Salmon, Trevor C. *International Security in the Modern World* (New York: St. Martin's Press, 1992), 63.

deterrence must include an expression of national will as expressed in law and conduct, a declaratory policy relative to consequences of an information warfare attack against the United States, and an indication of the resiliency of the information infrastructure to survive an attack. Technology to conduct information warfare is simple and ubiquitous – simply put, some form of infrastructure robustness and protection is essential.[250]

It is technically and economically impossible to design and protect the infrastructure to withstand any and all disruptions, intrusions, or attacks (or avoid all risk). The risk can be managed, however, by protecting selected portions of the infrastructure that support critical functions and activities necessary for maintaining political, military, and economic interests. An equally important function is to verify through independent assessments that the design principles are being followed, that protective measures are being implemented where appropriate, and that the information warfare (defense) readiness posture is implemented as planned.

Tactical warning, damage control, attack assessment, and restoration ensure the continuance of these critical functions and activities in the presence of disruptions or attacks. The essence of tactical warning is monitoring, detection of incidents, and reporting of the incidents. Monitoring and detection of infrastructure disruptions, intrusions, and attacks are also an integral part of the defense against information warfare. Providing an effective monitoring and detection capability will require some policy initiatives, some legal clarification, and an ambitious research and development program. The telecommunications infrastructure will be subject to some form of attack

[250] Ibid.

and we should have some capability to limit the damage that results and to restore the infrastructure.

Little research has been devoted to the basic procedures necessary to contain the potential damage brought about by an attack, let alone the tools which might provide some automated form of damage control. Some form of attack assessment is essential to determine the impact of an attack on critical functions and the appropriate response to an attack. Restoration of the infrastructure implies some capability to repair the damage and the availability of resources such as personnel, services, and the like.

The basic functions of monitoring, detection, damage control, and restoration must begin at the lowest possible operating level. Reports of the activity must be passed to regional and national-level organizations to establish patterns of activity and to request assistance as needed in damage control and restoration. Finally, some form of response to the intrusions or attacks may be necessary to deter future intrusions or attacks. The response could entail civil or criminal prosecution, use of military force, perception management, diplomatic initiatives, or economic mandates.

As a nation, we must ensure that the structure we are building has a strong foundation and that the weaknesses in that structure are not used to destroy it. This will be an extremely challenging task because the constitutionally guaranteed rights of United States citizens are expected to be upheld in the process. The onus of building and securing a strong information infrastructure will undoubtedly fall on both the public and private sectors. Moreover, a sound public-private partnership -- where the sectors are working in tandem to protect sensitive information and critical infrastructures -- will be required in order to protect our national interests and ensure the security of the state. Chapter 5 will examine this relationship/partnership between the public and private sectors and the requisite roles each will have to play in order to effectively address the vulnerabilities and the threats caused by technological advancements.

Chapter V

PUBLIC AND PRIVATE SECTOR INITIATIVES TO ADDRESS INFORMATION INFRASTRUCTURE VULNERABILITIES

The Information Age has fundamentally altered the nature and extent of our dependency on critical, nation-wide infrastructures. Increasingly, the U.S. Government, our economy, and our society are being connected into an ever expanding and interdependent digital nervous system of computers and information systems. Undeniably, with this increasing interdependence we have created and acquired significant vulnerabilities. To illustrate, one person with a computer, modem, and a telephone line anywhere in the world can potentially break into sensitive government files, shut down an airport's air traffic control system, or disrupt 911 services for an entire community.

The aftermath of the September 11, 2001 attacks on the World Trade Center and the Pentagon illuminated the significant vulnerability of America's infrastructure to terrorist attacks and the enormous, far reaching consequences of not adequately and effectively protecting it. While the terrorists were able to utilize deficiencies in America's overall approach to intelligence sharing and aviation security, similar vulnerabilities existed, and in many cases continue to exist, in every infrastructure vital to the security, economy, and survival of the nation – such as computer networks, energy supplies, transportation, and satellite systems.

The threats posed to our critical infrastructures levied by hackers, terrorists, criminal organizations, and foreign governments are real and growing. Thus, the need to assure delivery of critical services over our infrastructures is not only a concern for national security and federal law enforcement communities; it is also a growing concern for the business community in particular, since the security of information infrastructure is a vital element of electronic commerce (E-commerce).

While it is has been said that more than 90% of the nation's critical infrastructures are neither owned nor operated by the Federal Government, partnerships with the private sector and state and local governments are therefore needed.[251] This partnership is consequently the fundamental aspect of critical infrastructure protection. Further, President Clinton's Presidential Decision Directive 63 (PDD) detailed the President's policy on and vision for critical infrastructure protection for the nation. The Directive, in line with the Computer Security Enhancement Act of 1997, emphasized -- among others -- the importance of information sharing among and between the public and private sectors. Thus, PDD 63 sought "the voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships."[252]

In an interview prior to officially becoming the new Chief Information Officer (CIO) for the Department of Homeland Security (DHS), then Office of Homeland Security CIO, Steven Cooper, clearly indicated that one of his three primary responsibilities in his new position is to first guide "horizontal information sharing...

[251] Joshua Dean, "Systems Failure," *Government Executive Magazine,* 2 February 2002; available from http//www.govexec.com/news/index.cfm?mode=report&articleid=22061; Internet. *See also*, Shane Harris, "Cultural Barriers, Not Technology, Blamed for Poor Information Sharing," *Government Executive Magazine* (February 26, 2002).

[252] The White House, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998 (Washington, D.C.).

[a]mong the federal agencies.[253] [Second,] the information to be shared is essential information necessary to support Homeland Security but it really translates to combating terrorism. And then the third is, ...vertical information sharing. [I'm] talking about sharing and the integration of information among federal, state and private sector entities."[254] Cooper's plans for the CIO's office fully underscores the intent of both the Congress and the Clinton Administration relative to a comprehensive, public-private sector, approach which addresses critical national information infrastructure vulnerabilities.

In this light, drawing on the full breadth of expertise of critical infrastructure stakeholders, i.e., the federal government (federal agencies) and the private sector (industry, businesses, consumers), and establishing a collaborative relationship is essential to addressing this matter most effectively. Moreover, given the impact acts of terrorism have had on the United States, its interest, and countries around the world, governments, businesses, industries, and individuals are beginning to realize and appreciate the importance of information sharing between the stakeholders in the public and private sectors.

[253] Esther Shein, "Homeland Security CIO: Information (Sharing) Is Power," *CIO Information Network*, 4 June 2002; available http//cin.earthweb.com/news/article.php/10493_1183981; Internet.

[254] Ibid.

The Stakeholders

The stakeholders of the critical information infrastructure include all parties involved in the creation, development, implementation, maintenance, and consumption of information. The public-private sector partnership is a requisite to fully developing, securing, protecting, and maintaining our national information infrastructures. From the onset, the formal development of the national information infrastructure was an initiative instituted by the U.S. government. Consequently, it may be viewed as a key stakeholder; with the various federal agencies being instrumental in shaping the policies that are amenable to the success of the initiative.

The next significant stakeholder in the development and implementation of the national information infrastructure is the private sector. Without it the component parts of this infrastructure would not be possible. The various companies and businesses involved in the creation, publication, transmission, storage, organization, dissemination, recycling, processing of information, and providing for the facilitation of hardware and software, have been primarily instrumental in the construction of our national information infrastructure. While most of these companies participate in order to satisfy their own strategic or competitive objectives, their participation -- nonetheless -- is critical to the implementation and protection of the infrastructure.

The consumer or end-users -- and, in some cases the providers of information -- consist of another group of stakeholders. While the consumer's needs tend to be different and overlap with the services provided by the national information infrastructure, the consumer is also a major provider of the information injected into the infrastructure. Specifically, the information user has the following needs:

1. Searching, discovering, updating, transforming, and retrieving useful information.
2. Building and maintaining electronic repositories of information.
3. Creating and distributing information electronically.
4. Executing and recording commercial, legal, financial, and other business transactions.
5. Supporting collaborative work efforts among collocated or remote individuals.[255]

A review of the role and responsibilities of each stakeholder in the future of our critical information infrastructure will be examined individually.

The Public Sector

Many Americans, today, are beginning to recognize that the responsibility for protecting our critical infrastructure from domestic or international attack does not summarily rest with any one level of the federal, state, or local government. Structural, cultural, institutional, and statutory changes are needed to secure the nation's infrastructure so that domestic and/or international terrorists have less incentive to attack them and the nation can respond quickly if they do. Fundamentally, the success of efforts to defend and protect infrastructure will rest on the ability of federal, state, and local governments to cooperate with each other as well as the private sector.

President Clinton rightly challenged the federal government -- via PDD 63 -- to serve as a model for critical infrastructure protection; that is, to put our own house in

[255] GITS (Government Information Technology Services Working Group of the IITF Committee on Application and Technology). August 1994. A Vision for the Government Information Technology Services and the National Information Infrastructure Report.

order first. Given the complexity of the task, President Clinton understood the importance of taking advantage of the breadth of expertise within the federal government to ensure that those agencies with special capabilities and relationships with private industry were enlisted to participate fully in pursuit of this common goal.

Further, while no single authority, including the U.S. government has the capability to develop, mandate or legislate a coherent services framework -- within which individual commercial competitive solutions can coexist and interact -- the government would be expected to provide the leadership and vision to guide this process. It would further be expected to balance the interests of the many stakeholders, and to influence the shape of the information infrastructure.

While the construction of a "national information infrastructure" will be clearly undertaken by the private sector, the role of government will be to monitor the competitive entries into the information services market. Further, it will be required to provide the necessary monetary support to ensure that small and large businesses, non-profit organizations, and low to moderate income communities will be able to participate in the development of a national information infrastructure.[256]

Additionally, in keeping an ever present eye toward the motivations of business -- i.e., the pursuit of profits and competitive advantage -- government will, arguably, have to establish regulatory processes. These, Egan argues, tend to constrain earnings and market power; hence representing a formidable roadblock to private investment. In this

[256] Michael Lou, "Fly the friendly skies," *Satellite Communications* 18, no. 2 (February 1994): 20. *See also,* Arnaud de Borchgrave, Frank J. Cilluffo, Sharon Cardash, Michele M. Ledgerwood, "Cyber Threats and Information Security: Meeting the 21st Century Challenge", *CSIS* (2001).

scenario, Egan states, the primary role of a government is to prevent the over-regulation of industry in the market.[257]

One of the major issues facing the government stakeholder involves providing universal access to all. All the levels of government will have a role to play in ensuring the effective development and deployment of the information infrastructure. Further, the government will be responsible for ensuring that vigorous competition, fair access, basic levels of services, and interoperability exist and are available for everyone. In addition, the government will have to assume responsibility for providing privacy and security protection for all infrastructure users as well as coordinating the regulatory and policy-making efforts at federal, state, and local levels in order to complement the nation-wide vision of a standard national information infrastructure.[258]

A paramount role of the government will focus on the responsibility of setting and coordinating minimum standards for security and interoperability, and conducting and supporting fundamental research on new security technologies. This research will necessarily have to focus on such areas as biometrics and the improvement on smart card technologies, promoting awareness of issues relating to information protection, ensuring greater international cooperation between law enforcement and other agencies, and bringing down barriers which inhibit such cooperation.

[257] Bruce L. Egan, "Building value through telecommunications: Regulatory roadblocks on the information superhighway," *Journal of Telecommunications Policy* 18, UK, no. 8 (November 1994): 573-587.

[258] Lucas Mast, "Is the Government Protecting Our Information?" *CATO Institute* 28 November 28 2001 (Washington, D.C.: 2001).

The Congress has become instrumental in developing laws that require federal agencies to develop standards that will be utilized by both the federal government and industry. These standards are being developed in cooperation with both Internet companies such as Cisco Systems, IBM, and others, and telecommunications and software companies. Industry continues to lobby the Congress for standards that necessarily afford a reasonable degree of security and are attainable in a cost effective manner. Such standards, industry experts argue, should empower users to secure themselves, but should not be used as a "command and control" mechanism to force new regulatory burdens on users. Thus, the goal should be to standardize for interoperability and security, and not to mandate a particular technology.

As it relates to research and development (R&D), the government has a legitimate role in funding and supporting basic and applied research in the area of information security. Lest we forget, the Internet itself was the outgrowth of basic research initiatives by the Department of Defense Advanced Research Projects Agency (DARPA) in 1969.[259] Such research funding would be expected to be applied across disciplines and not limited to the computer sciences. Security depends not only on hardware and software, but also on policies, practices, and personnel. It is, therefore, the government's responsibility to understand the vulnerabilities of the infrastructure created by technological advancements as well as to understand who exploits them and why. It is also the government's responsibility to properly train its civilian workforce in this area as well.

[259] President, "Remarks by the President in Photo Opportunity with Leaders of High-Tech Industry and Experts on Computer Security. The Cabinet Room, The White House. 15 February 2000, William J. Clinton; available from http://10.147.64.15:5666/hyper/2000/0215/epf203.htm; Internet.

Education and training is an essential component of securing and protecting the information infrastructure. The absence of passwords or poor passwords are the most common and cost efficient way to obtain unauthorized access to a computer or computer system. As a result, users, administrators, and others must be educated and properly trained in the appropriate use and threats to computer systems. The bulk of this training should be done by the government to educate its workforce and contractors about the need for security precautions. Additionally, the government has a role in the promotion of the development of undergraduate and graduate level programs in information security in which federal grants and scholarships are offered. Several companies have established mentoring programs in this area in concert with several universities, for example, Purdue University, George Washington University, and James Madison University.

In addition to providing educational incentives and training to academia and its civilian employees respectively, the government will be required to be active in the promotion of new and emerging security technologies. One sound example of such technology is encryption.[260] After nearly ten years, the government finally liberalized the regulations concerning the use and export of commercial encryption software. Most companies are now free to create and use such software to protect confidentiality, integrity, and availability of information. This type of emerging technology will, by default, aid in the protection of the government's own infrastructure as well.

[260] See, Jack McCarthy, "Government Relax Encryption Regulations," *PC News World. Com* (3 April 2000); Reuters, "Lawmaker: More Encryption Needed," 21 September 2001 (Washington, D.C.); Declan McCullagh, "Congress Mulls Stiff Crypto Laws" *Wired News,* 13 September 2001 (Washington, D.C.); available from http:// www.wired.com; Internet. U.S. Department of Commerce, Draft II Encryption Export Regulations (17 December 1999); Cyberspace Electronic Security Act of 1999 (CESA 99).

In his testimony before the Senate Committee on Governmental Affairs, John S. Tritak, Director of the Critical Infrastructure Assurance Office (CIAO), reported on the contributions of federal agencies in critical infrastructure assurance.[261] He observed that "the heads of executive departments and agencies are responsible and accountable for providing and maintaining appropriate levels of information systems security, emergency preparedness, continuity of operations, and continuity of government [support] for programs under their control."[262] Tritak highlighted the roles and responsibilities of various departments that were either established under PDD 63 or whose responsibilities were broadened as a result of the directive. Thus, the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council was assigned this responsibility by the Clinton Administration -- via PDD 63.

Apart from the above, the National Infrastructure Protection Center (NIPC) -- a former division of the FBI -- was established by PDD 63. Prior to its move into the recently created Department of Homeland Security, NIPC as part of the FBI served as the nation's threat assessment, warning, and incident response center for cyber attacks. (It is expected to continue in this role as part of the new Department as well). This organization was also responsible for facilitating law enforcement investigations of cyber-related crimes.[263]

[261] Congress, Senate, Committee on Government Affairs, *Critical Infrastructure Protection: Who's in Charge?*: Hearing of John S. Tritak before the Committee on Governmental Affairs, 109th Cong., 1st sess., 4 October 2001.

[262] Ibid., 3.

[263] Ibid.

PDD 63 also established the Critical Infrastructure Assurance Office (CIAO). This interagency organization -- located at the Department of Commerce -- was established to provide support to the National Coordinator in carrying out policy developments and coordination functions. The Office focuses on three primary areas:

1. Promoting national outreach and awareness campaigns both in the private sector and at the state and local government level;
2. Assisting Federal agency analyses of critical infrastructure dependencies; and,
3. Coordinating the preparation of an integrated national strategy for critical infrastructure assurances.[264]

Another agency tasked with addressing infrastructure vulnerabilities is the National Institute of Standards and Technology (NIST). This agency, created as a result of the Computer Security Enhancement Act of 1987, is part of the Department of Commerce. It contributes to the development of the national information infrastructure by funding high-risk industrial ventures, performing laboratory research, and participating in policy and standards formation to ensure that the technologies are available for real-life applications.

As part of the federal government's efforts to ensure multi-agency participation in the formulation of a joint vision and strategy for addressing information vulnerabilities, the Committee on Applications and Technology of the Information Infrastructure Task Force was established. It is chaired by the Director of NIST. This Task Force is given the responsibility of studying how innovative technologies will help people do their jobs in new and different ways. In addition, the committee coordinates government-wide

[264] Ibid., 3.

efforts to develop information technology applications and recommend technology policy.

The Computer Security Enhancement Act of 1997 and Presidential Decision Directive 63 mandated federal agencies to spend the resources necessary to protect and defend its own infrastructure -- civilian and military. The Clinton Administration requested budgetary support in order to assist federal agencies in this effort. For example, on February 15, 2000, the Clinton White House announced funding support in the amount of $2 billion for critical infrastructure security and protection. This amount was an increase of 15% from the previous year's $1.75 billion appropriation. A significant portion of the increased funding -- $606 million -- was earmarked for research and development (R&D) efforts. The Clinton administration also provided full or pilot funding for the following initiatives:

1. Establishment of a Federal Cyber Services Training and Education initiative ($25 million)
2. Establishment of a permanent Expert Review Team (ERT) within the Department of Commerce's NIST whose function is to assist agencies who are tasked with conducting vulnerability analyses and developing Critical Infrastructure Protection (CIP) plans ($5 million)
3. Designing a Federal Intrusion Detection Network (FIDNET) to protect vital systems in federal civilian agencies ($10 million)
4. Funding of seven Public Key Infrastructure Models pilot programs at different federal agencies ($7 million)
5. Expanding Federal research and development investments in computer security by more than 32 percent in the FY2001 budget ($606 million)
6. Establishment of an Institute for Information Infrastructure Protection that will combine federal and private efforts to fill key gaps in critical infrastructure research and development. ($50 million)[265]

[265] The White House, Press Release, 15 February 2000.

In addition, President Clinton requested a $9 million supplemental appropriation for FY2000 in order to jump start several of the aforementioned cyber programs prior to the start of the new fiscal year. Specifically, this funding helped establish:

1. Institute for Information Infrastructure Protection ($4 million);
2. Federal Intrusion Detection Network (FIDNET) ($2 million);
3. Federal Cyber Service programs; ($2 million) and,
4. Expert Review Team at NIST (1 million).[266]

While funding these types of programs is a prerequisite to addressing vulnerabilities brought about by technology, poor or inadequate security, and protection, government is also required to address the lack of trust regarding the security of personal information that is in the government's hands. In order to reinforce the roll of the government while obtaining and maintaining the trust of the other stakeholders, the government must endeavor not to involve itself in activities that will result in the abdication of citizen's rights of privacy. Thus, a major concern in the fight to secure and protect national information infrastructures is the ability to ensure the information privacy of individuals, i.e., one's ability to control access or disclosure of information that is of a personal nature.

Creating a level of reassurance that the government is doing everything in its power to effectively secure and protect unnecessary and illegal access to personal information is a challenge for the public sector. In 2001, Representative Stephen Horn (R) of California -- in his second annual report card on computer security -- assigned federal agencies grades based on OMB reports and GAO audits. Representative Horn,

[266] Ibid.

Chairman of the House Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, stated that roughly "two-thirds of the agencies failed completely in their computer security efforts."[267] He added "[The] nation cannot afford to ignore the risks associated with cyber attacks."[268]

Overall, the National Science Foundation received the highest grade -- B+. Two other agencies scored above a grade of D -- the Social Security Administration (C+) and NASA (C-). Alarmingly, 16 out of the 24 largest federal agencies received grades of F in 2001! Thus, the average grade for federal agencies tasked with securing computer systems in 2001 was an F. Table 4 below depicts the grades assigned each agency in 2000 and 2001 by the Congressman.

Table 4. Government Report Card on Computer Security

AGENCY	2001 GRADE	2000 GRADE
Agriculture Department	F	F
U.S. Agency for International Development	F	C-
Commerce Department	F	C-
Defense Department	F	D+
Education Department	F	C
Energy Department	F	INCOMPLETE
Environmental Protection Agency	D+	D

CONTINUED

[267] Congress, House, Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations: Statement of Subcommittee Chairman Stephen Horn before the Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, 109th Cong., 2nd sess., 9 November 2001.

[268] Ibid.

Table 4. (continued)

Federal Emergency Management Agency	D	INCOMPLETE
General Services Administration	D	D
Department of Health and Human Services	F	F
Department of Housing and Urban Development	D	C-
Interior Department	F	F
Justice Department	F	F
Labor Department	F	F
National Aeronautics and Space Administration	C-	D-
Nuclear Regulatory Commission	F	INCOMPLETE
National Science Foundation	B+	B-
Office of Personnel Management	F	F
Small Business Administration	F	F
Social Security Administration	C+	B
State Department	D+	C
Transportation Department	F	INCOMPLETE
Treasury Department	F	D
Department of Veterans Affairs	F	D
Federal Average	**F**	**D-**

Chairman Horn further stated that "federal agencies rely on computer systems to support critical operations that are essential to the health and well-being of millions of

Americans. National defense, emergency services, tax collection and benefit payments all rely on automated systems and electronically stored information. Without proper protection, the vast amount of sensitive information stored on themselves [could be] subject to malicious attack."[269]

Additionally, Horn pointed to the damage caused by the Code Red[270] and Nimda[271] Internet worms that were perpetrated on computer systems in the summer and early fall of 2001 respectively, as evidence of what could happen to computers without "patched" (i.e., fixed) vulnerabilities and appropriate safeguards (i.e., firewalls and/or antivirus software). "Cyber attacks have the potential to cause great damage to the nation," Horn stated. Understandably, the Information Technology Association of America (ITAA) expressed its outrage with the results of the report and called on the "federal government to take immediate and effective steps to correct the situation, saying the situation dramatizes the need for additional funds and focus."[272] "No responsible parent would stand for this kind of performance," said Harris N. Miller, ITAA President. While Harris stated that the work of protecting federal information systems would require

[269] Ibid.

[270] The Code Red worm virus appeared on July 26, 2001, and existed in the memory of computer systems. At its peak, over 300,000 users were affected.

[271] The Nimda worm was first discovered on September 18, 2001. It is a mass-mailing worm that utilizes multiple methods to spread itself.

[272] Bob Cohen, "ITAA Calls Failing Grade for Fed Cyber Security Unacceptable," *Information Technology Association of America*, Press Release 9 November 2001.

money, he conceded that "federal agencies simply do not have the funding available in their current budgets."[273]

Nonetheless, George W. Bush's administration contends that the $2.7 billion it spends on computer security each year is adequate. Mark Forman, Associate Director for Information Technology and E-government at OMB, told the Horn subcommittee that spending more money on security did not always give agencies their desired results. OMB's goals, he said, were to ensure that senior managers devoted greater attention to security and that they included security in all new business cases and budget plans. Based on the results of federal audits and governmental studies, however, federal agencies have since been tasked with improving computer security and protection of critical information infrastructures and personal information.

Government is responsible for protecting the privacy, integrity, and quality of the information, accessed or disseminated on the information highway. Consumers should expect to have a reasonable expectation that their privacy -- regarding access to and use of their personal information -- will not be compromised or violated by government entities, employers, or persons with culpable intent. Government, with the help and assistance of the private sector, will be expected to ensure that personal information is not improperly altered or destroyed and, that it is accurate, timely, complete, and relevant for the purpose for which it is provided and used. In order to achieve these objectives, however, these activities must be initiated and implemented in unison and in partnership between the sectors.

[273] Ibid., *See also,* Eric Lundquist, "Cyber-Defense Plan Needs to Stay on Target," *e-Week Magazine* (23 September 2002); available from http:// www.eweek.com/article2/0%2C3959%2C547299%2C00.asp; Internet.

The Private Sector

The nation's entire information infrastructure may be attributed to the innovation, hard work, and expertise of industries and businesses that comprise the private sector. Further, while private industry may be credited with the creation and development of 90% of the nation's information infrastructure, they also share an equal percentage of the vulnerabilities that have dispersed throughout the infrastructure.

America's information industries and the progress they make in deploying the broad set of information technologies that fit under the umbrella of "national information infrastructure," have had, and will continue to have, substantial leverage on every aspect of our economic and social well being, national competitiveness, and security. As a result of the extensive role they play in the development of the information nucleus, the private sector must now play an integral role in and share the responsibility of securing and protecting our information nerve centers.

Virus attacks and denial of services are the most damaging and costly forms of attacks on the private sector. Mark Rasch, Senior Vice President and Legal Counsel for Global Integrity Corporation testified before Congress[274] that in addition to viruses and denial of service assaults, "attack categories are becoming less exclusive and exhaustive and more mutually inclusive. In addition to the above mentioned [virus and denial of services] attack types, we have seen as many as ten different others, namely:

1. Theft of Intellectual Property;
2. Sabotage to systems and networks;

[274] Congress, House, Subcommittee on *Government Management, Information, and Technology*: Testimony of Mark Rasch before the Subcommittee on Government Management, Information, and Technology, 108 Cong., 1st sess., 9 March 2000.

3. System Penetration by an external party;
4. Insider Abuse;
5. Financial Fraud;
6. Denial of Service;
7. Virus;
8. Unauthorized Insider Use of systems;
9. Web Attacks and Defacement; and
10. Other."[275]

Rasch explained that there was a secondary form of attack occurring as well. This, according to him, was distinct from the attacks that were directed on corporate systems and networks described above and quite possibly the most damaging to businesses, because of the lasting effects of the damage. These assaults, he observed, were typically initiated by persons who were employed by a company and wished to do damage to the organization "by their posting and communication on the Internet and World Wide Web. Either originating from inside their workplace or from home, human communication on-line has increased the vulnerability of corporate information assets."[276] Rasch's company assessed the on-line threat to include seven major categories:

1. The disclosure of client related information;
2. Overt threats to personnel or facilities;
3. Disclosure of stock pricing and stock manipulation;
4. The disclosure of technical information about corporate systems and network architecture;

[275] Ibid.

[276] Ibid.

5. Disclosure of intellectual property information and/or research and development secrets;
6. Trademark violations; and
7. Other.

This type of assail -- given its origins, i.e., employee malfeasance -- is incredibly damaging to an organization and can leave the company extremely vulnerable to its competitors. Further, given its nature, the wealth of information the employee has or has exposed to the public or their competitors, and the employee's intent to destroy or embarrass the corporation, this type of attack could cripple a company in the marketplace, both at home and abroad.

In addition, local, state, and federal law enforcement offices are now faced with a new and different type of criminal activity – computer crime. While this field of law enforcement is steadily increasing and the law enforcement community is doing everything in its power to address the violations as they occur, computer crimes are having damaging effects on businesses, e.g., intellectual property thefts, the economy, specifically financial markets, and potentially our relationships with other nation-states and foreign entities. This type of activity coupled with the increase in cyber attacks, the problems of computer security, in general, and Internet related security, in particular, will undoubtedly increase the level of concerns and pose considerable economic challenges all around.

A 2002 Computer Security Institute/FBI Computer Crime and Security Survey indicated that computer crime and other information security breaches were still on the rise, and the cost was increasing. For example, 90% of the 503 respondents in the survey reported computer security breaches within the twelve months prior to the survey. Furthermore, the total financial losses for the 223 organizations that could quantify them added up to $455,848,000 (up from $265,586,240 in 2000) -- a 100% increase in reported losses over the 2000 figure.[277] To summarize, attacks on networks can lead to lost money, time, products, reputations, loss of sensitive information and even lives.

Compromised information networks and attacks targeting the Internet are without question the most costly forms of invasion experienced in modern time. As a global leader in information and communications technology products and services, it is presumed the United States incurs the greatest amount of economic loss. Furthermore, U.S. spending in this area represents almost 35 percent of global spending and it has increased almost 70 percent since 1992, to almost $762 billion in 1999. Domestically, this technology has achieved a compound annual growth rate of 7.8 percent, compared to 7.5 percent for the rest of the world. It has also been an incredibly powerful source of American employment and job growth. According to the Information Technology Association of America (ITAA), approximately 10.4 million people earn their livings performing information technology jobs, 85 percent of this group work for small companies.[278]

With this said, the private sector must have primary responsibility for the design, deployment, operation, and protection in order to secure the domestic information

[277] Mindy McDowell, "Who's Securing Networked Systems?" *InfoSec Outlook.* 1, no. 6 (Washington, D.C.: The Information Technology Association of America, 2001).

[278] Digital Planet, *World Information and Technology Services Alliance and IDC,* (November 2000).

infrastructure.[279] While this effort cannot be achieved by a single entity, the primary players by default -- based on their business function -- must be the telecommunications companies, those who are involved in the evolution of the Internet, and cable companies. They will continue to build and manage the networks, provide the information tools, and much of the information that travels the networks, and develop many of the applications that use the networks. Most important among these is the integration of the disparate technologies and an ability to develop the technological tools to secure the networks from attacks.

The Consumer

One of the most significant developments to come out of this expansive form of information networks was the sudden growth of mainstream awareness of the Internet. This explosion of knowledge and usage surrounding this modern technology represents a dramatic crossover into popular culture for a medium that until very recently was obscure and limited only to the scientific community or elite. Further, the modern technology portends a new Internet demographic that is likely to change the state of the Internet more profoundly than growth, new services, or even newer technology.[280]

As consumers continue to make their contributions to the information infrastructure, people from all walks of life -- factory workers, teachers, physicians,

[279] See, Diane Frank, "Clarke Presses Industry on Security," *Federal Computer Week* 5 December 2001.

[280] This includes the elderly, school aged children, physically challenged, etc. *See also,* Lyman Chapin, "The State of the Internet," *Telecommunications* 28, no. 1 (January 1994): 13-16.

children, and civil servants -- will spur growth in the U.S. economy and increase national competitiveness and, information will become an accepted form of currency in our society.[281] As they become comfortable in their role as contributors and participants in the information infrastructure they must understand their responsibilities relative to the vulnerabilities that exist in it. While the private sector has a responsibility as information collectors to inform individuals why they want personal information, the individual also has a responsibility to understand the consequences of providing personal information to others. Therefore, the individual consumer is responsible for obtaining adequate, relevant information about the purpose for which the information that is being sought shall be used, the safeguards avoiding its misuse, their rights to withhold the information, and any rights to redressal.

Another interesting yet valid perspective on this discussion is the consumer's lack of confidence in the public sector's ability to adequately and efficiently protect and secure personal information. Additionally, the average consumer does not have a high level of confidence that the government will adequately protect the Internet and computer systems.[282]

[281] Eric Benhamou, "NII Development," *Telecommunications* 28 no. 1 (January 1994): 23-24.

[282] Tinabeth Burton, "ITAA Poll Finds Almost Three of Four Americans Concerned about Cyber Security," *Information Technology Association of America*, Press Release, 11 December 2001; available from http://www.itaa.org/news/pr/PressRelease.cfm?ReleaseID=1008095083; Internet. An analysis of this poll also appeared in the following article written by David Aponovich. "Poll: Americans Fear Cyber Attacks," *CIO Information Network*, 12 December 2001; available from http://cin.earthweb.com/news/article.php/10493_939191; Internet.

In a poll taken of 800 adults by the Information Technology Association of America (ITAA) and the security software company Tumbleweed Communications in November 2001, 74% of Americans feared their government-held personal information could be stolen or used for malicious purposes. Similarly, 74% said they were worried about terrorists using the Internet to launch cyber attacks against critical infrastructure assets like telephone networks or power plants.[283] This poll was taken shortly after the deadly terrorist attacks on the World Trade Center in New York City and the Pentagon in Arlington, VA on September 11, 2001, when emotions were still very high. It reinforced the importance which businesses should give to investing in infrastructure security and thereby, calming the fears of their customers.

While the terrorist attacks of September 11, 2001, "destroyed lives and property...[t]hey also destroyed peace of mind for many people using the Internet. In an era of great uncertainty, a perceived lack of Internet security is generating high anxiety in cyberspace. These survey findings tell me that government, industry and computer users must work together to slam the lid on cyber criminals, terrorists and hackers and to restore the faith of the online community."[284]

While the private sector gingerly attempts to calm public fears, several consumer protection groups have sprung up in order to provide a check on industry and to ensure that the rights of the end-user are protected. Thus, as the everyday consumer goes about his or her role as stakeholder in the use and distribution of information, consumer protection groups such as Computer Professionals for Social Responsibility (CPSR),

[283] Ibid.

[284] Ibid., quoting ITAA President Harris N. Miller.

Electronic Frontier Foundation (EEF), Clearinghouse on Computer Accommodation (COCA), and the American Library Association's Intellectual Freedom Committee, to name a few, serve to protect the rights of various groups of users of information.[285]

Such groups are important for ensuring that consumer's rights, such as privacy, security, rights to intellectual property, are not transgressed by overly zealous regulators or profit motivated providers of the networks and services.

Developing a National Strategy

Given the origins and status of the information infrastructure, i.e., vulnerabilities, which exist in the United States, the information sharing that was called for in the Computer Security Enhancement Act of 1997 and Presidential Decision Directive 63 must come to bare. While the federal government has been forthright and ever willing to share information with the private sector -- relative to the formulation of security policies, the nature of security and information breaches, and infrastructure protection strategies -- the private sector has been less than accommodating and unwilling to reciprocate.

[285] Computer Professionals for Social Responsibility (CPSR) is an alliance of computer scientists and others interested in computer technology's impact on society; Electronic Frontier Foundation (EEF) is a civil liberties group with a mission to protect privacy, free expression, and public access to information in new media; Clearinghouse on Computer Accommodation (COCA) is located within the General Services Administration (GSA) an agency of the federal government. Since 1985, COCA has been pioneering information policies and computer support practices that benefit federal employees with disabilities as well as members of the public with disabilities. Today, COCA provides a variety of services to people within and outside government employment. The ultimate goal of all COCA's activities is to advance equitable information environments consistent with non-discriminatory employment and service delivery goals; and, the American Library Association's Intellectual Freedom Committee's goal is to educate librarians and the general public about the nature and importance of intellectual freedom in libraries.

Industry leaders base their apprehension and skepticism for sharing information with the federal government on some factors including:

1. Proprietary concerns that will leave some businesses vulnerable to their competitors; thereby placing their competitive advantage at risk in the marketplace.
2. Fundamental distrust of government's use of sensitive business information and data and, how that information may be used against a company should the information become subject to Freedom of Information Act (FOIA) requests.
3. An unwillingness to disclose situations when security systems and computer firewalls may have been breached, i.e., hacked into, and information integrity compromised for fear of the public backlash that may follow.

In order to effectively address information infrastructure security and protection, specific national actions must be taken; however, these actions cannot be taken in a vacuum. Moreover, a public-private partnership must be established in order to develop a comprehensive national plan. Willis H. Ware, Director of the Critical Technologies Institute - RAND Corporation, detailed a National Action Plan – "in the nature of 'getting started' and 'understanding the scene'."[286] His Plan was based on seven actions that were in some cases strictly the responsibility of government, and in other cases government and/or private sector initiatives. While Ware's Action Plan called for a response to address the information infrastructure vulnerability issues from both the public and private sectors and, in some instances might be "undertaken concurrently", the plan primarily focused on government's role. The plan also and puts forth suggestions that were clearly oriented toward a governmental response.

[286] Willis H. Ware, *"The Cyber-Posture of the National Information Infrastructure,"* RAND Corporation; available from http://www.rand.org/publications/MR/MR976/mr976.html; Internet.

According to Ware, his Action Plan "reflects an intuitive ordering based on the following factors:

1. existing interest or activity already under way in the government;
2. near term versus longer-term importance and payoff, difficulty, and duration of the task;
3. contribution to an improved national infrastructure posture; and,
4. the calendar period over which the severity and probability of a major attack are likely to increase." [287]

Whether an approach similar to Ware's is followed or a combination of several approaches is launched, the onus will be on both the public and the private sectors to establish the requisite trust, working relationship, and information sharing agreements in order to achieve a safe and secure national information infrastructure.

Moreover, U.S. businesses will "increasingly become the point of attack for enemies of [the] United States" by hackers and national governments using sophisticated weapons such as worms and viruses that can be used for precise attacks, warned Lawrence Gershwin -- a top CIA official in testimony before a congressional committee.[288] Thus, if the public and private sectors do not work together to address the issue of securing and protecting our information infrastructures as well as the Internet,

[287] Ibid.

[288] Congress, Senate, *Joint Economic Committee*: Testimony of Lawrence Gershwin before the Senate Joint Economic Committee, 109th Cong., 1st sess., 18 June 2001. *See also,* Reuters, "Report: Many U.S. Firms at Risk for Cyberattacks," *CNN.com* (Washington) 8 January 2002; Daily Briefing, "Public, Private Sectors Advised to Share Data to Combat Cyber Attacks," *Government Executive Magazine* (19 October 2001); available from http://www.cmm.com/2002/TECH/industry/01/08/security.reut/index.html?related; Internet.

critical information systems and networks will be at greater risk of attack. Their refusal to cooperate with one another will also compromise the integrity of personal, military, and proprietary information and data.

A national strategy developed jointly between government and industry is an effective means for arriving at an agreement about respective roles and responsibilities. The purpose is to present an integrated, unified public-private strategy for government and industry to chart a common course toward achieving the overall goal of national critical infrastructure assurance. While efforts have been underway for some time to develop a national strategy in coordination with other federal departments, agencies, and the private sector, the Critical Infrastructure Assurance Office (CIAO) has a long road ahead before reaching a functional consensus.

As the stakeholders take on greater responsibilities in the development of a national strategy, it is important that their vision not become clouded by the notion of the national strategy being an end in itself. It should be part of a dynamic process in which government and industry continue to modify and refine their efforts at critical infrastructure security, assurance, and protection. Further, and as part of this dynamic, the developers of the national strategy must continue to adjust to new circumstances and refine the strategy as appropriate and when applicable.

Chapter VI

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

The Information Revolution and the technological advancements that have accompanied it precipitated a ripple effect of technical vulnerabilities that are plaguing our critical information infrastructures nationwide. While the technologies of the latter 20th century have in many ways improved our business processes, financial processes, and the ways in which we communicate, they have also contributed to a vast and far reaching problem relative to our national security.

The U.S. Congress attempted to address some of the vulnerabilities that were beginning to effect federal government business processes by passing the Computer Security Act of 1987. This Act required federal agencies to identify systems that contained sensitive information and to develop plans to safeguard them. Furthermore, agencies were required to:

1. Identify all development and operational systems with sensitive information;
2. Develop and submit to NIST and NSA for advice and comment a security and privacy plan for each system identified; and,
3. Establish computer security training programs.

The federal government, by virtue of the passage of this legislation, was beginning to seriously understand and attend to the threat to national security posed by computer vulnerabilities. Even though the Computer Security Act of 1987 was a step in the right direction, it did not close all the holes in the infrastructure.

In 1990, the General Accounting Office (GAO) examined the response and implementation of the Act. The GAO reported that as of January 1990, a mere 38 percent of the 145 planned controls had been implemented.[289] The report concluded the following:

> The government faces new levels of risk in information security because of increased use of networks and computer literacy and a greater dependence on information technology overall. As a result, effective computer security programs are more critical than ever in safeguarding the systems that provide essential government services.[290]

Having only reached a 38% compliance rate, the federal government realized the need to do more to fully and adequately protect its valuable informational assets. Unfortunately, however, instead of concentrating on making the systems more secure, the government chose to focus on the intruders, i.e., hackers, of these systems.

Ten years after the passage of the 1987 Act, the 105th Congress passed the Computer Security Enhancement Act of 1997 in order to expand the role and responsibilities of the National Institute of Standards for Technology (NIST). NIST is part of the Department of Commerce and is congressionally mandated to establish federal standards and guidelines for computer systems for the federal government. An additional function of NIST requires that the organization confer with the private sector and other federal agencies and departments in the development of standards for computer systems.

While Congress attempted to address the shortcomings plaguing the federal departments and agencies -- via legislation -- neither the 1987 nor 1997 acts adequately

[289] United States General Accounting Office, *Report on Implementation of Computer Security Act* (Washington, D.C.: Government Printing Office, 1990).

[290] Ibid.

addressed many of the vulnerabilities that have plagued our important information infrastructures. With our basic installations and facilities (e.g., electrical power grids, water, telecommunication networks, and financial services) vulnerable to attack and/or corruption, the security of the United States remained at risk. Further, with over ninety percent of the nation's infrastructure in the hands of the private sector much of the design, construction, and implementation of efficient and adequate security systems should be developed by the private sector. Given the dynamism of the technological advancements and the far reaching consequences of the vulnerabilities, it is imperative that the private sector and the public sector develop collaborative agreements to work together to develop solutions that address these problems.

Addressing the failures of the aforementioned Acts and the vulnerabilities prevalent in our nation's infrastructure became the focus of Presidential Decision Directive 63 (PDD 63) and the Clinton Administration's efforts to develop swift, flexible, and evolutionary approaches and methods. The Directive included and encouraged the participation of both the public and private sectors in order to protect America's interests both here and abroad and, ward against domestic and international terrorism. Presidential Decision Directive 63 built upon the recommendations of the Clinton administration's Commission on Critical Infrastructure Protection. This presidential Commission issued a report in October 1997 calling for a national effort to ensure the security of the nation's vulnerable and interconnected infrastructures, most notably those physical and cyber-based systems essential to the basic operations of the economy and government.[291] Thus,

[291] The White House, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998 (Washington, D.C.).

they included telecommunications, banking and finance, energy, water systems, public and private transportation, emergency services, and important government services.[292]

Presidential Decision Directive 63 may be construed as the first National Strategy articulating a Critical Infrastructure Protection Management Plan. The PDD 63 Plan was fully equipped with purpose, scope, guidelines, organization and structure, tasking, resource allocation, and a comprehensive implementation schedule. It was, and continues to be, a framework from which owners, operators, and government entities apply their funding resources and human capital to the never ending quest for full and complete critical infrastructure protection.

The Computer Security Enhancement Act of 1997 and Presidential Decision Directive 63 laid the ground work for the formulation of a relationship between the public and private sectors. Sharing the responsibility of critical infrastructure protection represented a transition to a new national cooperative paradigm. The 1997 Act encouraged the sharing of information between the public and private sectors where the public sector was mandated by Congress to provide the requisite guidance to the private sector should industry require it. PDD 63, subsequently, came along and provided a justification for public-private sector information sharing and put into motion vehicles, (e.g., Presidential Advisory Boards, Cross Industry Working Groups, etc.) to ensure its success.

Pursuant to the expectations of both the Act and the Directive, the federal government must take greater steps in protecting its own information systems, networks,

[292] Ibid., 1.

and critical infrastructure. Further, both government and industry are expected to work in unison to educate small and medium sized businesses about the importance of solutions through people and processes, not just technology. Thus, a reliance on the nation's critical installations and facilities exists for industry to run their businesses, for the federal government to carry out its governmental functions, and for the general public to access and receive services to conduct their lives.

The Information Age has necessitated a shift in the practices of the federal government. It has forced the legislative and executive branches of government, primarily, to reconsider how issues of safeguarding sensitive information and more importantly national security are addressed and what their respective roles will be in that effort. In addition, the long standing conflict that exists between the legislative and executive branches will need to be put to rest in order for these two important players to work together (in concert with the private sector) to develop federal laws and policies that address the infrastructures' security and protection.

National security, traditionally, has been recognized as the responsibility of the federal government. It fulfills that function with the collective efforts of the military, foreign policy initiatives, and the intelligence community. It defends our airspace and national borders, as well as monitors U.S. operations abroad in order to protect our national interests. With the advancements brought about by technology and the ensuing vulnerabilities that were created as a result of technological changes, the methods and approaches used to protect our national information infrastructures, (i.e., national security) were forever changed. No longer is the federal government solely responsible for putting systems in place to protect the homeland. The onus is now on the infrastructure's stakeholders -- public sector, the private sector, and to a larger extent the average citizen -- to share the responsibility for developing and implementing security measures, respectively, to ensure national security.

A national strategy is an effective way of addressing the failures in our valuable information infrastructures. The goal is to develop an integrated strategy which incorporates the needs of both government and industry in order to achieve quality infrastructure assurance. While efforts have been underway for some time to develop a national strategy in coordination with other federal departments, agencies, and the private sector, the Critical Infrastructure Assurance Office (CIAO) has a long road ahead before reaching a functional consensus.

As the stakeholders take on greater responsibilities in the development of a national plan, it is important that they remain focused on an approach that is evolutionary and not one that is static. The creation of a national strategy is not an end in itself. It should be part of a dynamic process in which government and industry continue to modify and refine their efforts at critical infrastructure security, assurance, and protection. Further, and as part of this dynamic, the developers of the national strategy must continue to adjust to new circumstances and refine, modify, enhance, and update the strategy as advancements occur and when appropriate.

Information technology is cooperative by nature and tremendous benefits can be derived from greater interconnectivity. As a result, and as we traverse the Information Age, nations have legitimate aspirations to create a global information system that adds value to their existing information infrastructures. Therefore, nations will explore various ways to integrate their networks with the international network. Once integration takes place, each connected nation will have an interest in maintaining the stability and survivability of the overall network. It is, therefore, the hope that each nation will have a vested interest in preventing global information warfare.

Given the composition of information technology and computer systems, they are arguably vulnerable by nature. As a result, taking defensive measures against a threat of information warfare will always be difficult and costly. Improving the defense of information systems also contributes to the security dilemma since decreasing one's susceptibility to information warfare increases the attraction of using information warfare offensively. In order to effectively neutralize the security dilemma presented by defensive postures, states may share defensive technologies to ensure that a defensive equilibrium is maintained. This serves dual purposes: (1) a relative balance of power is maintained among states; and, (2) the offensive threat of rogue states or terrorist groups is reduced. While states will want to ensure and maintain offensive capabilities, "just in case," security is best maintained, due to the nature of the threat, by developing defensive capabilities.

Despite collective interests and hopeful cooperation, information attacks will continue to be a viable national security concern. Unfortunately, a state's ability to control these types of attacks is currently very limited. By increasing security, gathering intelligence regarding any plans that might be in consideration, and pursuing a credible policy of deterrence, we can better ensure that the threat of information warfare (IW) is contained to isolated incidents from which the United States can recover. Unfortunately, however, the environment under which we currently operate can make no such promise; therefore, it is imperative that we effectively address these issues now.

Increasingly concerns are growing relative to the use of information warfare for blackmail, extortion, or for limited short-term gains. Such scenarios present other difficult political dilemmas that must be addressed at a global level. We must ask ourselves such probing questions as: Will we permit limited information warfare in order to pursue strategic or comparative political and economic gains? Or, is the fear of escalation an adequate deterrent to such ambitions? It is certain that the Information Age will continue to change many aspects of our society. According to Mitchell Kapor:

> Life in cyberspace is more egalitarian than elitist, more decentralized than hierarchical...it serves individuals and communities, not mass audiences. We might think of cyberspace as shaping up exactly like Thomas Jefferson would have wanted: founded on the primacy of individual liberty and commitment to pluralism, diversity, and community.[293]

The United States -- as the world's only super power -- must ensure that the infrastructure it is building has a strong foundation and that the weaknesses in that structure are not used to destroy it. This is undeniably a difficult task as the constitutionally guaranteed rights of U.S. citizens must be upheld and protected in the process. It is, however, a task we must undertake. Furthermore, it is impractical to stop the technology, but a decision must be made relative to the direction we wish the technology to take, and what rules and policies will govern its use. Methods of warfare will continue to evolve as the information revolution progresses. Finally, it will be necessary to ensure that the conceptions of national security evolve as well.

[293] Mitchell Kapor, "Where is the Digital Highway Really Heading? The Case for a Jeffersonian Information Policy," *Wired Magazine* (July 1993): 53-59.

Information warfare and information security must be incorporated into the national security of all nations interested in venturing into and making the transition into the Information Age. "Waiting for a crisis to force us to act globally runs the risk of making us wait too long."[294] In the case of information technologies we can neither afford to nor allow this to be the case fundamentally due to the fact that they are the foundation for our future.

The research reveals that as we become rooted in the Information Age it will become imperative for the legislative and executive branches of government to work together on solutions that will address the vulnerabilities that plague our critical information infrastructures. Furthermore, these two branches of government must address, in a comprehensive way, the threats of attack and destruction to our important installations and facilities -- that if carried out -- have the potential to cripple our nation. Time, energy, and money that should have been spent on discovering and fixing security bugs in the 1980s were used, instead, to design and implement an attack on hackers themselves. Additionally, this was an attack that focused only on domestic hackers[295] and did little to thwart the threat to United States national security or its interests.

[294] John L. Petersen, *The Road to 2015: Profiles of the Future* (California: Waite Group Press, 1994).

[295] The reference here is being made to Operation Sundevil. A Department of Justice, i.e., Secret Service, led operation that was by far the largest clamp down on computer crime in the United States in the 1990s. The focus of Operation Sundevil was the hackers' system of information distribution which consisted of hundreds of underground computer systems that housed information on how to break computer systems, files stolen from major U.S. corporations, and files that contained credit card access numbers used to commit credit fraud. Approximately 42 computers were seized along with 23,000 floppy disks of information during raids that occurred on May 7-9, 1990. See, Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (New York, Bantam Books, 1992), 158. Also, Paco Xander Nathan, "Jackson Wins, Feds

As we turn our attention to law enforcement, the United States has a vested interest in preventing computer crime and fraud. Further, government led sting operations to catch and prosecute those who use the computer as their weapon to commit crimes, are an effective means to address this type of unwelcome activities. The problem with utilizing this approach in isolation, however, is that it is misdirected because U.S. military systems and business systems remain open to attack or corruption. Furthermore, hackers will always exist. The most effective way to thwart their illegal activities is to plug the holes they use to gain access to critical information systems and/or critical infrastructures. The solution, therefore, is in giving a higher priority to increasing computer security via collaborative legislation which proactively seeks input from industry leaders and the executive branch with an eye towards that which is being practiced abroad. Anything short of this approach would be shortsighted and rendered ineffective.

In order to strengthen the homeland -- via the protection and security of critical information installations – the research reveals that we must change the way we think about network security and, use this awareness to create and institute a collaborative solution. Furthermore, we need to set clear, tangible goals with concrete timelines that will move us forward to it. In addition, we need to be able to identify our progress toward security just as clearly as we can now identify our vulnerabilities. As we address these issues, we need to, concurrently, remain serious and dedicated to understanding the

Lose," *Wired* (May 1993): 20. Nathan's article details the highly publicized case of Steve Jackson Games, where the proprietor, Steve Jackson, after unknowingly hiring a hacker, becomes the target of a Secret Service sting operation that nearly caused his company into bankruptcy. After filing suit against the Secret Service, Steve Jackson Games won the law suit and received compensation in the amount of $52,000 plus legal fees.

importance of cyber security, and the implication of inaction and a failure to effectively defend the nation's critical infrastructures. As we have learned, given the exponential financial losses over the years, complacency is no longer an option.

Given this new environment, the denial of service attacks that we now face today should be likened to the failed World Trade Center bombing of 1993; thus, a mere harbinger for a future strike that has devastating success.[296] Notwithstanding the efforts in more recent years to address the cyber threat, there has long been a disconnect between the recognition of the cyber threat and the allocation of resources to manage it. High-level officials from the public sector and senior executive management from the private sector have discussed the issue in various forums and they have even strategized over possible defenses. Yet, year after year, the number of attacks grows, while cyber-defense budgets remain significantly low.[297]

Cyber security needs to be a management priority in both the private and public sectors of the highest order. Without question, the nation's critical infrastructure is subject to a terrorist or military strike. It is simply just a matter of time before an attack occurs. Further, homeland defense is a business concern and should become a business priority. Network security cannot be left in the hands of information technology departments and technical staffs only; management must be expected to be an active

[296] The ultimate goal of this terrorist act was the complete demolition of one of the World Trade Center buildings. The attempts of the terrorists in this regard failed in 1993. The plan would ultimately be carried out on September 11, 2001 with the total demolition of the World Trade Center buildings.

[297] Lundquist, "Cyber-Defense Plan Needs to Stay on Target." See also, Frank Cilluffo, Joseph C. Collins, Arnaud de Borchgrave, Daniel Goure, and Michael Horowitz, "Defending America in the 21st Century: New Challenges, New Organizations and New Policies," *CSIS* (Washington, DC: 2000): 8, 15, 23.

participant and they must be held accountable.[298] According to Bill McVay, a senior policy analyst in the Office of Information and Regulatory Affairs – Office of Management and Budget (OMB), "the rate of change in information technology requires us to have a strong governance process. While the government will not become a dot-com", it will apply technologies that will require it to become a "click-and-mortar" type of organization that provides services both on-line and by traditional means.[299]

Given the foundation laid out by such Acts as the Computer Security Act of 1987, the Computer Security Enhancement Act of 1997, and the steps taken by the Clinton Administration beginning with the 1993 National Performance Review (NPR)[300] to improve government on many levels, the Bush Administration has begun to build upon these laws and policies. The Bush Administration has issued and is attempting to put in place National Strategies that address *Homeland Security, Cyber Security, and The Physical Protection of Critical Infrastructures and Key Assets* to name just a few as well as countless Presidential and National Security Decision Directives, e.g., National Security Presidential Directive 16.[301] The tragic events of September 11, 2001,

[298] Liza Porteus, "Management, Not Technology, Is The Problem, OMB Says." *Government Executive Magazine* (19 February 2002); available from http://www.govexec.com/dailyfed/0202/021902td.htm; Internet.

[299] Ibid.

[300] National Performance Review (NPR – now known as the National Partnership for Reinventing Government); Government Performance and Results Act (GPRA) of 1993 (also known as the Balanced Scorecard); Federal Acquisition Streamlining Act of 1994, the Government Management Reform Act of 1994, and the Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act) to name just a few.

[301] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *Washington Post*, 7 February 7 2003, sec. A01. National Security Presidential Directive 16 is a secret directive ordering the government to develop, for the first time, national-level guidance

undoubtedly precipitated many of the policy initiatives to come out of the Bush White House but, arguably, this president has been able to build upon much of what had been developed during the Clinton years.

Information infrastructures are vulnerable to attack. While this in itself poses a national security threat, the linkage between information systems and traditional critical infrastructures has increased the scope and potential of the information warfare threat. For economic reasons, increasing deregulation and competition create an increased reliance on information systems to operate, maintain, and monitor critical infrastructures. This in turn creates a tunnel of vulnerability previously unrealized in the history of conflict. Information warfare offers a veil of anonymity to potential attackers who can hide in the mesh of interwoven systems and often use previously conquered systems to launch their attacks.

The lack of geographical, spatial, and political boundaries offers further anonymity, legal, and regulatory harbor. This absence of traditional boundaries also invalidates previously established "nation-state" sanctuaries.[302] Information warfare is also relatively cheap to wage, offering a high return on investment for resource-poor adversaries. The technology required to mount attacks is relatively simple and

for determining when and how the United States would launch cyber-attacks against computer networks.

[302] Congress, Senate, Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information, *Crime, Terror, & War: National Security & Public Safety in the Information Age*: Hearing before the Judiciary, Subcommittee on Technology, Terrorism, and Government Information, 106th Cong., 1st sess., 13 November 1998.

ubiquitous. During the warfare, demand for information will dramatically increase while the capacity of the information infrastructure will most certainly decrease. The law, particularly international law, is currently ambiguous regarding criminality in and acts of war on information infrastructures. This ambiguity, coupled with a lack of clearly designated responsibilities for electronic defense, hinders the development of remedies and limits response options.

The current Administration's national security strategy for the United States suggests that the nation's economic and security interests are increasingly inseparable and that we simply cannot be successful in advancing our interests -- political, military and economic -- without active engagement in world affairs. In the broad sense, then, the scope of national information interests to be defended by information warfare defense and deterrence capabilities are those political, military, and economic interests. These include the continuity of a democratic form of government and a free market economy, the ability to conduct effective diplomacy, a favorable balance of trade, and a military force that is ready to fight and that can be deployed where needed. These interests are supported by the delivery of goods and services that result from the conduct of functional activities such as manufacturing, governing, banking and finance, and the like. Some of these activities are critical to the nation's political, military, and economic interests. These critical functional activities, in turn, depend on information technology and critical infrastructures such as banking and finance, electric power, telecommunications, and transportation.

In general, U.S. infrastructures are extremely reliable and available because they have been designed to respond to disruptions, particularly those caused by natural phenomena. However, deregulation and increased competition cause companies operating these infrastructures to rely more and more on information technology to centralize control of their operations, to support critical functions, and to deliver goods and services. Centralization and reliance on broadly networked information systems increase the vulnerabilities of the infrastructures and the likelihood of disruptions or malevolent attacks.

The information users who can be attacked through the shared elements of the national information infrastructure are those responsible for performing the critical functions necessary for the delivery of the goods and services upon which our political, military, and economic interests depend. The federal government must preserve its ability to fulfill its basic missions. To do that, government must be concerned about the ensured operation of the critical functions and the availability of information necessary to fulfill those missions. The intertwined nature of the functions of national interest and supporting infrastructures add to the complexity: there are critical functions which have national security implications and which must be defended; and there are critical portions of the infrastructures which are necessary for the operation of government and national functions.

Recommendations

As we endeavor to secure our cyber networks and protect our critical information installations, facilities, etc., we have learned that reacting after the fact is not good enough. We must stop the attack from happening or address the threat before the attack occurs. Rather than fight wars, we need to prevent conflicts. This profound shift in our national security paradigm will require a new approach complete with political, diplomatic, economic, psychological, and moral dimensions unlike any other we have seen. This is a mindset that stresses collaboration, information sharing, and trust.

In consideration of offering some recommendations to effectuate meaningful change in this area, it will be useful to consider maximizing our economic interdependence. This approach will likely detract from the advantages of state sponsored information warfare. Richard Cooper presents one of the most useful definitions of economic interdependence when applying the term to information warfare. He uses the term to "refer to the sensitivity of economic transactions between two or more nations to economic developments within those nations."[303] Focusing on economic sensitivity allows us to disregard conventional measures such as trade surpluses and deficits and look at the interlinked effects of economic stability between interdependent nations.

As applied to information warfare, our focus must be upon the extent to which interdependent nations are likely to feel the economic aftershocks of economic instability. If the United States were to become a victim of information warfare and, specifically an attack directed at our financial institutions, what effect would this type of attack have on

[303] Richard N. Cooper, "Economic Interdependence and Foreign Policy in the Seventies," *World Politics* (January 1972): 159.

the economic stability of the European Union states, Japan, or perhaps the nations of the Pacific Rim, and the Middle East? If interdependence is to act as a deterrent to information warfare, then levels of interdependence must be high enough as to ensure that the costs of waging information warfare outweighs the benefits. To cite Rosecrance and Stein, the interdependence of the financial system is now formal because we have vested interests in not letting the reserves of foreign currencies drop below a certain threshold which would harm our own economy.[304]

Realizing the devastating economic effects of waging an information war, interdependence will act as a disincentive to state-sponsored information warfare. This type of interdependence introduces complex variables into offensive information warfare strategies. Joseph Nye argues that there is power to be derived from making oneself less interdependent with other nations.[305] This is especially true as applied to information warfare. The effectiveness of offensive information warfare is increased as benefits exceed costs. One benefit of less interdependence with the target nation is that economic aftershocks will have less effect on the aggressor's economy. Decreasing economic interdependence might be seen as a precursor to waging information warfare, but it is not a readily realizable goal for most technologically advanced nations.

Reducing levels of economic interdependence is costly for two reasons: the benefits of interdependence can no longer be extracted and distributed among the citizenry, perhaps decreasing a nation's prosperity; and domestic political constraints can

[304] Richard Rosecrance and Arthur Stein, "Interdependence: Myth or Reality?" *World Politics* 26, no. 1 (1973): 1-27.

[305] Joseph S. Nye, *Understanding International Conflicts* (New York: Harper Collins, 1993), 166.

disrupt the nation's internal balance of power. Moreover, the domestic sectors of society that benefit from interdependence -- for example, multi-national corporations, financial institutions, and other investors -- will likely attempt to impact interests to prevent the breaking of interdependent links.[306]

In addition to the aforementioned discussion relative to recommendations for improving our current state of securing our critical information infrastructures, systems, and networks, the following is provided for additional consideration in the development of a new paradigm for national security in an uncertain world:

1. Increase information sharing efforts. Information sharing and analysis centers (ISACs) must be established where they do not exist in critical infrastructure sectors. Public–private information sharing must be expanded and inclusive. Those legal barriers that currently exist which inhibit adequate and effective industry cooperation, for example anti-trust laws, and, those issues impacting the industry-government relationship directly, for example the Freedom of Information Act, must be addressed immediately. What we learned in the wake of September 11, 2001, was not that we did not have enough data. In fact, just the opposite is true -- government is virtually drowning in data. The real challenge is information -- that is, putting the pieces together to make sense of what we have. Further, this

[306] Jack Snyder, *Myths of Empire: Domestic Politics and International Ambition.* (Ithaca: Cornell University Press, 1991).

understanding must be accomplished quickly. So that, in the case of first responders, for example, the central issue is getting the right information to the right people at the right time. That means sharing information across disparate organizations, systems, and databases.[307]

2. Increase critical infrastructure threat and defense awareness. Greater attention and resources are required in order to sufficiently explore and address the physical threat to critical infrastructure networks. This issue must be addressed by both the public and private sectors in order to fully comprehend the requirements for critical infrastructure protection and security. (CIP) must be viewed as a task of the highest priority and, more importantly, treated as such. We must anticipate the possibility of a network attack being combined with a physical attack and, what our defense will be.

3. Increase the amount of spending allotted to critical infrastructure defense, i.e., protection and security. While the Bush White House has recently issued a National Strategy to Secure Cyberspace,[308] a comprehensive yet effective plan is required -- with the requisite

[307] This includes a hodge podge of federal departments and agencies: DoD, FBI, FDA, FEMA, FAA, INS, CIA, and many more; State and local governments – typically viewed as the first responders to crisis; Companies that hold related information, such as bank records or health data, or manage elements of the infrastructure.

[308] The White House, “The National Strategy to Secure Cyberspace” (February 2003).

budgetary outlays -- to address cyberspace security. Thus, if the public and private sectors can increase spending for the security of computer and network systems the likelihood of damaging and crippling cyber attacks on critical infrastructures will be limited. Furthermore, recovering from a cyber attack is always more expensive than funding the resources to prepare for one; thus, upfront sacrifices relative to budgetary spending in the name of prevention is necessary. According to statistics, the federal government was estimated to have spent roughly $3 billion to address the Y2K (year 2000) crisis. One should expect the federal government to spend at least that amount if not much more on securing the nation's critical infrastructures and the Internet.

4. Training and education must be increased for persons responsible for developing the federal response to securing and protecting the infrastructures. As we step deeper into the Information Age the government faces the possibility of a terminal shortage of qualified technical staff to fill its critical infrastructure protection needs. Proposals to provide education grants and subsidies to or forgive the student loan debts of technical workers who accept positions in the government needs to be reexamined, further evaluated, and ultimately instituted. Continuous and relevant computer and network training and other forms of continuing education should be used as an

incentive not only for bringing in new personnel, but also for keeping the government's cyber-defense employees in their jobs. This will reduce the attraction to private sector jobs and lessen its appeal; thereby strengthening the personnel skill sets of government employees and re-establishing a government that is abundant in its human resource capabilities.

5. Develop a public-private sector endorsed strategy for critical infrastructure attack survivability. The successful response to and recovery from a critical infrastructure attack depends on the ability to ensure the continued functioning of the networks that are hit. Thus, network redundancy is required. This should include the development of wholly separate networks for crucial government functions. Furthermore, the establishment of a separate agency (or perhaps the creation of a new bureau in the newly formed Department of Homeland Security) to specifically address cyber attack response and recovery scenarios is required immediately. This will minimize the potential catastrophes and long lasting effects that may be caused by an electronic Pearl Harbor. Reinforce the roles of the public-private sector working groups and require them to provide periodic, e.g., quarterly, briefings to a federal Computer Information Officer (CIO). The position of a federal CIO would have to be established as recommended in the E-Government Act of 2001 (S. 803). It is further

recommended that this individual report directly to the President of the United States as part of the president's Cabinet and not as part of OMB as recommended in the E-Government Act. This position should be appointed by the president and confirmed by the Senate.

6. Develop a coordinated international cyber security approach to facilitate the investigation and punishment of cyber-crimes. Efforts to address critical infrastructure protection cannot be developed and/or applied from the perspective of the United States exclusively. This is not an issue that is now or will ever be strictly a concern of the United States. All nations that depend on the efficiency of domestic or global cyber networks have a stake in critical infrastructure protection. As a result, it is incumbent upon the U.S. to take the lead in developing international coordination of cyber-crime laws and cross-border sharing of information on cyber threats and attacks. Moreover, we must endeavor to establish connectivity and liaisons with other countries so that information can be shared. These efforts will prove to be invaluable and crucial to stemming the global expansion of cyber-crime and corruption. Further, the creation of an international cyber policing organization -- InterCyberPol -- that would be responsible for the electronic surveillance, monitoring, and detection of cyber crimes that impact many nations is important. For example, on-line Child Pornography that involves the transport of children for

purposes of pornography internationally; hacking activity involving the access of military sites and government entities.

7. Greater bicameral and bipartisan participation in the development of cyber-crime and critical infrastructure protection laws in the Congress that take privacy concerns into account. One of the barriers to information sharing and developing new legislation is the understandable concern about privacy and security of the data. This creates a familiar tension in government: the demand to move information quickly to achieve results versus the need to protect information to feel comfortable sharing it. Congress is obliged to develop laws that protect the nation and its citizenry. Given the prevalence of the technology, its impact on daily life and, the operations of business, Congress must be expedient in the establishment of new laws that address the pervasive change, being mindful, of course, of the rights to privacy all Americans are entitled to enjoy under the Constitution.

8. Improved Executive-Legislative relationships. As we continue to traverse the information age it will become increasingly more important for the Executive and Legislative branches of government to work in unison to address critical infrastructure protection and security matters.

In closing, although debated in military and defense circles, very little work has been done in the field of political science to examine security issues related to information technology.[309] Political scientists and leaders must recognize and examine the threat posed by new technologies and how they will affect both our national and international political relationships. This is a growing and emerging field that has far reaching implications in the social sciences -- namely political science.

The time is now for political scientists, students of the discipline, and enthusiasts of the field to become involved in the debate over the political ramifications and impacts that have accompanied the technological advancements of the Information Age.

[309] Eugene B. Skolnikoff, *The Elusive Transformation: Science Technology and the Evolution of International Politics.* (New Jersey: Princeton University Press, 1993), 169.

APPENDIX

Glossary of Terms

- A -

Access: The ability to enter a secured area. The process of interacting with a system. Used as either a verb or a noun.

Access Authorization: Permission granted to users, programs or workstations.

AOL: America On-line.

APC: Association for Progressive Communication – an organization that links approximately 20,000 non-governmental organizations (NGOs) ad individual members in 95 countries via e-mail and facsimiles. APC's membership includes Greenpeace, Amnesty International, the Sierra Club, many unions, and peace organizations.

Authenticate: In networking, to establish the validity of a user or an object (i.e. communications server).

Authorization: The process of determining what types of activities are permitted. Usually, authorization is in the context of authentication. Once you have authenticated a user, the user may be authorized different as of access or activity.

Availability: The portion of time that a system can be used for productive work, expressed as a percentage.

- B -

Bandwidth: Capacity of a network or data connection, often measured in kilobits/second (kbps) for digital transmissions.

BARC: Bhabha Atomic Research Center.

Business-Critical Applications: The vital software needed to run a business, whether custom-written or commercially packaged, such as accounting/finance, ERP, manufacturing, human resources, sales databases, etc.

- C -

CEO: Chief Executive Officer.

CERT: The Computer Emergency Response Team was established at Carnegie-Mellon University after the 1988 Internet worm attack.

Challenge/Response: A security procedure in which one communicator requests authentication of another communicator, and the latter replies with a pre-established appropriate reply.

CIA: Central Intelligence Agency.

CIAO: Critical Infrastructure Assurance Office.

CIO: Chief Information Officer.

CIP: Critical Infrastructure Protection.

Client/Device: Hardware that retrieves information from a server.

COCA: Clearinghouse on Computer Accommodation.

Coded File: In encryption, a coded file contains unreadable information.

Communications Server: Procedures designed to ensure that telecommunications messages maintain their integrity and are not accessible by unauthorized individuals.

Computer Security: Technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system.

Countermeasure: [As defined by the CSTB.] An added step or improved design that eliminates the vulnerability and renders a threat impotent. Also known as “safeguard”.

CPSR: Computer Professionals for Social Responsibility.

Critical Infrastructure: Categorized as information and communications; banking and finance; water supply; aviation; highways, mass transit, pipelines, rail, and waterborne commerce; emergency, fire, and continuity of government services; public health services; electrical power, oil and gas production, and storage.

Cryptography: A one-way function applied to a file to produce a unique "fingerprint" of the file for later reference.

CSPP: Computer Systems Policy Project. A leading information technology advocacy organization comprised exclusively of CEOs that develop and advocate public policy position on trade and technology policy issues.

CSTB: Computer Science and Telecommunications Board.

- D -

DARPA: Department of Defense Advanced Research Projects Agency.

Data Driven Attack: A form of attack in which the attack is encoded in innocuous-seeming data which is executed by a user or other software to implement an attack. In the case of firewalls, a data driven attack is a concern since it may get through the fir-firewall in data form and launch an attack against a system behind the firewall.

Data Encryption Standard: An encryption standard developed by EBM and then tested and adopted by the National Bureau of Standards. Published in 1977, the DES standard has proven itself over nearly 20 years of use in both government and private sectors.

Decode: Conversion of encoded text to plain text through the use of a code.

Decrypt: Conversion of either encoded or enciphered text into plaintext.

Dedicated: A special purpose device. Although it is capable of performing other duties, it is assigned to only one.

Defense in Depth: The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.

DES: Data encryption standard.

DHS: Department of Homeland Security.

DOD: Department of Defense.

- E -

E-Commerce: Electronic Commerce.

EEF: Electronic Frontier Foundation.

E-mail Bombs: Code that when executed sends many messages to the same address(s) for the purpose of using up disk space and/or overloading the E-mail or web server.

ENAIC: Electronic Numerical Integrator and Computer.

Encryption: The process of scrambling files or programs, changing one character string to another through an algorithm (such as the DES algorithm).

End-to-End Encryption: Encryption at the point of origin in a network, followed by decryption at the destination.

Environment: The aggregate of external circumstances, conditions and events that affect the development, operation and maintenance of a system.

ERP: An acronym for Enterprise Resource Planning systems that permit organizations to manage resources across the enterprise and completely integrate manufacturing systems.

- F -

FAA: Federal Aviation Administration.

FBI: Federal Bureau of Investigations.

FDA: Food and Drug Administration.

FEMA: Federal Emergency Management Agency.

FIDNET: Federal Intrusion Detection Network.

Firewall: A system or combination of systems that enforces a boundary between two or more networks.

FOIA: Freedom of Information Act.

- G -

GAO: General Accounting Office.

Gateway: A bridge between two networks.

GITS: Government Information Technology Services.

Global Security: The ability of an access control package to permit protection across a variety of mainframe environments, providing users with a common security interface to all.

GPRA: Government Performance and Results Act (also known as the Balanced Scorecard).

- H -

Hack: Any software in which a significant portion of the code was originally another program.

Hacker: Those intent upon entering an environment to which they are not entitled entry for whatever purpose [entertainment, profit, theft, prank, etc.]. Usually iterative techniques escalating to more advanced methodologies and use of devices to intercept the communications property of another.

Hacktivist: A person with computer knowledge and skill who converges hacking with activism; where "hacking" is used here to refer to operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software

HERF: High Energy Radio Frequency.

HPCA: High Performance Computing Act of 1991 (S. 272). Legislation that was introduced by Senator Albert Gore to initiated the concept of a national data superhighway.

HPCP: High Performance Computing Program. Part of the 1993 HPCA (see above) this program was to provide large economic and social benefits to the entire country. The benefits expected included new teaching tools, digital libraries of electronic information, standards and protocols for making government information readily accessible by electronic means, and upgrading health care computer systems.

- I -

Information Age: Characterized based on the widespread proliferation of emerging information and communication technologies that provide mankind the capability to overcome the barriers imposed on communications by time, distance, and location by minimizing the limits and constraints inherent in human capacities to process information and the ability to make decisions.

Information Systems Technology: The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information.

Information Superhighway, IWay, InfoBahn: See NII (National Information Infrastructure).

Information Warfare (IW): Involves actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. (DOD Directive 3600.1).

INS: Immigration and Naturalization Service.

Insider Attack: An attack originating from inside a protected network.

Internet (The Beginning): The Internet had its roots in early 1969 when the ARPANET was formed. ARPA stands for Advanced Research Projects Agency (which was part of the U.S. Department of Defense). One of the goals of ARPANET was research in distributed computer systems for military purposes. The first configuration involved four computers and was designed to demonstrate the feasibility of building networks using computers dispersed over a wide area. The advent of OPEN networks in the late 1980's required a new model of communications. The amalgamation of many types of systems into mixed environments demanded better translator between these operating systems and a non-proprietary approach to networking in general. Telecommunications Protocol/Internet Protocol {TCP/IP) provided the best solutions to this.

Internet (TOM): A web of different, intercommunicating networks funded by both commercial and government organizations. It connects networks in 40 countries. No one owns or runs the Internet. There are thousands of enterprise networks connected to the Internet, and there are millions of users, with thousands more joining every day.

Intrusion Detection: Detection of break-ins or break-in attempts either manually via software expert systems that operate on logs or other information available on the network.

ISACs: Information Sharing and Analysis Centers.

ISSA: Information Systems Security Association.

ITAA: Information Technology Association of America.

- J -

[No Entries]

- K -

Key: In encryption, a key is a sequence of characters used to encode and decode a file. You can enter a key in two formats: alphanumeric and condensed (hexadecimal). In the network access security market, "key" often refers to the "token," or authentication tool, a device utilized to send and receive challenges and responses during the user authentication process. Keys may be small, hand-held hardware devices similar to pocket calculators or credit cards, or they may be loaded onto a PC as copy-protected, software.

- L -

LBL: Lawrence Berkley Laboratory.

Local Area Network (LAN): An interconnected system of computers and peripherals, LAN users share data stored on hard disks and can share printers connected to the network.

- M -

Multi-User: The ability for multiple concurrent users to log on and run applications from a single server.

- N -

NASA: National Aeronautics and Space Administration.

Network Computer (NC): A "thin" client hardware device that executes applications locally by downloading them from the network. NCs adhere to a specification jointly developed by Sun, IBM, Oracle, Apple and Netscape.

Network Computing Architecture: A computing architecture in which components are dynamically downloaded from the network into the client device for execution by the client. The Java programming language is at the core of network computing.

NGO: Non-governmental organizations

Network Worm: A program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability or availability, A network worm may attack from one system to another by establishing a network connection. It is usually a self-contained program that does not need to attach itself to a host file to infiltrate network after network.

NII: National Information Infrastructure. Also known as the Information Superhighway, IWay, and InfoBahn. The NII is the physical and virtual backbone of an information society comprised of systems and networks that include financial networks, private corporate and institutional networks, public fee access networks, cooperative networks, subscription networks, government and defense networks, Department of Defense networks used for Command, Control, Communications, and Intelligence) also known as C3i), computer reliant public utilities, and computer reliant technology. The NII's primary objective was to facilitate development of a national policy that would encourage competition and the rapid deployment of new technology.

NIPC: National Infrastructure Protection Center.

NIST: National Institute of Standards for Technology.

NME: National Military Establishment.

NPR: National Performance Review.

NREN: National Research and Education Network.

NSA: National Security Agency.

NSC: National Security Council.

- O -

OMB: Office of Management and Budget.

One-Time Password: In network security, a password issued only once as a result of a challenge-response authentication process. Cannot be "stolen" or reused for unauthorized access.

Operating System: System software that controls a computer and its peripherals. Modern operating systems such as Windows 95 and NT handle many of a computer's basic functions.

- P -

Password: A secret code assigned to a user. Knowledge of the password associated with the user ID is considered proof of authorization. (See One-Time Password.)

PCCIP: President's Commission on Critical Infrastructure Protection. Established in 1996, the Commission was tasked with developing a report for submission to the President on the vulnerabilities and threats to the nation's critical infrastructures; recommend a national policy and implementation plan for protecting critical infrastructures; determine legal and policy issues for protecting infrastructures; and, propose statutory and regulatory changes necessary to effect the recommendations.

PDD 63: Presidential Decision Directive 63.

Performance: A major factor in determining the overall productivity of a system, performance is primarily tied to availability, throughput and response time.

Perimeter-based Security: The technique of securing a network by controlling access to all entry and exit points of the network.

PIN: In computer security, a personal identification number used during the authentication process. Known only to the user.

Policy: Organizational-level rules governing acceptable use of computing resources, security practices, and operational procedures.

Private Key: In encryption, one key (or password) is used to both lock and unlock data. Compare with public key.

Protocols: Agreed-upon methods of communications used by computers.

Public Key: In encryption a two-key system in which the key used to lock data is made public, so everyone can "lock." A second private key is used to unlock or decrypt.

- Q -

[No Entries]

- R -

R&D: Research and Development.

Remote Access: The hookup of a remote computing device via communications lines such as ordinary phone lines or wide area networks to access network applications and information.

Risk Analysis: The analysis of an organization's information resources, existing controls and computer system vulnerabilities. It establishes a potential level of damage in dollars and/or other assets.

Rogue program: Any program intended to damage programs or data. Encompasses malicious Trojan Horses.

- S -

Scalability: The ability to expand a computing solution to support large numbers of users without impacting performance.

Server: The control computer on a local area network that controls software access to workstations, printers and other parts of the network.

Server-based Computing: An innovative, server-based approach to delivering business-critical applications to end-user devices, whereby an application's logic executes on the server and only the user interface is transmitted across a network to the client. Its benefits include single-point management, universal application access, bandwidth-independent performance, and improved security for business applications.

Server Farm: A group of servers that are linked together as a 'single system image' to provide centralized administration and horizontal scalability.

Smart Card: A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.

Social Engineering: An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user, to attempt to gain illicit access to systems.

- T -

Threat: [As defined by the CSTB.] A hostile party with the potential to exploit a vulnerability and cause damage.

Token: A "token" is an authentication too, a device utilized to send and receive challenges and responses during the user authentication process. Tokens may be small, hand-held hardware devices similar to pocket calculators or credit cards. See key.

Trojan Horse: 1) Any program designed to do things that the user of the program did not intend to do or that disguises its harmful intent. 2) Program that installs itself while the user is making an authorized entry; and, then are used to break-in and exploit the system.

- U -

User: Any person who interacts directly with a computer system.

User ID: A unique character string that identifies users.

User Identification: User identification is the process by which a user identifies himself to the system as a valid user. (As opposed to authentication, which is the process of establishing that the user is indeed that user and has a right to use the system.)

User Interface: The part of an application that the user works with User interfaces can be text-driven, such as DOS, or graphical, such as Windows.

- V -

Virus: A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors. Viruses attach themselves to other files and code segments and spread through those elements, usually in response to action taken by users, e.g., opening an e-mail attachment.

Vulnerability: [As defined by the CSTB.] An aspect of some system that leaves it open to attack.

- W -

WANK: Worms Against Nuclear Killers. A computer worm protesting the Galileo launch that infected NASA computers in 1989. The WANK attack cost the space agency approximately $500,000 in wasted time and resources. While the attack did not affect the Galileo launch, the source of the attack was never identified.

Worm: A computer worm is an autonomous piece of software that spreads on its own.

- XYZ -

Y2K: An acronym for the Year 2000 problem that involved three issues - two-digit data storage, leap year calculations and special meanings for dates.

BIBLIOGRAPHY

BOOKS

Allison, Graham and Treverton, Gregory F. *Rethinking America's Security: Beyond the Cold War to New World Order.* New York: W.W. Norton & Company, 1992.

Beniger, James R. *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge: Harvard University Press, 1986.

Bentley, Arthur. *The Process of Government.* Bloomington: The Principia Press, Inc., 1935.

BloomBecker, Buck. *Spectacular Computer Crimes: What They Are and How They Cost American Business Half a Billion Dollars a Year.* Illinois: Dow Jones-Irwin, 1990.

Bowman, Stephen. *When the Eagle Screams: America's Vulnerability to Terrorism.* New York: Carol Publishing Group, 1994.

Brodie, Bernard and Fawn, M. *From Crossbow to H-Bomb.* Bloomington: Indiana University Press, 1973.

Carey, Roger and Salmon, Trevor C. *International Security in the Modern World.* New York: St. Martin's Press, 1992.

Clough, Bryan and Mungo, Paul. *Approaching Zero: the Extra-ordinary Underworld of Hackers, Phreakers, Virus Writers and Keyboard Criminals.* New York: Random House, 1992.

Corwin, Edwards S. *The President: Office and Powers.* New York: New York University Press, 1948.

Davis, Richard. *The Web of Politics: The Internet's Impact on the American Political System.* Oxford: University Press, 1999.

Deering, Christopher. *Congressional Politics.* Illinois: The Dorsey Press, 1969.

Denning, Peter J. *Computers Under Attack: Intruders, Worms, & Viruses.* New York: ACM Press, 1991.

Drucker, Peter. *Post-Capitalist Society.* New York, Harper Business, 1993.

Easton, David. *A Framework for Political Analysis,* 2nd ed. Chicago: The Chicago University Press, 1979.

Fenno, Richard. *The Power of the Purse.* Boston: Little Brown, 1966.

Fitzpatrick, John C. ed. *The Writings of George Washington.* Washington, D.C.: U.S. Government Printing Office, 1939.

Frederick, Howard H. *Global Communication and International Relation.* Belmont, CA: Wadsworth Publishing Company, 1993.

Gorbachev, Mikhail. *Perestroika.* New York: NY: Harper & Row, 1987.

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

Hart, James. *The Ordinance Making Powers of the President of the United States* Baltimore: Johns Hopkins University Press, 1925.

Havelock, Eric A., and Jackson P. Hershbell. *Communication Arts in the Ancient World.* New York, NY: Hastings House, 1978.

Headrick, Daniel R. *The Invisible Weapon: Telecommunications and International Politics 1851-1945.* New York, NY: Oxford University Press, 1991.

Jervis, Robert. *The Meaning of the Nuclear Revolution.* Ithaca: Cornell University Press, 1989.

Jewell, Malcolm, and Samuel Patterson. *The Legislative Process in the United States.* New York: Random House, 1977.

Kamarck, Elaine, and Joseph Nye. *Democracy.com? Governance in a Networked World.* New York: Hollis Publishing, 1999.

Kennedy, Paul. *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500-2000.* New York: Vintage Books, 1987.

Light, Paul. *Forging Legislation.* New York: W.W. Norton and Company, 1992.

Malbin, Michael. *Unelected Representative: Congressional Staff and the Future of Representative Government.* New York: Basic Books, 1980.

Mayer, Kenneth R. *With the Stroke of a Pen: Executive Orders and Presidential Power.* Princeton, N.J.: Princeton University Press, 2001.

McDonald, Forrest. *The American Presidency: An Intellectual History.* Lawrence: University Press of Kansas, 1994.

Nacht, Michael, Quester, George H., and Weltman, John J. *Challenges to American National Security in the 1990s.* New York: Plenum Press, 1991.

Neustadt, Richard E. *Presidential Powers.* New York: John Wiley and Son, Inc., 1964.

Nye, Joseph S. *Understanding International Conflicts.* New York: Harper Collins, 1993

Paludan, Phillip Shaw. *The Presidency of Abraham Lincoln.* Lawrence: University Press of Kansas, 1994.

Petersen, John L. *The Road to 2015: Profiles of the Future.* California: Waite Group Press, 1994.

Quittner, Joshua and Michelle Slatalla. *Masters of Deception: The Gang that Ruled Cyberspace.* New York: Harper Collins, 1995.

Ripley, Randall P. *Congress: Policy and Process.* New York: W.W. Norton and Company, 1988.

Rochlin, Gene I. *Trapped in the Net: The Unanticipated Consequences of Computerization.* New Jersey: Princeton University Press, 1997.

Rosenthal, Alan. *The Third House: Lobbyists and Lobbying in the State.* Washington, DC: Congressional Quarterly Press, 1993.

Rossiter, Clinton. *The Federalist Papers.* New York: Penguin Group, 1961.

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

Selltiz, Claire, Marie Jahoda, Morton Deutsch, and Stuart W. Cook. *Research Methods in Social Relations* New York: Holt, Rinehart & Winston, 1951.

Skolnikoff, Eugene B. *The Elusive Transformation: Science Technology and the Evolution of International Politics.* New Jersey: Princeton University Press, 1993.

Snyder, Jack. *Myths of Empire: Domestic Politics and International Ambition.* Ithaca: Cornell University Press, 1991.

Sterling, Bruce. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* New York: Bantam Books, 1992.

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

__________. *Silicon Snake Oil: Second Thoughts on the Information Highway.* Doubleday - Dell Publishing, Inc., 1995.

Toffler, Alvin. *The Third Wave.* New York: William Morrow and Company, Inc., 1980.

Treverton, Gregory F. *Reshaping National Intelligence for an Age of Information.* London: Cambridge University Press, 2001

Truman, David. *The Governmental Process: Political Interests and Public Opinion,* 1st ed. New York: Alfred A. Knopf, Inc., 1951.

Tyson, James L. *Target America: The Influence of Communist Propaganda on U.S. Media.* Chicago: Regnery Gateway, 1981.

Weltman, John J., Michael Nacht, and George H. Quester. *Challenges to American National Security in the 1990's.* New York: Plenum Press, 1991.

Wilhem, Anthony. *Democracy in a Digital Age: Challenges to Political Life in Cyberspace.* New York: Routledge, 2000.

Young, Oran. *Systems of Political Science.*

Zand, Dale E. *Information, Organization and Power: Effective Management in the Knowledge Society.* New York: McGraw-Hill, 1981.

CASE LAW

Armstrong v. United States, 80 U.S. 154, 156 (1871).

I.N.S. v. Chadha, 462 U.S. 919 (1983).

Morrison v. Olson, 487 U.S. 654 (1988).

Myers v. United States, 272 U.S. 52, 164 (1926).

Public Citizen v. Burke, 843 F.2d 1473, 1477 (D.C. Cir. 1988).

U.S. Chamber of Commerce v. Reich, 74 F.3d 1322, 1332-1337 (D.C. Cir. 1996).

Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

SCHOLARLY JOURNALS

American Bar Association. *Report of the Special Committee on Administrative Law.* Chicago: American Bar Association, 1934.

Arquilla, John and Ronfeldt, David. "Cyberwar and Netwar: Warfare Between Networks." *Comparative Strategy* 12, no. 2 (1993) : 141-165.

Chapman, Gary. "National Security and the Internet." LBJ School of Public Affairs. *The 21st Century Project.* University Station University of Texas (July 1998).

Cooper, Richard N. "Economic Interdependence and Foreign Policy in the Seventies." *World Politics* (January 1972) : 159.

Dubik, Colonel James M. and Sullivan, General Gordon R. "War in the Information Age." *Strategic Studies Institute.* U.S. Army War College (6 June 1994).

Egan, Bruce L. "Building Value Through Telecommunications: Regulatory Roadblocks on the Information Superhighway." *Journal of Telecommunications Policy* 18, no. 8, UK (November 1994) : 573-587.

Fleishman, Joel L., and Arthur H. Aufses. "Law and Orders: The Problem of Presidential Legislation," *Law and Contemporary Problems* 40 (1976).

Gore, Al. Infrastructure for the Global Village." *Scientific American*, Special Issue (1995) : 156-159.

Griswold, Erwin N. "Government in Ignorance of the Law," *Harvard Law Review* 43 (1934).

Heritage Foundation. "Defending the American Homeland: A Report of The Heritage Foundation Homeland Security Task Force." Washington, D.C.: The Heritage Foundation, 2002.

Jervis, Robert. "Deterrence Theory Revisited." *World Politics* (January 1979) : 289-324.

_________. "Cooperation Under the Security Dilemma." *World Politics* (January 1978) : 167-214.

Kapor, Mitchell. "Civil Liberties in Cyberspace." *Scientific American,* Special Issue (1995) : 174-178.

Legro, Jeffrey W. "Military Culture and Inadvertent Escalation in World War II." *International Security* 18, no.4 (Spring 1994) : 108.

Levy, Jack. "Theories of General War." *World Politics* 37, no. 3 (April 1985) : 344-374.

Lord, Clifford L. "Presidential Executive Orders" *WPA Historical Records Survey* 1, comp. (1944) : 1

__________. "List and Index of Presidential Executive Orders" Unnumbered Series *New Jersey Historical Records Survey Project* (1943) : v.

Mast, Lucas. "Is the Government Protecting Our Information?" *CATO Institute* (28 November 2001).

Miller, Geoffrey P. "The Unitary Executive in a Unified Theory of Constitutional Law: The Problem of Interpretation", 15 *Cardozo L. Rev.* 201 (1993).

Moeller, Michael. "Technology: Data Superhighway," *Communications International* 20, no. 7 (1993) : 16, 20.

National Science Foundation, Digital Government Research Center, *dg.o 2000 Conference. "Press Release."* [on-line] (NSR PR 00-31. 15 May 2000). Available from http://www.nsf.gov/odlpa/news/press/00pr0031.htm; Internet.

National Science Foundation, *Science – The Endless Frontier,* by Vennevar Bush. Washington: National Science Foundation, 1980.

National Research Council. "Computers at Risk: Safe Computing in the Information Age." *Computer Science and Telecommunications Board* (Washington, D.C.: National Academy Press, 1991) : 7.

National Research Council. "Cybersecurity Today and Tomorrow: Pay Now or Pay Later." *Computer Science and Telecommunications Board* (Washington, D.C.: National Academy Press, 2002) : 3.

National Resources Committee, *Research – A Nation Resource,* 3 vols. (Washington, D.C.: National Resources Committee, 1935 – 1941).

Olson, William J., and Alan Woll. "Executive Orders and National Emergencies." Cato Institute. *Policy Analysis* 358 (October 28, 1999) : 9.

Ronfeldt, David. "Cyberocracy is Coming." *The Information Society Journal* 8, no. 4 (1992) : 243-296.

Rosecrance, Richard and Arthur Stein. "Interdependence: Myth or Reality?" *World Politics* 26, no. 1 (1973) : 1-27.

Schoeff, Mark. "Cybersecurity: Current Challenges Larger than National Strategy Response" *Center for Strategic and International Studies* (18 September 2002).

Schwartau, Winn. "Something Other Than War." *Cyberwar 2.0.* Fairfax: AFCEA International Press, 1998.

Vaida, Bara. "Cyber Security: Expert Emphasizes That Cooperation Is Key To Security." *National Journal* (23 October 2001).

MAGAZINES

Anthes, Gary H. "Industry CEOs Push National Digital Net," *Computerworld* 27, no. 3 (18 January 1993) : 25.

_________. "Info-terrorist Threat Growing." *Computer World* 29, no. 5 (30 January 1995) : 1.

Aponovich, David. "Poll: Americans Fear Cyber Attacks." *CIO Information Network.* (12 December 2001). http://cin.earthweb.com/news/article.php/10493_939191; Internet.

Benhamou, Eric. "NII Development." *Telecommunications* 28, no. 1 (January 1994) : 23-24.

Burton, Tinabeth. "ITAA Poll Finds Almost Three of Four Americans Concerned about Cyber Security." *Information Technology Association of America*, Press Release. (11 December 2001). Available from http://www.itaa.org/news/pr/PressRelease.cfm?ReleaseID=1008095083; Internet.

Chan, Curtis. "Broadcasters and the IWay," *Broadcast Engineering* 36, no. 12 (December 1994) : 28-32.

Chabrow, Eric. "State CIOs Losing Faith In Bush Administration Promises." *InformationWeek.Com.* (4 March 2003). Available from http://www.informationweek.com; Internet.

Chapin, Lyman. "The State of the Internet." *Telecommunications* 28, no. 1 (January 1994) : 13-16.

Cohen, Bob. "ITAA Calls Failing Grade for Fed Cyber Security Unacceptable." *Information Technology Association of America*, (9 November 2001).

Datz, Todd. "A More Perfect Union. The E-Government Act of 2002: The Dollars, the Players, the Hurdles, the Future." *CIO Magazine* (1 March 2003). Available from http://www.cio.com/archive/030103/union_content.html; Internet.

Dean , Joshua. "Systems Failure," *Government Executive Magazine.* (2 February 2002). Available from http//www.govexec.com/news/index.cfm?mode=report&articleid=22061; Internet.

Der Derian, James. "Cyber-Deterrence." *Wired* (September 1994) : 116-122.

Frank, Diane. "Clark Presses Industry on Security." *Federal Computer Week* 5. 5 December 2001 [journal on-line]. Available from http://www.fcw.com/fcw/articles/ 2001/1203/web-clarke-12-05-01.asp; Internet.

Government Executive Magazine. "Public, Private Sectors Advised to Share Data to Combat Cyber Attacks." *Government Executive Magazine* (19 October 2001). Available from http://www.cmm.com/2002/TECH/industry/01/08/security.reut/index.html?related; Internet.

Harris, Shane. "Cultural Barriers, Not Technology, Blamed for Poor Information Sharing." *Government Executive Magazine.* (26 February 2002).

Kapor, Mitchell. "Where is the Digital Highway Really Heading?: The Case for a Jeffersonian Information Policy." *Wired Magazine.* (July 1993) : 53-59.

Lou, Michael. "Fly the friendly skies." *Satellite Communications* 18, no. 2 (February 1994) : 20.

Lundquist, Eric. "Cyber-Defense Plan Needs to Stay on Target." *e-Week Magazine* (23 September 2002). Available from http://www.eweek.com/article2/0%2C3959%2C547299%2C00.asp; Internet.

Mann, Paul. "Dialing for 'Info War'." *Aviation Week and Space Technology* 142, no. 4 (23 January 1995) : 31.

McCarthy, Jack. "Government Relax Encryption Regulations." *PC News World.Com* (3 April 2000).

McDowell, Mindy. "Who's Securing Networked Systems?" *InfoSec Outlook* 1, no. 6 The Information Technology Association of America, 2001.

Morain, Dan. “Hackers Victimize Cal-ISO.” *Los Angeles Times Online.* http://www.latimes.com/news/state/20010609/t00047994.html; Internet.

Nathan, Paco Xander. “Jackson Wins, Feds Lose.” *Wired.* (May 1993) : 20.

Newsbytes. “Hackers Now Setting Their Sights on Pakistan,” *Newsbytes*, (5 June 1998).

Porteus, Liza. “Management, Not Technology, Is The Problem, OMB Says.” *Government Executive Magazine.* (19 February 2002). Available from http://www.govexec.com/dailyfed/0202/021902td.htm; Internet.

Shein, Esther. “Homeland Security CIO: Information (Sharing) Is Power.” *CIO Information Network.* (4 June 2002). Available from http//cin.earthweb.com/news/article.php/10493_1183981; Internet.

Vaida, Bara. “Clarke Presses Private Sector to Protect Against Cyber Attacks,” *Government Executive Magazine* (14 February 2002).

NEWSPAPERS

Bridis, Ted. “Hackers Become an Increasing Threat.” *Associated Press* (7 July 1999).

Carter, Janelle. “Hackers Hit U.S. Military Computers.” *Associated Press* (6 June 1998).

Crenson, Matt. “U.S. May Use ‘E-Bomb’ During Iraq War.” *Associated Press* (19 March 2003).

Defense Daily. "Services Gear Up for Information War." *Defense Daily* 184, no. 48 (8 September 1994) : 377.

Gertz, Bill. “Electronic Crime Threatens Integrity of Long Distance Phone System.” *The Washington Times* (24 October 1994) : A3.

Glave, James. “Crackers: We Stole Nuke Data.” *Wired News* (3 June 1998).

Graham, Bradley. “Bush Orders Guidelines for Cyber-Warfare.” *Washington Post.* (7 February 2003) : A01.

Gross, Tom. “Israeli Claims to Have Hacked Saddam Off the Net.” *London Sunday Telegraph* (7 February 1999).

Harmon, Amy. "Hacktivists of all Persuasions Take Their Struggle to the Web." *The New York Times* (31 October 1999).

Kaplan, Fred. "U.S. Bombs Not Much 'Smarter'" *Boston Globe* (20 February 1998) : A01.

McCullagh, Declan. "Congress Mulls Stiff Crypto Laws." *Wired News* (13 September 2001). Available from http://www.wired.com; Internet.

Murdoch, Lindsay. "Computer Chaos Threat to Jakarta." *Sydney Morning Herald* (18 August 1999) : 9.

Randle, Jim. "New US Weapons." *Voice of America* (13 February 1998).

Raspberry, William. "Embracing Big Brother." *The Washington Post* (25 November 2002) : A15.

Reuters. "Experts: Cybersecurity Plan Offers Tips, Not Rules." *USA Today* (16 September 2002). Available from www.usatoday.com/tech/news/techpolicy/2002-09-16-cyber-plan_x.htm; Internet.

_________. "Lawmaker: More Encryption Needed." *Reuters* (21 September 2001).

_________. "Report: Many U.S. Firms at Risk for Cyberattacks." *CNN.com* (8 January 2002.

__________. "SQL Slammer Worm Spread Worldwide in 10 Minutes." *Reuters* (4 February 2003).

PUBLIC DOCUMENTS

General Accounting Office. *Report on Instances of Unauthorized Access to Space Physics Analysis Networks*. Washington, D.C.: GPO, 1989.

General Accounting Office. *Report on Implementation of Computer Security Act.* Washington, D.C.: GPO, 1990.

General Accounting Office. *Information Superhighway: An Overview of Technology Challenges.* Washington, D.C.: GPO, 1995.

General Accounting Office. *Customs Service Modernization: Strategic Information Management Must Be Improved for National Automation Program to Succeed.* GAO/AIMD-96-57. Washington, D.C.: GPO, 1996.

General Accounting Office. *Defense IRM: Critical Risks Facing New Materiel Management Strategy.* GAO/AIMD-96-109. Washington, D.C.: GPO, 1996.

General Accounting Office. *Information Management Reform: Effective Implementation Is Essential for Improving Federal Performance.* GAO/T-AIMD-96-132. Washington, D.C.: GPO, 1996.

General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks.* GAO/T-AIMD-96-92. Washington, D.C.: GPO, 1996.

General Accounting Office. *Information Technology Investment: Agencies Can Improve Performance, Reduce Costs, and Minimize Risks.* GAO/AIMD-96-64. Washington, D.C.: GPO, 1996.

General Accounting Office. *Information Security: Opportunities for Improved OMB Oversight of Agency Practices.* GAO/AIMD-96-110. Washington, D.C.: GPO, 1996.

General Accounting Office. *Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks.* GAO-01-1168T. Washington, D.C.: GPO, 2001.

General Accounting Office. *Homeland Security, Intergovernmental Coordination and Partnership Will Be Critical to Success.* GAO-02-901T. Washington, D.C.: 2002.

Government Information Technology Services. Government Information Technology Services Working Group. Committee on Application and Technology: *A Vision for the Government Information Technology Services and the National Information Infrastructure Report.* (August 1994).

National Institute of Standards and Technology. Computer Security Division. *Threat Assessment of Malicious Code and Human Threats.* (1992) Washington, D.C.: GPO, 1992.

Office of Management and Budget. *(House) H.R. 1903 – Computer Security Enhancement Act (Sensenbrenner (R) Wisconsin and 29 Others).* Available from http://www.whitehouse.gov/omb/legislative/sap/105-1/hr1903-h.html; Internet. September 15, 1997.

Office of Science and Technology Policy. National Security and International Affairs Division. *Cybernation: The American Infrastructure in the Information Age. A Technical Primer on Risk Reliability.* (7 January 1998).

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* Washington, D.C.: GPO, 1997.

U.S. Department of Commerce. "Guide to a Balanced Scorecard Performance Management Methodology: Moving from Performance Measurement to Performance Management." *Procurement Executives' Association* (Washington, D.C.: 1999).

U.S. Department of Defense. Defense Science Board. *Report of the Task Force on Information Warfare-Defense.* (Washington, D.C.: GPO, 1996) : 1.

U.S. Congress. "Defending America in the 21st Century: New Challenges, New Organizations and New Policies" by Frank Cilluffo, Joseph C. Collins, Arnaud de Borchgrave, Daniel Goure, and Michael Horowitz. *CSIS* (Washington, D.C.: GPO, 2000) : 8, 15, 23.

U.S. Congress. "Cyber Threats and Information Security: Meeting the 21st Century Challenge" by Arnaud de Borchgrave, Frank J. Cilluffo, Sharon Cardash, and Michele M. Ledgerwood. *CSIS* (Washington, D.C.: GPO, 2001).

U.S. Congress. *Annals of Congress* 1. Washington, D.C.: GPO, 1789.

U.S. Congress. House. *CIS/Index.* "Presidential Executive Orders and Proclamations.

U.S. Congress. House. Committee on Science and Technology. *Digital Tech Corps: Hearing before the Committee on Science and Technology.* 102nd Cong., 2nd sess., October 1991.

U.S. Congress. House. Committee on Science. *The Computer Security Enhancement Act of 1997: Hearing before the Subcommittee on Technology.* 105nd Cong., 1st sess., 19 June 1997.

U.S. Congress. House. Committee on Science. Congressman Sensenbrenner speaking for the *The Computer Security Enhancement Act of 1997* to the *Subcommittee on Technology.* 105nd Cong., 1st sess. *Congressional Record.* (19 June 1997).

U.S. Congress. House. Committee on Rules. Principal Deputy Assistant Attorney General, Douglas R. Cox speaking for the *Legislative and Budget Process* to the Committee on Rules. 106th Cong., 2nd sess. *Congressional Record.* (27 October 1999).

U.S. Congress. House. Subcommittee Chairman Stephen Horn speaking before the *Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations.* (9 November 2001).

U.S. Congress. Senate. Committee on Government Operations. *National Emergencies Act: Hearing before the Committee on Government Operations.* Cong., 2nd sess., 1972.

U.S. Congress. Senate. Committee on Governmental Affairs. *Hackers Penetrate D.O.D Computer Systems: Hearing before the Subcommittee on Government Information & Regulation.* 102nd Cong., 2nd sess., 20 November 1991.

U.S. Congress. Senate. Committee on Governmental Affairs. *Jack L. Brock speaking For Hackers Penetrate DOD Computer Systems before the Subcommittee on Government Information & Regulation.* 102nd Cong., 2nd sess., 20 November 1991.

U.S. Congress. Senate. Committee on Governmental Affairs. *John S. Tritak speaking for Critical Infrastructure Protection: Who's in Charge? Before the Committee on Governmental Affairs*, 4 October 2001.

U.S. Congress. Senate. Chairman Jon Kyl speaking for *Crime, Terror, & War: National Security & Public Safety in the Information Age* before the Committee on the Judiciary Subcommittee on Technology, Terrorism, and Government Information. (13 November 1998.)

U.S. Congress. Senate. Committee on Government Reform. Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations. Mark Rasch speaking before the *Subcommittee on Government Management, Information, and Technology*. (9 March 2000).

U.S. Congress. Senate. Lawrence Gershwin speaking before the *Joint Economic Committee*. (18 June 2001).

U.S. Constitution, art. 1, sec. 8.

U.S. Constitution, art. 2, sec. 2.

U.S. Constitution, art. 2, sec. 3.

U.S. Department of Commerce. *Draft II Encryption Export Regulations.* (17 December 1999).

U.S. Department of State. *Computer Security and Critical Infrastructure: Clinton on Keeping America Secure for 21st Century. USIS Washington File.* January 22, 1999.

U.S. Department of State. *U.S. Corporations Warned of Cyber-Terrorism: Greater Security Needed Against Electronic Attacks,* by Charlene Porter. *USIS Washington File.* November 4, 1999.

U.S. Department of State. U.S. Foreign Policy Agenda. *Weapons of Mass Destruction (WMD): The New Strategic Framework* 7, no. 2. Washington, D.C.: GPO, July 2002.

U.S. Library of Congress. Congressional Research Service. *CRS Report for Congress. Federal Support of Basic Research and the Establishment of the National Science Foundation and Other Research Agencies (June 1988)*, by William C. Boesman. 88-456 SPR, June 28, 1988.

_______________. Congressional Research Service. *CRS Report for Congress. Federal Research and Developing Funding: A Concise History (December 1995),* by Richard E. Rowberg. 95-1209 SPR, December 15, 1995.

_______________. Congressional Research Service. *CRS Report for Congress. Presidential Directives: Background and Overview (July 1998),* by Harold C. Relyea. 98-611 GOV, July 16, 1998.

_______________. Congressional Research Service. *CRS Report for Congress. Cyberwarfare (June 2001),* by Steven A. Hildreth. June 19, 2001.

U.S. President, William J. Clinton. Executive Order 13010. *Federal Register* 16, no. 138 (17 July 1996) : 3747-3750.

____________. Executive Order 13119 (1999).

____________. Executive Order 13120 (1999).

____________. *Technology for America's Economic Growth: A New Direction* Washington, D.C.: White House, Office of the Press Secretary, 1993.

____________. *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998.

____________. Remarks by the President in Photo Opportunity with Leaders of High-Tech Industry and Experts on Computer Security. The Cabinet Room. The White House. (15 February 2000). Available from http://10.147.64.15:5666/hyper/2000/0215/epf203.htm; Internet.

U.S. President, Abraham Lincoln. Emancipation Proclamation (1862 original).

__________. Emancipation Proclamation (1863 final).

U.S. President, Ronald Reagan. Executive Order 12865 (1993)

__________. Executive Order 12947 (1995)

__________. Executive Order 12978 (1995).

U.S. President, Franklin D. Roosevelt. Executive Order 9066.

U.S. President, Harry S Truman. Executive Order 9981; 10340.

The White House. Vice President Albert Gore speaking for the Federal-State-Local Telecommunications Summit (9 January 1994). Available from http://whitehouse.gov; Internet.

The White House. "Berger Confirms Clinton Effort to Develop National Computer Security System." *USIS Washington File.* July 28, 1999.

The White House. "National Strategy to Secure Cyberspace." (February 2003) Washington, D.C.: GPO, 2003.

UNITED STATES CODE

Brooks Act. U.S. Code (1972).

Computer Security Act. U.S. Code (1987).

Computer Security Enhancement Act. U.S. Code (1997).

Cyberspace Electronic Security Act of 1999. U.S. Code (1999).

E-Government Act. U.S. Code (2002).

Federal Acquisition and Streamlining Act. U.S. Code (1994).

Federal Property and Administrative Services Act. U.S. Code (1949).

Government Performance and Results Act. U.S. Code (1993).

Government Management Reform Act. U.S. Code (1994).

Information Technology Management Reform Act. U.S. Code (1996).

National Emergencies Act, 50 U.S. Code, sec. 1601-51. (1972).

National Information Infrastructure Act. U.S. Code (1993).

UNPUBLISHED WORKS

Hallion, Richard P. "Precision Guided Munitions and the New Era of Warfare." *Air Power Studies Centre* Working Paper No. 53. Washington, D.C.

Schwartau, Winn. "Class II Information Warfare: Corporate Espionage and Sabotage." Presentation at the *Second International Conference on Information Warfare.* Montreal (18 January 1995).

Steele, Robert. "War and Peace in the Age of Information." Superintendent's Guest Lecture, *Naval Post Graduate School* (17 August 1993).

___________. "The Military Perspective on Information Warfare: Apocalypse Now." Keynote address at the *Second International Conference on Information Warfare: Chaos on the Electronic Superhighway.* Montreal (19 January 1995).

Stoll, Clifford. "Stalking the Wiley Hacker." *Communications of the ACM* (May 1988).

Ware, Willis H. "The Cyber-Posture of the National Information Infrastructure." *RAND Corporation.* (1997). Available from http://www.rand.org/publications/MR/MR976/mr976.html; Internet.